Álgebra superior

Carmen Gómez Laveaga
Departamento de Matemáticas
Facultad de Ciencias UNAM

A Luis
A mis hijos Alejandro, Ernesto y Aurora
A mis nietos Sabina, Pablo e Isabella

Índice general

"¿Qué importa saber lo que es una línea recta si no se sabe lo que es la rectitud ?".
Séneca
4? - 65

Introducción

Este libro está dirigido a alumnos que deban cursar la(s) materia(s) introductoria(s) de álgebra en las distintas carreras que así lo requieran. El espíritu es que sea lo más completo posible, en el sentido de que, dependiendo de cada programa, los temas que lo conforman estén cubiertos en el libro y el lector interesado puede tener una idea general sobre la materia; en particular cómo se construyen los distintos sistemas de numéricos: naturales, enteros, racionales, reales y complejos.

Por ejemplo, si en un programa aparece el tema de cálculo combinatorio, en donde se trabaja con conjuntos finitos, se puede manejar la idea intuitiva de este concepto sin tener que pasar por el capítulo 3 (conjuntos finitos).

El capítulo 0 tiene la intención de introducir, muy brevemente, el lenguaje matemático y algunos tipos de demostración. El hecho de que sea bastante corto es porque, desde mi punto de vista, el aprendizaje y el rigor matemático se van adquiriendo y desarrollando de manera paulatina.

En los capítulos 2, 6 y 9 se presentan los números naturales, enteros, y racionales de una manera intuitiva.

En el capítulo 5 se introducen los Sistemas de Peano en donde se demuestra que dos sistemas de estos se pueden considerar como el "mismo" (isomorfos) y donde se presentan los números naturales como un sistema de Peano.

En los capítulos 8, 10, 11 y 12 se presentan modelos de los sistemas numéricos, respectivamente enteros, racionales, reales y complejos.

El capítulo 7 está dedicado al estudio de números enteros desde el punto de vista de la divisibilidad (Teoría de números) y el capítulo 13 al estudio de polinomios.

Los temas de los capítulos 14 y 15 tiene como finalidad el estudio de sistemas de ecuaciones lineales.

La mayoría de los capítulos cuentan con una buena cantidad de ejercicios con distintos niveles de dificultad para que el alumno refuerce y madure los conceptos desarrollados.

Agradecimientos

Quisiera mencionar la revisión tan minuciosa que realizó de este libro el (la) profesor (a) a quien se le encomendó el arbitraje de él, le agradezco de manera muy especial sus comentarios y sugerencias.
También agradezco a Rolando Gómez Macedo y Ernesto Mayorga Saucedo el magnífico e invaluable trabajo que hicieron al transcribir las notas a LaTeX de manera tan profesional.

No soy demostrable
en la teoría T.
Kurt Gödel
1906 - 1978

***Capítulo* 0**

Algo de lógica

Parte fundamental en la matemática es su lenguaje, éste se usa para expresar de manera precisa y sin ninguna ambigüedad las proposiciones de una teoría.
Las proposiciones son expresiones o afirmaciones que tienen uno y sólo un valor de verdad asignado: verdadero (V) o falso (F). Generalmente usamos el lenguaje ordinario para enunciar las proposiciones, esto nos puede dificultar la decisión de si un razonamiento es válido o no debido a que las palabras pueden tener distintos significados y son presa de interpretación. Es aquí donde la lógica matemática juega un papel fundamental: proporciona herramientas para construir proposiciones y nos da reglas para deducir, con las cuales podemos decidir si un razonamiento es válido o no, lo que nos lleva a concluir la veracidad de una proposición.
Es importante dejar bien claro que el objetivo de esta introducción no es hacer un estudio amplio, detallado y totalmente formal de la lógica matemática, sino más bien dejar en claro qué es "demostrar" en matemáticas.

§ 0.1 Introducción de los símbolos lógicos y tablas de verdad

Iniciamos introduciendo algunos símbolos lógicos: conectivos lógicos, paréntesis, variables, constantes extralógicos y cuantificadores.
En lo que sigue P , Q, R, P_1, etc. denotarán proposiciones.

I) ***Los conectivos lógicos*** son símbolos mediante los cuales podemos construir nuevas proposiciones a través de otras y estos son los siguientes
i) $\wedge$: "***y***". $\boldsymbol{P \wedge Q}$ se lee P y Q.

ii) $\vee$: "***o***". $\boldsymbol{P \vee Q}$ se lee P o Q, donde la "o" es inclusiva, es decir, significa P o Q o ambas.

iii) $\neg$: "***no***". $\boldsymbol{\neg P}$ se lee no P

iv) $\Rightarrow$: "***implica***". $\boldsymbol{P \Rightarrow Q}$ se lee P implica Q y se define en términos de $\neg$ y $\vee$ por $P \Rightarrow Q : (\neg P) \vee Q$.

v) $\Leftrightarrow$: "***si y sólo si***". $\boldsymbol{P \Leftrightarrow Q}$ se lee P "si y sólo si" Q y se define en términos de $\neg$ y $\wedge$ por $P \Leftrightarrow Q : (P \Rightarrow Q) \wedge (Q \Rightarrow P)$.

Ejemplo 0.1.1. Consideremos las siguientes proposiciones:

P: "El viento sopla muy fuerte"; Q: "se caen las hojas de los árboles";
R: "Luisa come mucho"; S: "Luisa tiene hambre";
T: "Alberto estudia"; U: "José trabaja"

Construyamos otras proposiciones usando los conectivos lógicos.

(i) $\wedge$:

$P \wedge Q$: "El viento sopla muy fuerte y se caen las hojas de los árboles"

$R \wedge T$: "Luisa come mucho y Alberto estudia"

$S \wedge U$: "Luisa tiene hambre y José trabaja"

(ii) $\vee$:

$P \vee R$: "El viento sopla muy fuerte o Luisa come mucho"

$S \vee U$: "Luisa tiene hambre o José trabaja"

$T \vee U$: "Alberto estudia o José trabaja"

(iii) $\neg$:

$\neg Q$: "No se caen las hojas de los árboles"

$\neg S$: "Luisa no tiene hambre"

$\neg T$: "Alberto no estudia"

(iv) $\Rightarrow$:

$P \Rightarrow Q$: "Si el viento sopla muy fuerte, entonces se caen las hojas de los árboles"

$S \Rightarrow U$: "Si Luisa tiene hambre, entonces José trabaja"

$T \Rightarrow P$: "Si Alberto estudia, entonces el viento sopla muy fuerte"

(v) $\Leftrightarrow$:

$P \Leftrightarrow Q$: "El viento sopla muy fuerte si y sólo si se caen las hojas de los árboles"

$R \Leftrightarrow S$: "Luisa come mucho si y sólo si Luisa tiene hambre"

$T \Leftrightarrow U$: "Alberto estudia si y sólo si José trabaja"

Existen distintas maneras de referirse a $P \Rightarrow Q$, por supuesto todas significan lo mismo. Algunas son "si P, entonces Q", "para que P es necesario Q", "P es suficiente para Q".

También existen distintas maneras de referirse a $P \Leftrightarrow Q$, y todas significan lo mismo. Algunas son "P es equivalente a Q", "una condición necesaria y suficiente para Q es P".

Evidentemente el valor de verdad que se asigna a las proposiciones construidas mediante el uso de conectivos lógicos dependerá del valor de verdad de las proposiciones que la componen. Como $P \Rightarrow Q$ y $P \Leftrightarrow Q$ se definen a través de $\wedge$, $\vee$ y $\neg$ será suficiente dar las tablas de verdad de estos conectivos. Estas tablas resultan bastante intuitivas.

$\wedge$: P	Q	$P \wedge Q$
V	V	V
V	F	F
F	V	F
F	F	F

$P \wedge Q$ es verdadera únicamente cuando ambas proposiciones, P y Q, son verdaderas.

$\vee$: P	Q	$P \vee Q$
V	V	V
V	F	V
F	V	V
F	F	F

$P \vee Q$ es verdadera únicamente cuando al menos una de ellas, P o Q, es verdadera.

$\neg$: P	$\neg P$
V	F
F	V

$\neg P$ es verdadera únicamente cuando P es falsa.

Teniendo estas tablas de verdad es posible construir las tablas de verdad de $P \Rightarrow Q$ y $P \Leftrightarrow Q$.

$\Rightarrow$: P	Q	$\neg P$	$P \Rightarrow Q$: $(\neg P) \vee Q$
V	V	F	V
V	F	F	F
F	V	V	V
F	F	V	V

Así $P \Rightarrow Q$ es falsa únicamente cuando, P es verdadera y Q es falsa.

$\Leftrightarrow$: P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$P \Leftrightarrow Q$: $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$
V	V	V	V	V
V	F	F	V	F
F	V	V	F	F
F	F	V	V	V

Así $P \Leftrightarrow Q$ es verdadera únicamente cuando ambas, P y Q, son verdaderas o ambas son falsas.

II) ***Los paréntesis*** son símbolos que sirven para agrupar proposiciones evitando con esto cualquier ambigüedad. Por ejemplo, no es lo mismo $\neg(P \wedge Q)$ que $(\neg P) \wedge Q$ y para ver esto basta comparar sus respectivas tablas de verdad.

Ejemplo 0.1.2. Consideremos las proposiciones P y Q del ejemplo 0.1.1

$\neg (P \wedge Q)$: "No es cierto que, el viento sopla muy fuerte y se caen las hojas de los árboles".

$(\neg P) \wedge Q$: "El viento no sopla muy fuerte y las hojas se caen de los árboles".

$P \wedge (\neg Q)$: "El viento sopla muy fuerte y las hojas no se caen de los árboles".

$\neg (P \vee Q)$: "No es cierto que, el viento sopla muy fuerte o se caen las hojas de los árboles".

$P \vee (\neg Q)$: "El viento sopla muy fuerte o las hojas no se caen de los árboles".

$(\neg P) \vee Q$: "El viento no sopla muy fuerte o las hojas se caen de los árboles".

$\neg (P \Rightarrow Q)$: "No es cierto que si el viento sopla muy fuerte, entonces se caen las hojas de los árboles".

$(\neg P) \Rightarrow Q$: "Si el viento no sopla muy fuerte, entonces las hojas se caen de los árboles".

$P \Rightarrow (\neg Q)$: "Si el viento sopla muy fuerte, entonces las hojas no se caen de los árboles".

$\neg(P \Leftrightarrow Q)$: "No es cierto que el viento sopla muy fuerte si y sólo si las hojas se caen de los árboles".

$(\neg P) \Leftrightarrow Q$: "El viento no sopla muy fuerte si y sólo si las hojas se caen de los árboles".

$P \Leftrightarrow (\neg Q)$: "El viento sopla muy fuerte si y sólo si las hojas no se caen de los árboles".

Como puede verse en todos estos ejemplos, dependiendo de dónde hayamos puesto el conectivo $\neg$ se obtienen proposiciones distintas.

III) ***Constantes extralógicos*** son símbolos que utilizamos para referirnos a elementos específicos en el "universo de trabajo" Por ejemplo, si estamos trabajando con los números reales, en la expresión "a es un número real tal que $a^3 = -1$", nos estamos refiriendo al número -1, ya que -1 es el único número real tal que $(-1)^3 = -1$. En la expresión "a es un número entero tal que $0 < a < 2$", nos referimos al número 1.

IV) ***Las variables***, que usualmente denotamos por $x, y, \ldots$, con o sin subíndices, no tienen valores determinados. Existen expresiones en las que en su construcción aparecen una o más variables y a las que no se les puede asignar un valor de verdad. Por ejemplo, a la expresión $x > -1$ no se le puede asignar un valor de verdad puesto que no sabemos quién es x. A este tipo de expresiones se les llama **predicado**. Sin embargo, dando valores específicos a x, obtenemos una proposición que puede ser verdadera o falsa según sea el caso. En nuestro ejemplo, si le diéramos el valor específico de -2 en los números reales a x, obtendríamos la proposición $-2 > -1$ que sabemos es falsa, pero para $x = 7$, tendríamos $7 > -1$ que es verdadera. Si denotamos por $P(x)$ a una expresión que habla de x, por cada valor específico que damos a x, por ejemplo a, obtenemos una proposición $P(a)$. Además, si $P(x)$ y $Q(x)$ son predicados, a partir de ellos podemos construir otros usando conectivos lógicos, por ejemplo

$$\neg P(x), \quad P(x) \wedge Q(x), \quad P(x) \vee Q(x), \quad P(x) \Rightarrow Q(x), \quad P(x) \Leftrightarrow Q(x).$$

En cada una de estos dando valores específicos a x, obtenemos proposiciones. Por ejemplo si $x = a$, $P(a) \wedge Q(a)$, $P(a) \vee Q(a)$, $\neg P(a)$, $P(a) \Rightarrow Q(a)$ y $P(a) \Leftrightarrow Q(a)$.

V) ***Cuantificadores universales.*** Ya hemos mencionado que al darle un valor lógico específico a una variable x en un predicado $P(x)$ obtenemos una proposición, esto es, si $x = a$, $P(a)$ es una proposición. Supongamos ahora que tenemos

un predicado $P(x)$ y que x toma valores en un conjunto X, al que llamamos conjunto de referencia o alcance de x, y supongamos que para cada valor específico de x, $P(x)$ es verdadera; esto lo podemos enunciar de la siguiente manera "para todo x $P(x)$" (siempre teniendo en cuenta que se tiene un conjunto de referencia). Introducimos un símbolo para referirnos a "para todo" que es $\forall$, al cual se le llama el cuantificador universal. Así que de un predicado $P(x)$ podemos construir una proposición que es $\forall x\ P(x)$ que será verdadera cuando $P(a)$ sea verdadera para cualquier valor a tomado en X. Por ejemplo, si el conjunto de referencia es el conjunto de los números reales, y $P(x) : x^2 \geq 0$, entonces $\forall a\ P(a)$ es una proposición verdadera. Al ser $\forall x\ P(x)$ una proposición su negación, es decir, $\neg(\forall x\ P(x))$, es también una proposición que será verdadera cuando $\forall x\ P(x)$ es falsa. Pero ¿qué significa que $\forall x\ P(x)$ es falsa? Significa que para algún valor a de x en el conjunto de referencia, $P(a)$ es falsa, o lo que es lo mismo, existe un valor a de x para el cual $\neg P(a)$ es verdadera. Es aquí donde introducimos el símbolo lógico $\exists$ que significa "existe" y se llama el cuantificador existencial. Así pues la negación de la proposición $\forall x\, P(x)$ es la proposición $\exists x\ \neg P(x)$:"existe x tal que no $P(x)$" y significa que en nuestro conjunto de referencia hay al menos un elemento a tal que $\neg P(a)$ es verdadera. Por otro lado, la negación de la proposición $\exists x\ P(x)$ es la proposición $\forall x\ \neg P(x)$, esto es, $\neg(\exists x\ P(x))$ significa que no existe x tal que $P(x)$ es verdadera, lo que nos lleva entonces a que sin importar el valor a que toma x en nuestro conjunto de referencia, $P(a)$ es falsa, con lo cual tendremos entonces que $\forall\ x\ \neg P(x)$ es verdadero. Tenemos entonces que

$$\neg(\forall x\ P(x)) \Longleftrightarrow \exists x\ \neg P(x)$$

$$\neg(\exists x\ P(x)) \Longleftrightarrow \forall x\ \neg P(x)$$

Por último presentamos distintas maneras de enunciar proposiciones que expresan a $\forall$ y $\exists$, por supuesto todas ellas dicen lo mismo.

$\forall x\ P(x)$: "para todo x $P(x)$"; "$P(x)$ para todo x"; "dado x $P(x)$"; "para cada x $P(x)$"; "$P(x)$ para cada x".

$\exists x\ P(x)$: "existe x tal que $P(x)$"; "para alguna x $P(x)$"; "$P(x)$ para alguna x".

Ejemplo 0.1.3. (a) $P(x)$: "x es mamífero" es un predicado, pero si damos el conjunto X de referencia como todos los perros y los gatos, tendremos que $\forall\ x\ P(x)$ es una proposición verdadera. Para el conjunto de referencia X de

todos los animales, $\forall\ x\ P(x)$ es falsa, puesto que no todos los animales son mamíferos.

(b) $Q(x)$: "x y Ana son amigas" es un predicado. Si consideramos como conjunto de referencia X de todas las amigas de Ana, entonces $\forall\ x\ Q(x)$ es verdadera, pero si en el conjunto X están todas las amigas de Ana y otras personas que no son amigas de Ana, entonces $\forall\ x\ Q(x)$ es falsa.

(c) $R(x)$: "$x^2 \geq 0$" es un predicado y si el conjunto X de referencia son los números reales, $\forall\ x\ R(x)$ es una proposición verdadera, pero si consideramos como X al conjunto de los números complejos, $\forall\ x\ R(x)$ es falsa (basta ver que para el número complejo i, $i^2 = -1 < 0$).

§ 0.2 Tautologías y contradicción

Se dice que una proposición es una **tautología** si su valor de verdad siempre es verdadero sin importar el valor de verdad de las proposiciones que la componen. En el caso en que la proposición $P \Leftrightarrow Q$ sea una tautología diremos que P y Q son proposiciones **tautológicamente equivalentes**. Al ser dos proposiciones P y Q tautológicamente equivalentes, tenemos que P es verdadera si y sólo si Q lo es. De esta manera, si queremos demostrar P y resulta que nos es más fácil demostrar Q, podemos hacerlo, ya que entonces P será verdadera.

Ejemplo 0.2.1. La proposición $P \vee (\neg P)$ es una tautología porque siempre es verdadera.

P	$\neg P$	$P \vee (\neg P)$
V	F	V
F	V	V

Ejemplo 0.2.2. La proposición $(P \Rightarrow Q) \Leftrightarrow [(\neg Q) \Rightarrow (\neg P)]$ es una tautología. Efectivamente, su tabla de verdad es

P	Q	$\neg P$	$\neg Q$	$P \Rightarrow Q$	$(\neg Q) \Rightarrow (\neg P)$	$(P \Rightarrow Q) \Leftrightarrow [(\neg Q) \Rightarrow (\neg P)]$
V	V	F	F	V	V	V
V	F	F	V	F	F	V
F	V	V	F	V	V	V
F	F	V	V	V	V	V

Así que $P \Rightarrow Q$ y $(\neg Q) \Rightarrow (\neg P)$ son proposiciones tautológicamente equivalentes. Esto en particular significa que $P \Rightarrow Q$ es verdadera si y sólo si $(\neg Q) \Rightarrow (\neg P)$ es verdadero.

Ejemplo 0.2.3. Consideremos la proposición $[P \wedge (P \Rightarrow Q)] \Rightarrow Q$ y construyamos su tabla de verdad

P	Q	$P \Rightarrow Q$	$P \wedge (P \Rightarrow Q)$	$[P \wedge (P \Rightarrow Q)] \Rightarrow Q$
V	V	V	V	V
V	F	F	F	V
F	V	V	F	V
F	F	V	F	V

Concluimos entonces que $[P \wedge (P \Rightarrow Q)] \Rightarrow Q$ es una tautología.

Ejemplo 0.2.4. Consideremos la proposición

$$[(P \vee Q) \Rightarrow R] \Leftrightarrow [(P \Rightarrow R) \wedge (Q \Rightarrow R)]$$

y construyamos su tabla de verdad

P	Q	R	$P \vee Q$	$(P \vee Q) \Rightarrow R$	$P \Rightarrow R$	$Q \Rightarrow R$	$(P \Rightarrow R) \wedge (Q \Rightarrow R)$	$[(P \vee Q) \Rightarrow R] \Leftrightarrow [(P \Rightarrow R) \wedge (Q \Rightarrow R)]$
V	V	V	V	V	V	V	V	V
V	V	F	V	F	F	F	F	V
V	F	V	V	V	V	V	V	V
V	F	F	V	F	F	V	F	V
F	V	V	V	V	V	V	V	V
F	V	F	V	F	V	F	F	V
F	F	V	F	V	V	V	V	V
F	F	F	F	V	V	V	V	V

Concluimos entonces que $[(P \vee Q) \Rightarrow R] \Leftrightarrow [(P \Rightarrow R) \wedge (Q \Rightarrow R)]$ es una tautología.

En el otro extremo tenemos que: una proposición se llama una **contradicción** si es siempre falsa sin importar el valor de verdad de las proposiciones que la componen.

P	$\neg P$	$P \wedge (\neg P)$
V	F	F
F	V	F

Observando la tabla de verdad de la proposición $P \Rightarrow Q$, tenemos que cuando P y $P \Rightarrow Q$ son verdaderas necesariamente Q es verdadera, esto es, de P y $P \Rightarrow Q$ verdaderas se obtiene como consecuencia que Q es verdadera. A esta regla de se le llama **modus ponens**. De esta manera, si queremos mostrar que Q es verdadera a partir de que P es verdadera, debemos ver que $P \Rightarrow Q$ es verdadera. A P se le llama **hipótesis** y a Q **conclusión**.

La demostración de una proposición consiste en que, de suponer la hipótesis verdadera y del uso adecuado de proposiciones verdaderas ya conocidas obtengamos que la conclusión es verdadera. Esto es, si suponemos que P es verdadera y si se tiene una sucesión de proposiciones verdaderas $P \Rightarrow P_1$, $P_1 \Rightarrow P_2$,..., $P_{n-1} \Rightarrow P_n$, $P_n \Rightarrow Q$, entonces podemos afirmar que Q es verdadera y esto es porque: si P y $P \Rightarrow P_1$ son verdaderas, entonces P_1 es verdadera; como P_1 es verdadera y $P_1 \Rightarrow P_2$ también lo es, entonces P_2 es verdadera; continuando de esta manera P_n es verdadera y por ser $P_n \Rightarrow Q$ verdadera; concluimos que Q es verdadera.

Ejemplo 0.2.5.

Hipótesis:	P : Pedro estudia.
Proposiciones verdaderas:	$P \Rightarrow P_1$: Si pedro estudia entonces pedro tiene buenas calificaciones
	$P_1 \Rightarrow Q$: Si pedro tiene buenas calificaciones, entonces Pedro tendrá beca
Conclusión:	Q : Pedro obtendrá una beca.

Si sabemos que $P \Rightarrow P_1$ y $P_1 \Rightarrow Q$ son verdaderas, de suponer P verdadera llegamos a que Q es verdadera.

§ 0.3 Algunos métodos de demostración

(*I*) *Demostración directa:* es la que hemos expuesto en el ejemplo 0.2.5 y el párrafo anterior a él.

(*II*) *Demostración por contraposición:* si tenemos una proposición $P \Rightarrow Q$, ya hemos visto que ésta es tautológicamente equivalente a $(\neg Q) \Rightarrow (\neg P)$ (véase el ejemplo 1.2), lo que nos dice que si queremos demostrar que $P \Rightarrow Q$ es verdadera, podemos hacerlo demostrando la proposición tautológicamente equivalente $(\neg Q) \Rightarrow (\neg P)$.

Definición 0.3.1. *Un número entero x es par si existe un entero z tal que $x = 2 \cdot z$ y un número entero es impar si no es par.*

Ejemplo 0.3.2. Consideremos las proposiciones

P : x es impar.

Q : $x + 2$ es impar.

Demostraremos que $P \Rightarrow Q$ es verdadera, mostrando que $\neg Q \Rightarrow \neg P$ es verdadera.

$\neg P$: x es par.

$\neg Q$: $x + 2$ es par.

$x + 2$ par $\Rightarrow x + 2 = 2 \cdot y$ (definición)

$x + 2 = 2 \cdot y \Rightarrow x = 2 \cdot y - 2$ (restando a ambos lados 2)

$x = 2 \cdot y - 2 \Rightarrow x = 2 \cdot (y - 1)$ (el producto en los enteros distribuye a la suma)

$x = 2 \cdot (y - 1) \Rightarrow x$ es par (definición)

Hemos demostrado que $(\neg Q) \Rightarrow (\neg P)$ es verdadera con lo cual $P \Rightarrow Q$.

(*III*) *Demostración por reducción al absurdo:* si queremos demostrar que $P \Rightarrow Q$ es verdadera, suponer P y $\neg Q$ verdaderas nos llevará a una contradicción del tipo $R \wedge (\neg R)$.

Ejemplo 0.3.3. Aceptamos como verdaderas las siguientes proposiciones: P : "Dados los enteros x, y y z, si $x \cdot y = x \cdot z$ y $x \neq 0$, entonces $y = z$" y Q : "Para todo entero x, $x \cdot 0 = 0$".

Demostraremos por reducción al absurdo que para una pareja de enteros, "Si $x \cdot y = 0$, entonces $x = 0$ o $y = 0$".

Suponemos $x \cdot y = 0$ y la negación de "$x = 0$ o $y = 0$". Siendo la negación de "$x = 0$ o $y = 0$" equivalente a "$x \neq 0$ y $y \neq 0$" (véase el ejercicio 0.1.11 (5)), demostraremos que $x \cdot y = 0$ y $x \neq 0$ y $y \neq 0$ nos lleva a una contradicción.

Supongamos que $x \cdot y = 0$, $x \neq 0$ y $y \neq 0$. Luego $x \cdot y = 0 = x \cdot 0$ (proposición verdadera Q) y como $x \neq 0$, entonces $y = 0$ (proposición verdadera P), lo cual es una contradicción porque tendríamos que $y \neq 0$ y $y = 0$. Por lo tanto debe ser $x = 0$ o $y = 0$.

(*IV*) *Demostración por casos:* consideremos la proposición $(P_1 \vee P_2) \Rightarrow Q$. En el ejemplo 0.2.4 se mostró que esta proposición es tautológicamente equivalente a la proposición $(P_1 \Rightarrow Q) \wedge (P_2 \Rightarrow Q)$, así que para demostrar que

$(P_1 \vee P_2) \Rightarrow Q$ es verdadera basta con demostrar que $(P_1 \Rightarrow Q) \wedge (P_2 \Rightarrow Q)$ es verdadera, pero esta última lo es si y sólo si $P_1 \Rightarrow Q$ y $P_2 \Rightarrow Q$ son ambas verdaderas. Entonces, para demostrar que $(P_1 \vee P_2) \Rightarrow Q$ es verdadera debemos demostrar que en el caso en que consideremos P_1 verdadera, entonces $P_1 \Rightarrow Q$ es verdadera y en el caso ene que consideremos P_2 verdadera, entonces $P_2 \Rightarrow Q$ es verdadera.

Ejemplo 0.3.4. Sabemos que en el sistema de los números complejos existe un número que denotamos por i tal que $i^2 = -1$ y que cada número real es un número complejo.

$P_1 : x$ es un número real.
$P_2 : x = i \cdot y$ donde y es un número real.
$Q : x^2$ es un número real.

Para demostrar que $(P_1 \vee P_2) \Rightarrow Q$, esto es, si x es un número real o si x es de la forma $x = i \cdot y$ donde y es un número real, entonces x^2 es un número real, demostraremos que $P_1 \Rightarrow Q$ y $P_2 \Rightarrow Q$ son ambas verdaderas.
$P_1 \Rightarrow Q$ es verdadera porque si x es un número real, x^2 es un número real ya que el producto de dos números reales es un número real.
$P_2 \Rightarrow Q$ es verdadera porque si $x = i \cdot y$, entonces $x^2 = i^2 \cdot y^2 = -y^2$, donde $-y^2$ es un número real.
Entonces podemos afirmar sin lugar a dudas que $(P_1 \vee P_2) \Rightarrow Q$ es verdadera.

§ 0.4 Ejercicios del capítulo 0.

0.1.1. Determine cuáles de las siguientes oraciones son proposiciones.

(1) El 7 de diciembre de 1941 fue domingo.
(2) Algunos números enteros son negativos.
(3) ¡Si todas las mañanas fueran tan soleadas y despejadas como ésta!
(4) El número 15 es un número par.
(5) Esta frase es falsa.
(6) ¿Qué hora es?
(7) Todos los círculos del mismo radio son iguales.
(8) En los números enteros, $11 + 6 \neq 12$.
(9) La tierra es redonda.

0.1.2. Diga si cada una de las siguientes proposiciones acerca de los números enteros es verdadera o falsa.

(1) $(3 + 1 = 4) \vee (2 + 5 = 9)$
(2) $(5 - 1 = 4) \wedge (9 + 12 \neq 7)$
(3) $(3 < 10 = 4) \vee (7 \neq 2)$
(4) $(4 = 11 - 7) \Rightarrow (8 > 0)$
(5) $(4^2 \neq 16) \Rightarrow (4 - 4 = 8)$
(6) $(5 + 2 = 10) \Leftrightarrow (17 + 19 = 36)$
(7) $(6 = 5) \Leftrightarrow (12 \neq 12)$

0.1.3. Comparar las tablas de verdad de $\neg(P \vee Q)$ y $(\neg P) \vee Q$.

0.1.4. Sean P y Q proposiciones tales que $P \Rightarrow Q$ es falsa. Determine los valores de verdad de

(1) $\neg P \vee Q$
(2) $P \wedge Q$
(3) $Q \Rightarrow P$
(4) $\neg Q \Rightarrow \neg P$
(5) $P \Leftrightarrow Q$

0.1.5. Si P y R representan proposiciones verdaderas y Q y S representan proposiciones falsas, encuentre el valor de verdad de las proposiciones compuestas dadas a continuación:

(1) $\neg P \wedge R$
(2) $\neg Q \vee \neg R$
(3) $\neg[\neg P \wedge (\neg Q \vee P)]$
(4) $\neg[(\neg P \wedge \neg Q) \vee \neg Q]$
(5) $(P \wedge R) \vee \neg Q$
(6) $(Q \vee \neg R) \wedge P$
(7) $(\neg P \wedge Q) \vee \neg R$
(8) $\neg(P \wedge Q) \wedge (P \wedge \neg Q)$
(9) $(\neg R \wedge \neg Q) \vee (\neg R \wedge Q)$
(10) $\neg[(\neg P \wedge Q) \vee R]$
(11) $\neg[R \vee (\neg Q \wedge \neg P)]$
(12) $\neg P \Rightarrow \neg Q$
(13) $\neg(P \Rightarrow Q)$
(14) $(P \Rightarrow Q) \Rightarrow R$
(15) $P \Rightarrow (Q \Rightarrow R)$
(16) $[S \Rightarrow (P \wedge \neg R)] \wedge [(P \Rightarrow (R \vee Q)) \wedge S]$

(17) $[(P \wedge \neg Q) \Rightarrow (Q \wedge R)] \Rightarrow (S \vee \neg Q)$

0.1.6.

(*a*) Si la proposición Q es verdadera, determine todas las asignaciones de valores de verdad para las proposiciones P, R y S para que la proposición

$$[Q \Rightarrow ((\neg P \vee R) \wedge \neg S)] \wedge [\neg S \Rightarrow (\neg R \wedge Q)]$$

sea verdadera.
(*b*) Responda la parte (*a*) si Q es falsa.

0.1.7. Sean $P(x)$, $Q(x)$ y $R(x)$ los siguientes predicados.

$P(x) : x \leq 3$.
$Q(x) : x + 1$ es impar.
$R(x) : x > 0$.

Si nuestro conjunto de referencia consta de todos los enteros, ¿cuáles son los valores de verdad de las siguientes proposiciones?

(1) $P(1)$
(2) $Q(1)$
(3) $\neg P(3)$
(4) $Q(6)$
(5) $P(7) \vee Q(7)$
(6) $P(3) \wedge Q(4)$
(7) $P(4)$
(8) $\neg[P(-4) \vee Q(-3)]$
(9) $P(3) \vee [Q(3) \vee \neg R(3)]$
(10) $\neg P(3) \wedge [Q(3) \vee R(3)]$
(11) $P(2) \Rightarrow [Q(2) \Rightarrow R(2)]$
(12) $[P(2) \wedge Q(2)] \Rightarrow R(2)$
(13) $P(0) \Rightarrow [\neg Q(-1) \Leftrightarrow R(1)]$
(14) $[P(-1) \Leftrightarrow Q(-2)] \Leftrightarrow R(-3)$

0.1.8. Sean $P(x)$, $Q(x)$ y $R(x)$ los siguientes predicados.

$P(x) : x^2 - 7x + 10 = 0$.
$Q(x) : x^2 - 2x - 3 = 0$.
$R(x) : x < 0$.

Determine la verdad o falsedad de las siguientes proposiciones, en las que nuestro conjunto de referencia consta de todos los enteros. Si la proposición es falsa dé un contraejemplo o explicación.

(1) $\forall x[P(x) \Rightarrow \neg R(x)]$
(2) $\forall x[Q(x) \Rightarrow R(x)]$
(3) $\exists x[Q(x) \Rightarrow R(x)]$
(4) $\exists x[P(x) \Rightarrow R(x)]$

0.1.9. Determine el valor de verdad de cada una de las siguientes proposiciones. El conjunto de referencia de cada proposición es el conjunto de números reales.

(1) $\forall x(x^2 > x)$
(2) $\exists x(x^2 > x)$
(3) $\forall x(x > 1 \Rightarrow x^2 > x)$
(4) $\exists x(x > 1 \Rightarrow x^2 > x)$
(5) $\forall x(x > 1 \Rightarrow \frac{x}{x^2+1} < \frac{1}{3})$
(6) $\exists x(x > 1 \Rightarrow \frac{x}{x^2+1} < \frac{1}{3})$

0.1.10. Sean P, Q y R proposiciones. Construya una tabla de verdad para cada una de las siguientes proposiciones compuestas. ¿Cuáles de las proposiciones son tautologías?

(1) $\neg P \wedge Q$
(2) $\neg(P \wedge Q)$
(3) $P \Rightarrow P$
(4) $\neg(P \vee \neg Q) \Rightarrow \neg P$
(5) $P \Rightarrow (Q \Rightarrow R)$
(6) $(P \Rightarrow Q) \Rightarrow R$
(7) $(P \Rightarrow Q) \Rightarrow (Q \Rightarrow P)$
(8) $[P \wedge (P \Rightarrow Q)] \Rightarrow Q$
(9) $(P \wedge Q) \Rightarrow P$
(10) $Q \Leftrightarrow (\neg P \vee \neg Q)$
(11) $[(P \Rightarrow Q) \wedge (Q \Rightarrow R)] \Rightarrow (P \Rightarrow R)$

0.1.11. Usando tablas de verdad, compruebe las equivalencias siguientes:

(1) $\neg(\neg P) \Leftrightarrow P$
(2) $P \wedge Q \Leftrightarrow Q \wedge P$
(3) $P \vee Q \Leftrightarrow Q \vee P$
(4) $\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$

(5) $\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$
(6) $(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$
(7) $(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$
(8) $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$
(9) $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$

A las formulas (2) y (3) las llamamos leyes de conmutatividad para los conectivos $\wedge$ y $\vee$. A las fórmulas (4) y (5) las llamamos leyes de De Morgan; a las leyes (6) y (7) leyes de asociatividad para los conectivos $\wedge$ y $\vee$, y a las leyes (8) y (9) las llamamos leyes de distributividad para los conectivos involucrados.

0.1.12. Sean P y Q proposiciones. Se define la disyunción exclusiva $\veebar$ como

$$P \veebar Q : (P \wedge \neg Q) \vee (\neg P \wedge Q)$$

(1) Dé la tabla de verdad para el conectivo $\veebar$.
(2) Determine si las siguientes proposiciones acerca de los números enteros es verdadera o falsa.
(I) $[3 + 1 = 4] \veebar [2 + 5 = 7]$
(II) $[3 + 1 = 4] \veebar [2 + 5 = 9]$
(III) $[3 + 1 = 7] \veebar [2 + 5 = 7]$
(IV) $[3 + 1 = 7] \veebar [2 + 5 = 9]$
(3) Demuestre que $P \veebar Q \Leftrightarrow \neg(P \Leftrightarrow Q)$ es una tautología.

0.1.13. Justifica cada paso de la siguiente demostración directa, que prueba que si x es un número entero, entonces $x \cdot 0 = 0$. Suponga que los siguientes son teoremas previos:

(1) Si a, b y c son numeros enteros, entonces $b + 0 = b$ y $a(b + c) = ab + ac$.
(2) Si a, b y c son numeros enteros tales que $a + b = a + c$, entonces $b = c$.

Demostración. $x \cdot 0 + 0 = x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0$; por lo tanto, $x \cdot 0 = 0$.

Aceptamos que un número entero x es impar a si existe un número entero z tal que $x = 2 \cdot z + 1$.

0.1.14. Dé una demostración directa de las siguientes proposiciones.

(1) Para todos los enteros m y n, si m y n son pares, entonces $m + n$ es par.
(2) Para todos los enteros m y n, si $m + n$ es par, entonces m y n son los dos pares o los dos impares.

En los ejercicios 0.1.1.15 al 0.1.1.17 aceptaremos las propiedades de la suma y el producto de los números enteros (véase teoremas 6.1.3 y 6.1.5).

0.1.15. Dé una demostración por contraposición de cada una de las siguientes proposiciones.

(1) Para todo entero m, si m es par, entonces $m + 7$ es impar.
(2) Para todos los enteros m y n, si mn es impar, entonces m y n son impares.
(3) Para todos los enteros m y n, si $m + n$ es par, entonces m y n son los dos pares o los dos impares.
(4) Para todos los enteros m y n, si $m \cdot n > 25$, entonces $m > 5$ o $n > 5$.

0.1.16. Realice una demostración por reducción al absurdo de la siguiente proposición: para cualquier entero n, si n^2 es impar, entonces n es impar.

0.1.17. Demuestre el siguiente resultado dando una demostración directa, otra por contraposición y otra por reducción al absurdo: Si n es un entero impar, entonces $n + 11$ es par.

0.1.18. Dé una demostración por reducción al absurdo de la siguiente afirmación: si se colocan 100 pelotas en nueve urnas, alguna urna contiene 12 pelotas o más.

0.1.19. Dé una demostración por reducción al absurdo de la siguiente afirmación: si se distribuyen 40 monedas en nueve bolsas de manera que cada bolsa contenga al menos una moneda, al menos dos bolsas contienen el mismo número de monedas.

0.1.20. Sea

$$A = \frac{a_1 + a_2 + \cdots + a_n}{n}$$

el promedio de los números reales $a_1, a_2, \ldots, a_n$. Demuestre por reducción al absurdo, que existe i tal que $a_i \geq A$.

0.1.21. Sea

$$A = \frac{a_1 + a_2 + \cdots + a_n}{n}$$

el promedio de los números reales $a_1, a_2, \ldots, a_n$. Pruebe o desapruebe: existe i tal que $a_i > A$. ¿Qué método de demostración utilizó?

0.1.22. Sea

$$A = \frac{a_1 + a_2 + \cdots + a_n}{n}$$

el promedio de los números reales $a_1, a_2, \ldots, a_n$. Suponga que existe i tal que $a_i < A$. Pruebe o desapruebe: existe j tal que $a_j > A$. ¿Qué método de demostración utilizó?

Definición 0.1.23. *Si x es un número real, se define el valor absoluto de x como* $| x | = x$ *si* $x \geq 0$ *y* $| x | = x$ *si* $x < 0$.

0.1.24. Utilice la demostración por casos para probar que $|xy| = |x||y|$ para todos los números reales x y y.

0.1.25. Demuestre la desigualdad $-|x| \leq x \leq |x|$, donde x es un número entero. Para ello divida la demostración en dos casos: $x \geq 0$ y $x < 0$.

0.1.26. En matemáticas, con frecuencia se debe afirmar no sólo la existencia de un objeto a (ya sea un número, un triángulo, etcétera) que satisfaga un proposición $P(x)$, sino también el hecho de que este objeto a es el único para el que se satisface $p(x)$ es verdadera. Entonces, el objeto es único. Esto se denota con el cuantificador $\exists! x P(x)$, que se lee como "Existe un único x". Este cuantificador puede definirse en términos de los cuantificadores existencial y universal:

$$\exists! x P(x) : [\exists x P(x)] \wedge \left(\forall x \forall y \left[(P(x) \wedge P(y)) \Rightarrow (x = y)\right]\right)$$

Esta definición indica que "una demostración de existencia y unicidad" requiere "una demostración de existencia", que con frecuencia se realiza construyendo un ejemplo que satisfaga $P(x)$, y "una demostración de la unicidad".

(1) Considere la proposición $\exists! x(x^2 = 4)$. Dé un ejemplo de un conjunto de referencia en el que la proposición es verdadera y un ejemplo de otro conjunto de referencia donde la proposición es falsa.

(2) Sea $P(x, y) : y = -2x$, el conjunto de referencia está formado por todos los enteros. Determine cuáles de las proposiciones son verdaderas o falsas.

(I) $[\forall x \exists! y P(x, y)] \Rightarrow [\exists! y \forall x P(x, y)]$

(II) $[\exists! y \forall x P(x, y)] \Rightarrow [\forall x \exists! y P(x, y)]$

La esencia de las matemáticas
reside en su libertad.
George Cantor
1945 - 1918

***Capítulo* 1**

Conjuntos, relaciones y funciones

§ 1.1. Introducción a la teoría de conjuntos

Algunos conceptos de este capítulo serán presentados de manera intuitiva, lo que nos permitirá avanzar rápidamente para poder trabajar y ejercitar las operaciones con conjuntos.

Por un ***conjunto*** entenderemos a una colección de objetos, donde debe quedar totalmente claro cuándo un objeto es miembro del conjunto y cuándo no. A los objetos que forman parte de un conjunto los llamaremos sus ***elementos***. Así pues para dar un conjunto debemos decir quiénes son exactamente todos sus elementos y, así, dado cualquier objeto podamos decidir si es o no un elemento del conjunto. Introduciremos notaciones adecuadas para expresar de una manera más precisa los conceptos y resultados en la teoría de conjuntos.

Para expresar que un objeto es elemento de un conjunto usaremos el símbolo "$\in$". Escribiremos $x \in A$ para expresar que

"*x es elemento de A*" o "*x es miembro de A*" o también
"*x pertenece a A*".

A "$\in$" se le conoce como el símbolo de pertenencia.

De igual manera usaremos $\notin$ para expresar la negación de la pertenencia (la no pertenencia) esto es, escribiremos $x \notin A$ para expresar que

"*x no es elemento de A*" o "*x no es miembro de A*" o también
"*x no pertenece a A*".

Para dar un conjunto debemos expresar de alguna manera quiénes son los elementos que lo determinan y esto lo podemos hacer de alguna de las dos formas siguientes:

1) Dando una lista completa de todos los elementos del conjunto, cuando esto sea posible, lo que generalmente se puede hacer cuando la lista es "pequeña", o cuando dados algunos de sus elementos y usando puntos suspensivos se entiende sin ninguna duda cuáles son los demás elementos.
2) Dando una propiedad (proposición) que resulte verdadera solamente para los elementos del conjunto y que sea falsa para los objetos que no pertenece a él.

Formalicemos e introduzcamos notación adecuada para las dos ideas anteriores. Si 1, 3 y 5 son todos los elementos del conjunto A, escribimos $A = \{1, 3, 5\}$. Para $n \geq 1$, por $a_1, \ldots, a_n$ entenderemos que se tienen objetos $a_1, a_2, a_3, \ldots$ etc. hasta llegar a a_n. Por ejemplo, si $n = 5$, $a_1, \ldots, a_5$ serán a_1, a_2, a_3, a_4 y a_5; si $n = 1$ se tendrá un sólo objeto a_1.
Si $a_1, \ldots, a_n$ son todos los objetos del conjunto A, escribimos

$$A = \{a_1, \ldots, a_n\}$$

y a esta forma de dar un conjunto se le llama ***por extensión***.
En el caso en que los elementos del conjunto A estén descritos por una proposición $p(x)$, escribiremos

$$A = \{x \mid p(x) \text{ es verdadera}\}$$

o simplemente $A = \{x \mid p(x)\}$. Esto significa que un objeto a pertenece al conjunto A si y sólo si $p(a)$ es verdadera. De esta manera, si $p(b)$ es falsa, entonces podemos afirmar que $b \notin A$. Como mencionamos en 1), también podemos describir un conjunto dando algunos de sus elementos y usando puntos suspensivos cuando quede claro quiénes son los demás elementos. Aun cuando en capítulos posteriores introduciremos los sistemas numéricos, $\mathbb{N}$ el conjunto de los números naturales, $\mathbb{Z}$ el conjunto de los números enteros, $\mathbb{Q}$ el conjunto de los números racionales, $\mathbb{R}$ el conjunto de los números reales, suponemos que se conocen de manera intuitiva, la suma y productos en cada uno de ellos y las propiedades básicas, así como el orden usual. Por ejemplo, si $A = \{0, 2, 4, 6, 8, \ldots\}$ los elementos de A serán todos los "números naturales" que son pares. Sin embargo, a este conjunto A también podemos describirlo mediante una proposición $p(x)$, por ejemplo

$$p(x) : \textit{x es un número natural y x es par}$$

es decir,

$$A = \{x \mid x \text{ es un número natural y } x \text{ es par}\}.$$

Ejemplo 1.1.1. El ***conjunto vacío***, denotado por $\varnothing$, es el conjunto que no tiene elementos, es decir, $\varnothing = \{\ \}$. Así que para cualquier objeto arbitrario x se tiene que $x \notin \varnothing$. A este conjunto también podemos describirlo mediante la proposición $p(x) : x \neq x$, ya que para cualquier objeto x, "$x \neq x$" es falsa y así, $\varnothing = \{x \mid x \neq x\}$.

Ejemplo 1.1.2. $A = \{a\}$ es el conjunto que tiene un único elemento que es a y también podemos describirlo como $A = \{x \mid x = a\}$. En este caso estamos usando la proposición $p(x) : x = a$.

Ejemplo 1.1.3. Sea $a \neq b$. $A = \{a, b\}$ es el conjunto cuyos únicos elementos son a y b. Si x es un objeto tal que $x \neq a$ y $x \neq b$, entonces $x \notin A$. También se puede escribir $A = \{x \mid x = a \text{ o } x = b\}$. La proposición que usamos aquí es $p(x) : x = a$ o $x = b$. A este conjunto se le llama ***par no ordenado*** de a y b.

Ejemplo 1.1.4. Se puede describir los elementos de un conjunto, usando proposiciones distintas, por ejemplo

$$A = \{x \mid x \text{ es un número natural y } x + 1 = 2\}$$

o

$$A = \{x \mid x \text{ es un número natural y } 0 < x < 2\}.$$

Estas proposiciones son: $p(x)$: x es un número natural y $x + 1 = 2$, $q(x)$: x es un número natural y $0 < x < 2$.

Hemos dicho que un conjunto queda determinado por sus elementos. Formalicemos:

Definición 1.1.5. *Dos conjuntos A y B son* ***iguales*** *($A = B$) si ambos tienen exactamente los mismos elementos, es decir, $A = B$ si y sólo si son verdaderas las proposiciones*

"si $x \in A$, entonces $x \in B$" y "si $x \in B$, entonces $x \in A$".

Usando conectivos lógicos, la definición de igualdad se expresa:

$$A = B \underset{def.}{\iff} \forall x(x \in A \iff x \in B)$$

Nota 1.1.6. El símbolo $\underset{\boldsymbol{def.}}{\iff}$ significa que se está estableciendo una definición.

Ejemplo 1.1.7. Consideremos una pareja de casados M y H y sea A el conjunto de hijos de M y B el conjunto de hijos de H. No necesariamente $A = B$. A y B serán iguales si los hijos de cada uno de ellos son los mismos que tienen en común. Si por el contrario, al menos uno de ellos ha tenido hijos con otra pareja, entonces $A \neq B$. Este ejemplo nos indica que debemos tener cuidado para decidir cuándo dos conjuntos dados son iguales.

Para mostrar que dos conjuntos dados no son iguales basta exhibir un elemento de alguno de los conjuntos que no sea elemento del otro. Así

$$A \neq B \iff \exists x\,[(x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)]$$

Observación 1.1.8. Es importante mencionar que el orden en que se dan los elementos de un conjunto es irrelevante, es decir, para dar un conjunto basta decir quiénes son sus elementos sin importar el orden en que se dan.

$$\{a, b\} = \{b, a\} \text{ y } \{a, b, c\} = \{a, c, b\} = \{b, c, a\} = \cdots \text{ etc.}$$

Además en el caso en que $a = b$, {a,b}={a,a}={a}.

***Definición 1.1.9**. Dados dos conjuntos A y B, diremos que A es un **subconjunto** de B y lo denotaremos por $\boldsymbol{A \subseteq B}$ (o $\boldsymbol{B \supseteq A}$), si cada elemento de A es también elemento de B.*

$$A \subseteq B \underset{def.}{\iff} \forall x(x \in A \implies x \in B)$$

Evidentemente si $A = B$, entonces $A \subseteq B$, así que en el caso en que $A \subseteq B$ y $A \neq B$, diremos que A es un ***subconjunto propio*** de B y lo denotaremos por $\boldsymbol{A \subsetneq B}$. En el caso de que A no sea subconjunto de B, lo denotaremos por $\boldsymbol{A \not\subseteq B}$.

$$A \not\subseteq B \iff \exists x(x \in A \wedge x \notin B)$$

Para mostrar que $A \not\subseteq B$ es suficiente exhibir un elemento de A que no sea elemento de B, como se muestra en el siguiente

Ejemplo 1.1.10. Sean $A = \{a, b, c, 1\}$, $B = \{1, a\}$ y $C = \{1, 2, 3\}$. $B \subseteq A$ puesto que los elementos de B, que son 1 y a, son también elementos de A. $B \not\subseteq C$ ya que existe un elemento en B, que es a, que no pertenece a C.

Podemos formular la igualdad en términos de subconjuntos.

***Teorema 1.1.11**. Dos conjunto A y B son iguales si y sólo si $A \subseteq B$ y $B \subseteq A$.*

Teorema 1.1.12. *Sean A y B conjuntos arbitrarios. Entonces*

(1) $\varnothing \subseteq A$.

(2) $A \subseteq A$.

(3) Si $A \subseteq B$ *y* $B \subseteq C$, *entonces* $A \subseteq C$.

Demostración. Lo demostraremos por reducción al absurdo (véase (*III*) pág. 10)

(1) Si $\varnothing \not\subseteq A$, entonces deberíamos poder exhibir un elemento en $\varnothing$ que no pertenece a A, lo que evidentemente es imposible ya que $\varnothing$ no tiene elementos. Por lo tanto debe ser $\varnothing \subseteq A$.

(2) Es inmediato.

(3) Sea $x \in A$. Como $A \subseteq B$, entonces $x \in B$ y como $B \subseteq C$, entonces $x \in C$. Por lo tanto $A \subseteq C$. ∎

Observación 1.1.13. $A \neq \varnothing$ significa que A tiene por lo menos un elemento y en este caso se tendrá $\varnothing \subsetneq A$, que es, $\varnothing$ es un subconjunto propio de A.

§ 1.2. Operaciones entre conjuntos

Introduciremos las operaciones básicas que se realizan entre conjuntos, que son la *unión*, la *intersección*, la *diferencia*, la *potencia* y el *producto cartesiano*, lo que nos permitirá construir nuevos conjuntos a partir de dos conjuntos dados. Por otro lado, así como las operaciones de suma y producto en los sistemas numéricos (números naturales, números enteros, etc.) satisfacen ciertas propiedades como por ejemplo la así llamada *ley de asociatividad* para la suma y producto que son:

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

también las operaciones entre conjuntos tienen ciertas propiedades.

Definición 1.2.1. *Sean A y B conjuntos. La* ***unión*** *de A y B es el conjunto*

$$\boldsymbol{A \cup B} = \{x \mid x \in A \; o \; x \in B\}.$$

Según la definición, se tiene entonces que

$$x \in A \cup B \underset{def.}{\Longleftrightarrow} (x \in A \vee x \in B).$$

Luego para que un elemento x pertenezca a $A \cup B$, debe ser verdadera al menos una de las proposiciones "$x \in A$" o "$x \in B$", es decir, es necesario y suficiente que x sea elemento de alguno de los dos conjuntos. Solamente para ilustrar, consideremos A y B subconjuntos de un conjunto X. Entonces

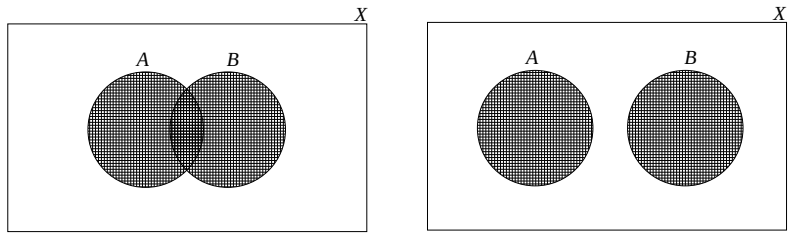


FIGURA 1. La región sombreada ilustra la unión de A y B

Para mostrar que un objeto x no es elemento de $A \cup B$, se debe verificar que "$x \in A$ o $x \in B$" es falsa, lo que es equivalente a que "$x \notin A$ y $x \notin B$" es verdadera. Así tenemos

$$x \notin A \cup B \Longleftrightarrow (x \notin A \wedge x \notin B).$$

Nuevamente para ilustrar, consideremos A y B subconjuntos de un conjunto X. Entonces

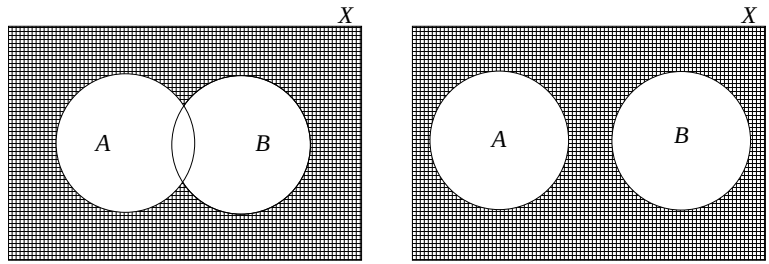


FIGURA 2. La región sombreada ilustra los elementos de X que no pertenecen a la unión de A y B

Ejemplo 1.2.2.
(a) Sean $A = \{a, b\}$ y $B = \{c, 1, 2\}$. Entonces $A \cup B = \{a, b, c, 1, 2\}$.
(b) Sean $A = \{2, 3, 4\}$ y $B = \{1, 2, 3\}$. Entonces $A \cup B = \{1, 2, 3, 4\}$. Por ejemplo $5 \notin A \cup B$ ya que $5 \notin A$ y $5 \notin B$.

Nota 1.2.3. Para demostrar la igualdad $A = B$ de dos conjuntos A y B, hemos visto que esto es equivalente a demostrar $A \subseteq B$ y $A \supseteq B$. Conservando el orden en que aparecen A y B en la igualdad, cuando hagamos la demostración de $A \subseteq B$ o de $A \supseteq B$ lo indicaremos al principio de ésta con los símbolos **⊆)** o **⊇)** respectivamente.

Tratándose de una proposición de la forma $P \Leftrightarrow Q$, haremos lo mismo; $\Longrightarrow)$ significa que se demostrará $P \Rightarrow Q$ y $\Longrightarrow)$ significa que se demostrará $Q \Rightarrow P$.

Las propiedades de la unión son

Teorema 1.2.4. *Sean A, B y C conjuntos. Entonces*

(1) $A \subseteq A \cup B$; $B \subseteq A \cup B$.
(2) $A = A \cup \varnothing$; $A \cup A = A$.
(3) $(A \cup B) \cup C = A \cup (B \cup C)$.
(4) $A \cup B = B \cup A$.
(5) $A \cup B = B$ *si y sólo si* $A \subseteq B$.

Demostración. La demostración de la afirmación (4) la dejaremos como ejercicio (véase ejercicio 1.2.5).

(1) $A \subseteq A \cup B$.
Sea $x \in A$. Luego es verdadera: $x \in A$ o $x \in B$ y por lo tanto $x \in A \cup B$ y así $A \subseteq A \cup B$. La demostración de $B \subseteq A \cup B$ se hace de manera similar.

(2) $A \cup \varnothing = A$.
$\supseteq$) Si $x \in A \cup \varnothing$, por definición se tiene que $x \in A$ o $x \in \varnothing$. Pero $x \in \varnothing$ siempre es falsa, sin importar quién es x, así que se debe tener $x \in A$.
$\subseteq$) Por el inciso (1), tenemos que $A \subseteq A \cup \varnothing$.

(3) $(A \cup B) \cup C = A \cup (B \cup C)$.
$\subseteq$) Si $x \in (A \cup B) \cup C$, entonces $x \in A \cup B$ o $x \in C$. Continuamos la demostración considerando los diferentes casos que se pueden presentar. Si $x \in C$, por el inciso (1), entonces $x \in B \cup C$ y nuevamente por el inciso (1), $x \in A \cup (B \cup C)$. Ahora, si $x \in A \cup B$, entonces $x \in A$ o $x \in B$. En el caso de que $x \in A$, obtenemos $x \in A \cup (B \cup C)$ y en caso de que $x \in B$ obtenemos que $x \in B \cup C$ y de aquí $x \in A \cup (B \cup C)$, aplicando siempre el inciso (1). Finalmente, como en cualquiera de los casos que se pueden presentar llegamos a que $x \in A \cup (B \cup C)$ concluimos que $(A \cup B) \cup C \subseteq A \cup (B \cup C)$.
$\supseteq$) De manera totalmente similar se prueba que $A \cup (B \cup C) \subseteq (A \cup B) \cup C$. Por lo tanto se tiene la igualdad de estos dos conjuntos.

(5) $A \cup B = B$ si y sólo si $A \subseteq B$.
$\Longrightarrow$) Supongamos que $A \cup B = B$. Por el inciso (1), $A \subseteq A \cup B = B$.
$\Longleftarrow$) Supongamos que $A \subseteq B$. Por el inciso (1) $B \subseteq A \cup B$ así que sólo debemos probar que $A \cup B \subseteq B$. Para esto, sea $x \in A \cup B$. Entonces $x \in A$ o $x \in B$. Si

$x \in A$, como por hipótesis $A \subseteq B$, se debe tener $x \in B$. Así que $x \in A$ o $x \in B$ implica, en cualquiera de los dos casos que, $x \in B$, luego $A \cup B \subseteq B$. Entonces $A \cup B = B$.■

La segunda operación que definimos sobre conjuntos es la intersección.

Definición 1.2.5. *Sean A y B conjuntos. La* ***intersección*** *de A y B es el conjunto*

$$\boldsymbol{A \cap B} = \{x \mid x \in A \text{ y } x \in B\}.$$

Usando los conectivos lógicos se tiene que

$$x \in A \cap B \underset{def.}{\iff} (x \in A \wedge x \in B).$$

Según la definición, para que un elemento pertenezca a $A \cap B$, éste debe pertenecer a ambos conjuntos A y B, esto es, la intersección de dos conjuntos consiste de los elementos que son comunes a ambos conjuntos. Para ilustrar la intersección de dos conjuntos consideremos A y B subconjuntos de un conjunto X. Entonces

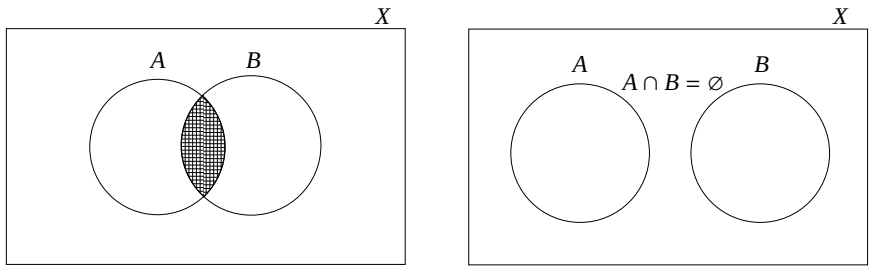


FIGURA 3. La región sombreada ilustra la intersección de A y B

Si los conjuntos A y B no tienen elementos en común, se tendrá pues que $A \cap B = \varnothing$ y en este caso diremos que A y B son ***conjuntos ajenos***.

Veamos ahora qué significa que un objeto x no pertenece a $A \cap B$. Para que un objeto x pertenezca a $A \cap B$, x deberá ser elemento tanto de A como de B, así que basta con que alguna de estas afirmaciones falle para que x no sea elemento de $A \cap B$. Entonces

$$x \notin A \cap B \iff (x \notin A \vee x \notin B).$$

Ejemplo 1.2.6. Sean los conjuntos $A = \{a, b, c, 1, 2, 3, 5\}$ y $B = \{b, d, 1, 2, 3\}$. Entonces $A \cap B = \{b, 1, 2, 3\}$. En este caso a, c, d y 5 no pertenecen a $A \cap B$ por que $a \notin B$, $c \notin B$, $d \notin A$ y $5 \notin B$.

Ejemplo 1.2.7. Sean $A = \{a, b, c\}$ y $B = \{1, 2\}$. Entonces A y B son conjuntos ajenos porque A y B no tienen elementos en común, es decir, $A \cap B = \emptyset$.

Nuevamente para ilustrar, consideremos A y B subconjuntos de X. Entonces

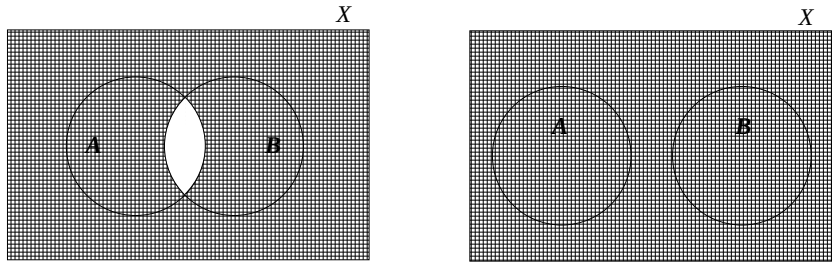


Figura 4. La región sombreada ilustra los elementos de X que no pertenecen a la intersección de A y B

La intersección de conjuntos tiene propiedades muy similares a las de la unión.

Teorema 1.2.8. *Sean A, B y C conjuntos. Entonces*

(1) $A \cap B \subseteq A$; $A \cap B \subseteq B$.
(2) $A \cap \emptyset = \emptyset$; $A \cap A = A$.
(3) $(A \cap B) \cap C = A \cap (B \cap C)$.
(4) $A \cap B = B \cap A$.
(5) $A \cap B = A$ *si y sólo si* $A \subseteq B$.

Demostración. Demostraremos que $A \cap \emptyset = \emptyset$, (3) y (5) y dejamos como ejercicio las otras (véase ejercicio 1.2.6).

(2) Si fuera $A \cap \emptyset \neq \emptyset$, entonces, por definición, existiría un elemento $x \in A \cap \emptyset$, lo que significaría que $x \in \emptyset$ que es un absurdo ya que $\emptyset$ no tiene elementos, por tanto no puede ser $A \cap \emptyset \neq \emptyset$ y así $A \cap \emptyset = \emptyset$.

(3) $(A \cap B) \cap C = A \cap (B \cap C)$.
$\subseteq$) Si $x \in (A \cap B) \cap C$ entonces $x \in A \cap B$ y $x \in C$, lo que implica, por definición, que ($x \in A$ y $x \in B$) y $x \in C$ y como $x \in B$ y $x \in C$, se tiene que $x \in B \cap C$ y ya que también $x \in A$, entonces $x \in A \cap (B \cap C)$.
$\supseteq$) $A \cap (B \cap C) \subseteq (A \cap B) \cap C$ es completamente similar a la demostración anterior.

(5) $A \cap B = A$ si y sólo si $A \subseteq B$.
$\Longrightarrow$) Supongamos $A \cap B = A$. Entonces por el inciso (1) $A = A \cap B \subseteq B$.
$\Longleftarrow$) Supongamos que $A \subseteq B$.
$\subseteq$) $A \cap B \subseteq A$ por el inciso (1).
$\supseteq$) $A \subseteq A \cap B$ puesto que si $x \in A$, entonces $x \in B$ por hipótesis. Luego $x \in A \cap B$. ∎

Otras propiedades de la unión e intersección se dan en el siguiente teorema.

Teorema 1.2.9. *Sean A, B y C conjuntos.*

(1) Si $A \subseteq B$, entonces $A \cup C \subseteq B \cup C$.
(2) Si $A \subseteq B$, entonces $A \cap C \subseteq B \cap C$.
(3) Si $A \subseteq C$ y $B \subseteq C$, entonces $A \cup B \subseteq C$.
(4) Si $C \subseteq A$ y $C \subseteq B$, entonces $C \subseteq A \cap B$.

Demostración. Demostraremos (1) y (3) dejando como ejercicio los demás incisos (véase ejercicio 1.2.7).

(1) Suponemos $A \subseteq B$ y sea $x \in A \cup C$. Entonces $x \in A$ o $x \in C$. Como $x \in A$ implica $x \in B$, se tiene que $x \in B$ o $x \in C$ y por lo tanto $x \in B \cup C$. Luego $A \cup C \subseteq B \cup C$.
(3) Suponemos que $A \subseteq C$ y $B \subseteq C$ y sea $x \in A \cup B$. Entonces $x \in A$ o $x \in B$. En cualquiera de los dos casos, por hipótesis, se tiene que $x \in C$ con lo que concluimos $A \cup B \subseteq C$. ∎

El siguiente resultado muestra cómo interactúan la unión respecto a la intersección y la intersección respecto a la unión, que es, cada una de estas dos operaciones distribuye a la otra.

Teorema 1.2.10. *Sean A, B y C conjuntos. Entonces*

(1) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
(2) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Demostración. Como lo hemos venido haciendo, demostraremos uno de ellos y dejamos como ejercicio la demostración del otro (Ver ejercicio 1.2.8).

(2) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
$\subseteq$) Sea $x \in A \cap (B \cup C)$. Luego $x \in A$ y $x \in B \cup C$. Esto es $x \in A$ y ($x \in B$ o $x \in C$).
a) Si $x \in B$, entonces $x \in A \cap B$, por lo que, por el teorema 1.2.4 (1), $x \in (A \cap B) \cup (A \cap C)$.

b) Si $x \in C$, entonces $x \in A \cap C$, por lo que, por el teorema 1.2.4 (1), $x \in (A \cap B) \cup (A \cap C)$.

Como en ambos casos $x \in (A \cap B) \cup (A \cap C)$, entonces $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

$\supseteq$) Ahora, sea $x \in (A \cap B) \cup (A \cap C)$. Luego $x \in A \cap B$ o $x \in A \cap C$. Si $x \in A \cap B$, entonces $x \in A$ y $x \in B$ y por ser $B \subseteq B \cup C$, se tiene que $x \in B \cup C$ y de aquí $x \in A \cap (B \cup C)$. El caso en que $x \in A \cap C$ es totalmente similar y llegamos también a la conclusión de que $x \in A \cap (B \cup C)$. Por lo tanto $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.

Entonces $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. ∎

En el siguiente teorema se presenta la "*propiedad universal*" de la unión y de la intersección que las caracteriza mediante dos condiciones que deben satisfacer.

Teorema 1.2.11. *Sean A, B y C conjuntos. Entonces*

(1) $C = A \cup B$ si y sólo si C satisface las siguientes dos condiciones
(i) $A \subseteq C$ y $B \subseteq C$.
(ii) Si D es un conjunto tal que $A \subseteq D$ y $B \subseteq D$, entonces $C \subseteq D$.
(2) $C = A \cap B$ si y sólo si C satisface las siguientes dos condiciones
(i) $C \subseteq A$ y $C \subseteq B$.
(ii) Si D es un conjunto tal que $D \subseteq A$ y $D \subseteq B$, entonces $D \subseteq C$.

Demostración.

(1) $\Longrightarrow$) Supongamos que $C = A \cup B$. Entonces
(*i*) $A \subseteq C$ y $B \subseteq C$, por (1) del teorema 1.2.4.
(*ii*) Si D es un conjunto tal que $A \subseteq D$ y $B \subseteq D$, entonces por (3) del teorema 1.2.9, $C = A \cup B \subseteq D$.

$\Longleftarrow$) Supongamos que C es un conjunto que satisface
(*i*) $A \subseteq C$ y $B \subseteq C$,
(*ii*) Si D es un conjunto tal que $A \subseteq D$ y $B \subseteq D$, entonces $C \subseteq D$.

Demostraremos que $C = A \cup B$ mostrando que cada uno de los conjuntos es subconjunto del otro.

$\supseteq$) Por la hipótesis (*i*) $A \subseteq C$ y $B \subseteq C$. Entonces, por (3) del teorema 1.2.9, $A \cup B \subseteq C$.

$\subseteq$) Como $A \cup B$ es un conjunto que satisface $A \subseteq A \cup B$ y $B \subseteq A \cup B$ ((1) del teorema 1.2.4), entonces, por (*ii*) de la hipótesis, $C \subseteq A \cup B$.

Por lo tanto $C = A \cup B$.

La técnica para la demostración del inciso (2) es similar a la utilizada anteriormente, así que dejamos ésta como ejercicio (véase ejercicio 1.2.9). ■

En el caso de que $A \cap B = \varnothing$ se dice que la unión de A y B es una unión ajena y se denota por $\dot{\cup}$.
Otra de las operaciones básicas es la *diferencia de conjuntos*.

Definición 1.2.12*. Sean A y B conjuntos. La* ***diferencia*** *de A y B es el conjunto*

$$\boldsymbol{A - B} = \{x \mid x \in A \text{ y } x \notin B\}.$$

Expresemos, usando conectivos lógicos, cuándo un objeto es elemento de $A - B$.

$$x \in A - B \underset{def.}{\Longleftrightarrow} (x \in A \wedge x \notin B).$$

Para ilustrar la diferencia de dos conjuntos consideremos A y B subconjuntos de un conjunto X. Entonces

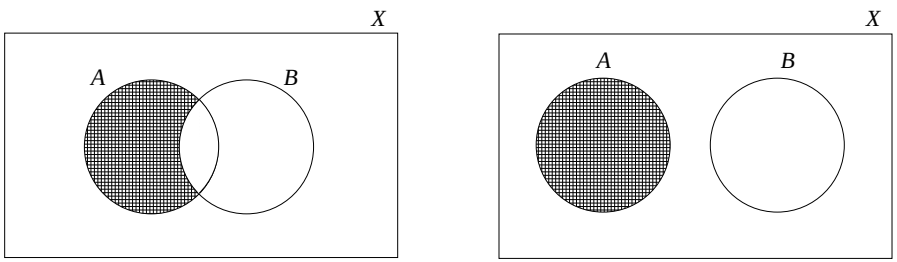


Figura 5. La región sombreada muestra la diferencia de A y B

Para mostrar que un objeto no pertenece a $A - B$, de la definición, basta ver que $x \notin A$ o $x \in B$, es decir,

$$x \notin A - B \Longleftrightarrow (x \notin A \vee x \in B).$$

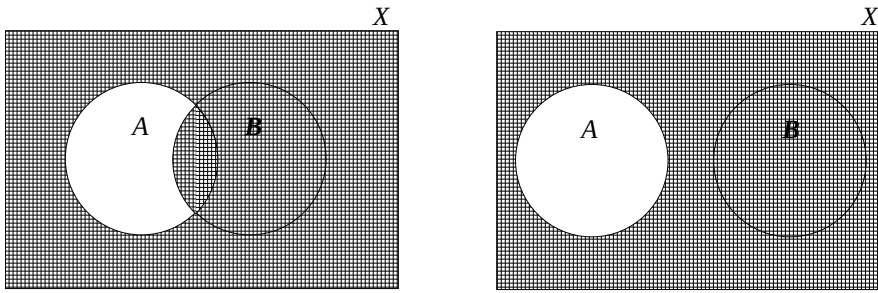


Figura 6. La región sombreada ilustra los elementos de X que no pertenecen a la diferencia de A y B

Ejemplo 1.2.13. Sean $A = \{a, 1, c, 3, 5\}$ y $B = \{b, c, 2, 3\}$. Entonces $A - B = \{a, 1, 5\}$ y $B - A = \{b, 2\}$.

Ejemplo 1.2.14. Sea $\mathbb{N}$ el conjunto de todos los números naturales y

$$B = \{x \in \mathbb{N} \mid x \text{ es un número par}\}.$$

Teniendo en cuenta que un número natural es par o impar pero no ambos,

$$\mathbb{N} - B = \{x \in \mathbb{N} \mid x \text{ no es un número par}\} = \{x \mid x \in \mathbb{N} \text{ y } x \text{ es un número impar}\}$$

y

$$\begin{aligned} B - \mathbb{N} &= \{x \in B \mid x \notin \mathbb{N}\} \\ &= \{x \in \mathbb{N} \mid x \text{ es un número par y } x \notin \mathbb{N}\} \\ &= \varnothing. \end{aligned}$$

Queda claro de estos ejemplos que la diferencia no es una operación conmutativa, es decir, en general $A - B \neq B - A$. Es más $(A - B) \cap (B - A) = \varnothing$.

***Proposición 1.2.15**. Sean A y B conjuntos. Entonces*

(1) $A - A = \varnothing$; $A - \varnothing = A$.
(2) $A - B \subseteq A$.
(3) $(A - B) \cap B = \varnothing$.
(4) $A - B = A$ *si y sólo si* $A \cap B = \varnothing$.

Demostración. Demostraremos (3) y (4), dejando como ejercicio la demostración de (1) y (2) (véase ejercicio 1.2.10).

(3) Si hubiese un elemento $x \in (A - B) \cap B$, entonces $x \in A - B$ y $x \in B$. Pero eso significa que $x \notin B$ y $x \in B$, lo cual es imposible. Por lo tanto $(A - B) \cap B = \varnothing$.
(4) $A - B = A$ si y sólo si $A \cap B = \varnothing$.
$\Longrightarrow$) Supongamos que $A - B = A$. Entonces $A \cap B = (A - B) \cap B = \varnothing$, donde la última igualdad es por el inciso (3).

$\Longleftarrow$) Supongamos que $A \cap B = \varnothing$. Por el inciso (2) $A - B \subseteq A$, así que basta demostrar que $A \subseteq A - B$ para tener la igualdad. Si $x \in A$, entonces, por ser $A \cap B = \varnothing$, se debe tener que $x \notin B$ y por consiguiente $x \in A - B$. Luego $(A - B) = A$. ∎

Observación 1.2.16. Como $(A - B) \cap B = \varnothing$ y $B - A \subseteq B$, entonces $(A - B) \cap (B - A) = \varnothing$.

La diferencia de conjuntos tampoco es asociativa como es muestra el siguiente ejemplo.

Ejemplo 1.2.17. Consideremos $A = \{a, b, 1, 2, 7, 9\}$, $B = \{a, 2, 3, 4, 5\}$ y $C = \{b, 1, 4, 7, 10\}$. Como $A - B = \{b, 1, 7, 9\}$, $B - C = \{a, 2, 3, 5\}$, entonces $(A - B) - C = \{9\}$ y $A - (B - C) = \{b, 1, 7, 9\}$. Por lo tanto $(A - B) - C \neq A - (B - C)$.

Aún cuando la diferencia no distribuye a la unión ni a la intersección, sí satisface las siguientes propiedades conocidas como las ***leyes de De Morgan***.

Teorema 1.2.18 *(Leyes de De Morgan). Sean A, B y C conjuntos. Entonces*

(1) $A - (B \cup C) = (A - B) \cap (A - C)$.
(2) $A - (B \cap C) = (A - B) \cup (A - C)$.

Demostración. Como lo hemos venido haciendo, demostramos uno de los dos incisos y dejamos como ejercicio el otro (véase ejercicio 1.2.11).

(1) $A - (B \cup C) = (A - B) \cap (A - C)$.
$\subseteq$) $A - (B \cup C) \subseteq (A - B) \cap (A - C)$.
Sea $x \in A - (B \cup C)$. Entonces $x \in A$ y $x \notin B \cup C$. Pero $x \notin B \cup C$ implica que $x \notin B$ y $x \notin C$. Por lo tanto $x \in A$, $x \notin B$ y $x \notin C$, por lo que $x \in A - B$ y $x \in A - C$ y así $x \in (A - B) \cap (A - C)$.
$\supseteq$) $(A - B) \cap (A - C) \subseteq A - (B \cup C)$.
Sea $x \in (A - B) \cap (A - C)$. Entonces $x \in A - B$ y $x \in A - C$ lo que significa que $x \in A$ y $x \notin B$ y $x \in A$ y $x \notin C$, que es, $x \in A$ y $x \notin B$ y $x \notin C$. Como $x \notin B$ y

$x \notin C$ implica que $x \notin B \cup C$, entonces tenemos que $x \in A$ y $x \notin B \cup C$. Por lo tanto $x \in A - (B \cup C)$.∎

Como veremos al final de este capítulo (Sección 1.8) no existe un "conjunto universal" que tenga como elementos a todos los conjuntos. Sin embargo, en matemáticas es usual que se trabaje con conjuntos que son subconjuntos de un conjunto fijo $\boldsymbol{X}$ dado de antemano. En este caso se define el ***complemento de un conjunto A en X*** (recordemos que estamos considerando $A \subseteq X$) como la diferencia $X - A$ y la cual denotamos por $\boldsymbol{A^c}$, es decir, $\boldsymbol{A^c = X - A}$. Lo que estamos haciendo es, en estos casos, simplificar la notación lo cual tiene sus ventajas ya que ciertas propiedades se recuerdan con mayor facilidad, por ejemplo, las leyes de De Morgan:

$$(A \cup B)^c = A^c \cap B^c \quad \text{y} \quad (A \cap B)^c = A^c \cup B^c.$$

Se dan respectivamente, el complemento en X de la unión de A y B es igual a la intersección de los complementos en X de A y de B, y el complemento en X de la intersección de A y B es igual a la unión de los complementos en X de A y B. Cuando quede claro del contexto se puede omitir "en X".

Es importante hacer hincapié en que cuando hablemos del complemento de un conjunto A, debe quedar bien claro con respecto a qué conjunto X estamos considerando este complemento.

Antes de pasar a la última operación, que es el producto cartesiano, introducimos el *conjunto potencia* de un conjunto X, también llamado *partes de X*.

Definición 1.2.19*. Dado un conjunto X, el* ***conjunto potencia*** *de X, también llamado* ***partes de X****, es el conjunto*

$$\boldsymbol{\mathscr{P}(X)} = \{A \mid A \subseteq X\}.$$

Nótese que todos los elementos de $\mathscr{P}(X)$ son conjuntos.

Ejemplo 1.2.20. $\mathscr{P}(\varnothing) = \{\varnothing\}$.

Ejemplo 1.2.21. Si $X = \{a\}$, $\mathscr{P}(X) = \{\varnothing, \{a\}\} = \{\varnothing, X\}$.

Ejemplo 1.2.22. Sea $X = \{\varnothing, a, b\}$.

$$\mathscr{P}(X) = \{\varnothing, \{\varnothing\}, \{a\}, \{b\}, \{\varnothing, a\}, \{\varnothing, b\}, \{a, b\}, X\}.$$

Como para cada conjunto X, $\varnothing \subseteq X$, entonces $\mathscr{P}(X) \neq \varnothing$ para todo conjunto X y en el caso en que $X \neq \varnothing$, $\mathscr{P}(X)$ tendrá por lo menos dos elementos que son $\varnothing$ y X.

Un concepto importante en la Teoría de Conjuntos es el de *pareja ordenada* que consiste de una pareja de objetos de los cuales debe quedar claro quién va en primer lugar y quién en segundo. Se denotará a la pareja ordenada de los objetos a y b por $\mathbf{(a, b)}$ y se deberá definir de tal manera que se satisfaga:

$$(a, b) = (c, d) \text{ si y sólo si } a = c \text{ y } b = d. \qquad (*)$$

Durante varios años se buscó una definición conjuntista (es decir, definida como un conjunto) de par ordenado, con el único propósito de que se verificara $(*)$, quedando así incluido este concepto en la Teoría de Conjuntos. Alrededor de los años 30's del siglo XX, Kuratowski y Winner introdujeron la definición conjuntista de par ordenado.

Definición 1.2.23. *El* ***par ordenado*** *de a y b es el conjunto*

$$\mathbf{(a, b)} = \{\{a\}, \{a, b\}\}.$$

Ejemplo 1.2.24. $(a, a) = \{\{a\}, \{a, a\}\} = \{\{a\}, \{a\}\} = \{\{a\}\}$.

Ejemplo 1.2.25. Si $a \neq b$, entonces $(a, b) \neq (b, a)$. Por ejemplo $(1, 2) = \{\{1\}, \{1, 2\}\}$ y $(2, 1) = \{\{2\}, \{2, 1\}\}$

Veamos que con esta definición se satisface $(*)$.

Teorema 1.2.26. *$(a, b) = (c, d)$ si y sólo si $a = c$ y $b = d$.*

Demostración.
$\Longrightarrow$) Supongamos que $(a, b) = (c, d)$ y consideremos por separado los dos casos posibles $a = b$ o $a \neq b$.

(i) $a = b$.
$(a, b) = \{\{a\}, \{a, b\}\} = \{\{a\}\} = \{\{c\}, \{c, d\}\}$. Como $\{\{a\}\}$ tiene un único elemento, entonces $\{\{c\}, \{c, d\}\}$ debe tener un único elemento, lo que significa que debe ser $\{c\} = \{c, d\}$ y nuevamente, como $\{c\}$ tiene un único elemento, entonces $\{c, d\}$ tiene un único elemento y por lo tanto se debe tener $c = d$. Entonces $\{\{a\}\} = \{\{c\}\}$ implica $\{a\} = \{c\}$ que a su vez implica $a = c$. En este caso se tiene entonces que $a = b = c = d$.

(ii) $a \neq b$.
Como $\{a, b\} \in (a, b)$ y $(a, b) = (c, d)$ por hipótesis, entonces $\{a, b\} \in (c, d)$, por lo que $\{a, b\} = \{c\}$ o $\{a, b\} = \{c, d\}$. El primer caso no puede suceder por que eso implicaría que $a = b$, que no es el caso. Entonces

$\{a, b\} = \{c, d\}$, lo que implica forzosamente que $c \neq d$, pues en caso contrario se llegaría nuevamente a que $a = b$. Por otro lado como $\{a\} \in \{\{c\}, \{c, d\}\}$, entonces $\{a\} = \{c\}$, pues ya hemos visto que $c \neq d$. Por lo tanto $a = c$. Por último, ya que $\{a, b\} = \{c, d\}$, $a \neq b$ y $a = c$, entonces $b = d$.

$\Longleftarrow$) Es inmediato. ∎

Habiendo definido el par ordenado, estamos ahora en condiciones para definir el producto cartesiano de dos conjuntos.

Definición 1.2.27. *Sea A y B conjuntos. El* ***producto cartesiano*** *de A y B denotado por $A \times B$ es el conjunto*

$$\boldsymbol{A \times B} = \{(a, b) \mid a \in A \text{ y } b \in B\}.$$

Dada una pareja ordenada (a, b), para que sea elemento de $A \times B$, se debe tener, por definición, que $a \in A$ y $b \in B$, es decir,

$$(a, b) \in A \times B \underset{def.}{\Longleftrightarrow} (a \in A \wedge b \in B).$$

Si una pareja (c, d) no pertenece a $A \times B$ significa que no se cumple al mismo tiempo las dos propiedades "$c \in A$" y "$d \in B$", lo que significa que se debe tener que $c \notin A$ o $d \notin B$. Entonces

$$(c, d) \notin A \times B \Longleftrightarrow (c \notin A \vee d \notin B).$$

Ejemplo 1.2.28. Si $A = \emptyset$ o $B = \emptyset$, entonces $A \times B = \emptyset$.

Ejemplo 1.2.29. Si $A \neq \emptyset$ y $B \neq \emptyset$, entonces $A \times B \neq \emptyset$. Como $A \neq \emptyset$ y $B \neq \emptyset$, entonces existen elementos a y b tales que $a \in A$ y $b \in B$, y por lo tanto $(a, b) \in A \times B$, lo que muestra que $A \times B \neq \emptyset$.

Ejemplo 1.2.30. Si $A = \{a, b\}$ y $B = \{1, a\}$, entonces

$$A \times B = \{(a, 1), (b, 1), (a, a), (b, a)\} \text{ y } B \times A = \{(1, a), (1, b), (a, a), (a, b)\}.$$

Teorema 1.2.31. *Sean A, B, C y D conjuntos no vacíos tales que $A \times B = C \times D$. Entonces $A = C$ y $B = D$.*

Demostración. Sean $a \in A$ y $b \in B$ arbitrarios. Entonces $(a, b) \in A \times B$ y como $A \times B = C \times D$, entonces $(a, b) \in C \times D$ lo que significa que $a \in C$ y $b \in D$. Luego $A \subseteq C$ y $B \subseteq D$. De manera análoga se demuestra que $C \subseteq A$ y $D \subseteq B$. Y con esto se tiene que $A = C$ y $B = D$. ∎

Es claro que si $A \neq B$ y ambos son no vacíos, entonces $A \times B \neq B \times A$.

Nota 1.2.32. Es importante la hipótesis de que cada conjunto debe ser no vacío pues puede tenerse por ejemplo $A = \emptyset$, $B \neq \emptyset$, $C \neq \emptyset$, $D = \emptyset$ y en este caso evidentemente $A \neq C$ y $B \neq D$ y sin embargo $A \times B = \emptyset = C \times D$.

Como lo muestra el siguiente teorema, el producto cartesiano distribuye a la unión, intersección y diferencia de conjuntos.

Teorema 1.2.33. *Sean A, B y C conjuntos. Entonces*

(1) $A \times (B \cup C) = (A \times B) \cup (A \times C)$; $(A \cup B) \times C = (A \times C) \cup (B \times C)$,
(2) $A \times (B \cap C) = (A \times B) \cap (A \times C)$; $(A \cap B) \times C = (A \times C) \cap (B \times C)$,
(3) $A \times (B - C) = (A \times B) - (A \times C)$; $(A - B) \times C = (A \times C) - (B \times C)$.

Demostración.

(1) $A \times (B \cup C) = (A \times B) \cup (A \times C)$.
$\subseteq$) Sea $(a, b) \in A \times (B \cup C)$. Entonces $a \in A$ y $b \in B \cup C$, que es, $a \in A$ y ($b \in B$ o $b \in C$).
(i) Si $b \in B$, entonces $(a, b) \in A \times B$ y así $(a, b) \in (A \times B) \cup (A \times C)$.
(ii) Si $b \in C$, entonces $(a, b) \in A \times C$, por lo que $(a, b) \in (A \times B) \cup (A \times C)$.
En ambos casos $(a, b) \in (A \times B) \cup (A \times C)$.
$\supseteq$) Si $(a, b) \in (A \times B) \cup (A \times C)$, entonces $(a, b) \in (A \times B)$ o $(a, b) \in (A \times C)$.
(i) Si $(a, b) \in (A \times B)$, entonces $a \in A$ y $b \in B$ y de aquí $a \in A$ y $b \in B \cup C$, por lo que $(a, b) \in A \times (B \cup C)$.
(ii) Si $(a, b) \in (A \times C)$, entonces $a \in A$ y $b \in C$, lo que implica que $a \in A$ y $b \in B \cup C$, y así $(a, b) \in A \times (B \cup C)$. En ambos casos llegamos a que $(a, b) \in A \times (B \cup C)$.

(2) $(A \cap B) \times C = (A \times C) \cap (B \times C)$.
$\subseteq$) Sea $(a, b) \in (A \cap B) \times C$. Entonces $a \in A \cap B$ y $b \in C$, y esto implica que ($a \in A$ y $a \in B$) y $b \in C$. Por lo tanto $(a, b) \in A \times C$ y $(a, b) \in B \times C$ y así $(a, b) \in (A \times C) \cap (B \times C)$.
$\supseteq$) Sea $(a, b) \in (A \times C) \cap (B \times C)$. Entonces $(a, b) \in (A \times C)$ y $(a, b) \in (B \times C)$ lo que implica ($a \in A$ y $b \in C$) y ($a \in B$ y $b \in C$). Por lo tanto $a \in A \cap B$ y $b \in C$ y así $(a, b) \in (A \cap B) \times C$.

(4) $A \times (B - C) = (A \times B) - (A \times C)$.

$\subseteq$) Sea $(a,b) \in A \times (B - C)$. Entonces $a \in A$ y $b \in B - C$, lo que implica que $a \in A$ y ($b \in B$ y $b \notin C$), así que $(a,b) \in A \times B$ y $(a,b) \notin A \times C$. Por lo tanto $(a,b) \in (A \times B) - (A \times C)$.

$\supseteq$) Sea $(a,b) \in (A \times B) - (A \times C)$. Entonces $(a,b) \in A \times B$ y $(a,b) \notin A \times C$ lo que implica que: ($a \in A$ y $b \in B$) y ($a \notin A$ o $b \notin C$). Como $a \in A$, la afirmación $a \notin A$ o $b \notin C$ implica que debe ser $b \notin C$. Por lo tanto $a \in A$ y $b \in B$ y $b \notin C$, que es, $a \in A$ y $b \in B - C$ y así $(a,b) \in A \times (B - C)$.

Las demostraciones que faltan no son complicadas y se dejan como ejercicio (véase ejercicio 1.2.38). ∎

Es importante mencionar que en el caso del producto cartesiano, éste no es conmutativo ni asociativo. De la conmutatividad ya hemos mencionado que si $A \neq B$ y ambos A y B son no vacíos, entonces $A \times B \neq B \times A$. Sobre la asociatividad, que no se cumple para el producto cartesiano, la razón es que la naturaleza de los elementos de $(A \times B) \times C$ es distinta a la de los elementos de $A \times (B \times C)$ como lo muestra el ejemplo 1.2.34. Sin embargo hay una identificación muy clara entre los elementos de $(A \times B) \times C$ y los elementos de $A \times (B \times C)$ que es, a $((a,b),c)$ se le identifica de manera natural con $(a,(b,c))$.

Ejemplo 1.2.34. Consideremos los conjuntos $A = \{a\}$, $B = \{1,2\}$ y $C = \{3\}$ y sean $A \times B = \{(a,1),(a,2)\}$ y $B \times C = \{(1,3),(2,3)\}$. Entonces

$$(A \times B) \times C = \{((a,1),3),((a,2),3)\} \text{ y } A \times (B \times C) = \{(a,(1,3)),(a,(2,3))\}.$$

§ 1.3. Relaciones binarias

En esta sección introduciremos el concepto de relación entre dos conjuntos (*relación binaria*) y como podrá apreciar el lector, siendo tan general la definición de relación, en realidad estamos interesados en cierto tipo de ellas que aparecen con mucha frecuencia en matemáticas, siendo éstas las *relaciones de orden*, las *relaciones de equivalencia* y las *funciones*.

***Definición 1.3.1**. Sean X y Y conjuntos. Una **relación R de X en Y** es una pareja ordenada $(R, X \times Y)$, donde $R \subseteq X \times Y$. Si R es una relación de X en Y y $(x,y) \in R$, diremos que **x está relacionado con y**.*

Si R es una relación de X en Y y $(a,b) \in R$, diremos que a está relacionado con b respecto a R.

Para dar una relación son tres datos los que debemos presentar: el conjunto X, el conjunto Y y el subconjunto R de $X \times Y$.

Teorema 1.3.2. *Sean X, Y, X' y Y' conjuntos no vacíos. Las relaciones R de X en Y y R' de X' en Y' son iguales si y sólo si $X = X'$, $Y = Y'$ y $R = R'$.*

La demostración es sencilla y se deja como ejercicio. (ejercicio 1.3.1)
De la definición se ve que hay tantas relaciones de X en Y como subconjuntos tiene $X \times Y$. Como $\varnothing$ siempre es un subconjunto de $X \times Y$ sin importar quienes sean X y Y, a esta relación la llamamos **relación vacía**. En particular si $X = \varnothing$ o $Y = \varnothing$, entonces existe una única relación de X en Y que es la relación vacía.

Definición 1.3.3. *Sea R una relación de X en Y ($R \subseteq X \times Y$).*

(1) El ***dominio*** *de R, $Dom(R)$, es el conjunto*

$$Dom(R) = \{x \in X \mid \text{existe } y \in Y \text{ tal que } (x, y) \in R\}.$$

(2) La ***imágen*** *o* ***rango*** *de R, $Im(R)$, es el conjunto*

$$Im(R) = \{y \in Y \mid \text{existe } x \in X \text{ tal que } (x, y) \in R\}.$$

Ejemplo 1.3.4. Considérese los conjuntos $X = \{a, b, c, d, e\}$, $Y = \{2, 5, 7, 9, 10\}$ y

$$R = \{(a, 2), (a, 5), (b, 2), (d, 9), (d, 10), (e, 7)\}.$$

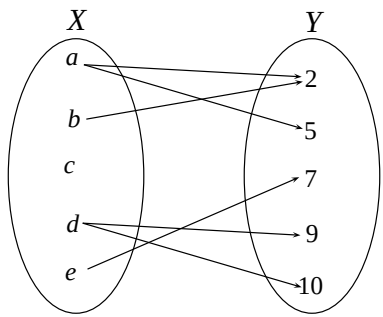


FIGURA 7. Representación de la relación $R = \{(a, 2), (a, 5), (b, 2), (d, 9), (d, 10), (e, 7)\}$

Entonces con respecto a la relación R

(1) a está relacionado con 2 y con 5.
(2) b está relacionado con 2.
(3) d está relacionado con 9 y con 10.
(4) e está relacionado con 7.

(5) c no está relacionado con nadie.

Es claro que entonces $Dom(R) = \{a, b, d, e\}$ y que $Im(R) = \{2, 5, 7, 9, 10\}$.

Así pues, dada una relación de X en Y quedan automáticamente determinados dos subconjuntos, uno de X y uno de Y, que son $Dom(R)$ e $Im(R)$ respectivamente.

Ejemplo 1.3.5. Para cualesquiera conjuntos X y Y si R es la relación vacía, entonces
$Dom(R) = \emptyset$ e $Im(R) = \emptyset$.

Ejemplo 1.3.6. Sean $X = \{a, b, c\}$, $Y = \{1, 2, 3, 4\}$ y $R = \{(a, 1), (a, 2), (c, 4)\}$. Entonces $Dom(R) = \{a, c\}$ e $Im(R) = \{1, 2, 4\}$.

Ejemplo 1.3.7. Sea X cualquier conjunto. $\Delta_X = \{(x, x) \mid x \in X\}$ es una relación de X en X en la que $Dom(\Delta_X) = X$ y $Im((\Delta_X)) = X$. A Δ_X se le llama la diagonal de X.

***Definición 1.3.8**. Dada una relación R de X en Y, la **relación inversa** de R es la relación, R^{-1}, de Y en X dada por*

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

Se tiene entonces que $Dom(R^{-1}) = Im(R)$ e $Im(R^{-1}) = Dom(R)$.

Ejemplo 1.3.9. Sea X cualquier conjunto y $\mathscr{P}(X)$ el conjunto potencia de X. Sea R la relación de X a $\mathscr{P}(X)$ definida por $R = \{(x, y) \in X \times \mathscr{P}(X) \mid x \in y\}$. Entonces $Dom(R) = X$, $Im(R) = \{y \in \mathscr{P}(X) \mid y \neq \emptyset\}$, $R^{-1} = \{(y, x) \mid x \in y\}$. Si $X = \emptyset$ se puede verificar sin ningún problema que en este caso $R = \emptyset$, $Dom(R) = \emptyset$, $Im(R) = \emptyset$ y $R^{-1} = \emptyset$.
En particular si $X = \{1, 2, 3\}$ se tiene entonces que según la relación R

(1) 1 está relacionado con $\{1\}$, $\{1, 2\}$, $\{1, 3\}$ y $\{1, 2, 3\}$.
(2) 2 está relacionado con $\{2\}$, $\{1, 2\}$, $\{2, 3\}$ y $\{1, 2, 3\}$.
(3) 3 está relacionado con $\{3\}$, $\{1, 3\}$, $\{2, 3\}$ y $\{1, 2, 3\}$.

Ahora, según la relación R^{-1} se tiene

(1) $\{1\}$, $\{1, 2\}$, $\{1, 3\}$ y $\{1, 2, 3\}$ están relacionados con 1.
(2) $\{2\}$, $\{1, 2\}$, $\{2, 3\}$ y $\{1, 2, 3\}$ están relacionados con 2.
(3) $\{3\}$, $\{1, 3\}$, $\{2, 3\}$ y $\{1, 2, 3\}$ están relacionados con 3.

Ejemplo 1.3.10. La relación Δ_X definida en el ejemplo 1.3.7 es igual a su relación inversa Δ_X^{-1}.

Definición 1.3.11. *Sea R una relación de X en Y, $A \subseteq X$ y $B \subseteq Y$. La* ***imagen*** *de A bajo la relación de R y la* ***imagen inversa*** *de B bajo R son, respectivamente, los conjuntos*

$$\boldsymbol{R[A]} = \{y \in Y \mid \textit{existe } x \in A \textit{ tal que } (x,y) \in R\}.$$

$$\boldsymbol{R^{-1}[B]} = \{x \in X \mid \textit{existe } y \in B \textit{ tal que } (x,y) \in R\}.$$

Ejemplo 1.3.12. Sean $X = \{a, b, c, d, e\}$, $Y = \{e, f, g, h, i, j\}$ y

$$R = \{(a, j), (a, g), (c, h), (e, e)\}.$$

Entonces $Dom(R) = \{a, c, e\}$ y que $Im(R) = \{j, g, h, e\}$.
Si $A_1 = \{a, d\}$, $A_2 = \{b, c, d\}$, $A_3 = \{b, d\}$, entonces $R[A_1] = \{j, g\}$, $R[A_2] = \{h\}$ y $R[A_3] = \emptyset$.
Si $B_1 = \{e, f, g\}$, $B_2 = \{g, j\}$, $B_3 = \{f, i\}$, entonces $R^{-1}[B_1] = \{e, a\}$, $R^{-1}[B_2] = \{a\}$ y $R^{-1}[B_3] = \emptyset$.

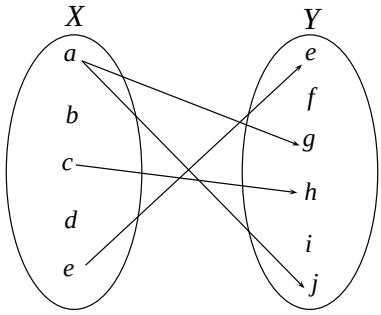


FIGURA 8. Ilustración de la relación $R = \{(a, j), (a, g), (c, h), (e, e)\}$

Algunas relaciones se pueden "componer" de la siguiente manera:

Definición 1.3.13. *Sean R_1 y R_2 relaciones de X en Y y de Y en Z respectivamente. La* ***composición de R_1 con R_2****, denotada por* $\boldsymbol{R_2 \circ R_1}$*, es la relación de X en Z dada por*

$$\boldsymbol{R_2 \circ R_1} = \{(x,z) \mid \textit{existe } y \in Y \textit{ tal que } (x,y) \in R_1 \textit{ y } (y,z) \in R_2\}$$

Ejemplo 1.3.14. Consideremos los conjuntos $X = \{a, b, c, d, e\}$, $Y = \{a, c, d\}$ y $Z = \{a, b, c, d, f, g\}$ y las relaciones $R = \{(a, a), (a, c), (a, d), (b, c), (d, c), (e, d)\}$ y

$S = \{(a, a), (a, c), (d, f)\}$ de X en Y y de Y en Z respectivamente. Entonces se tiene que $S \circ R = \{(a, a), (a, c), (a, f), (e, f)\}$.

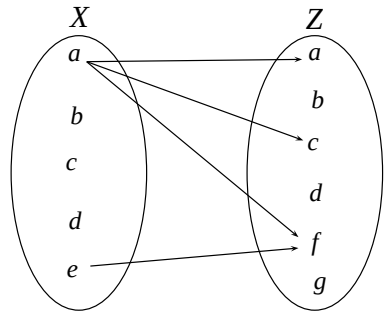


Figura 9. Ilustración de la relación $S \circ R$

Ejemplo 1.3.15. Sean $X = \{a, b, c, d, e\}$, $Y = \{1, 3, 5, 7\}$ y $Z = \{\alpha, \beta, \gamma, \delta, \epsilon\}$ conjuntos; $R = \{(a, 1), (a, 3), (d, 7), (e, 7)\}$ y $S = \{(5, \alpha), (5, \beta), (5, \gamma)\}$ relaciones de X en Y y de Y en Z respectivamente.

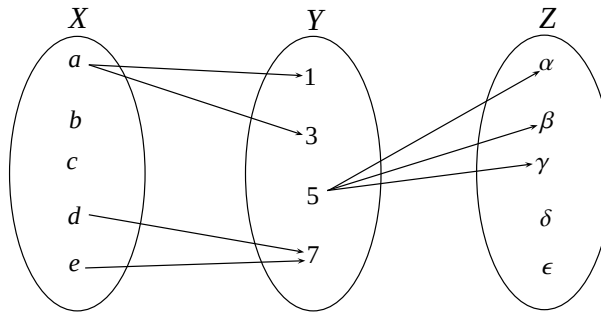


Figura 10. Ilustración de la relación $S \circ R$

Entonces $S \circ R = \varnothing$.

Ejemplo 1.3.16. Sean X y Y conjuntos. Para cada relación R de X en Y se tiene que
$R \circ \Delta_X = R$ y $\Delta_Y \circ R = R$.

Ejemplo 1.3.17. Sean $X = \{a, b, c, d\}$, $Y = \{0, 1\}$ y $Z = \{a, 0, 2\}$, R_1 la relación de X en Y dada por $R_1 = \{(a, 1), (b, 1), (d, 0)\}$ y R_2 la relación de Y en Z dada por $R_2 = \{(1, 0), (1, 2)\}$. Entonces $R_2 \circ R_1 = \{(a, 0), (a, 2), (b, 0), (b, 2)\}$.

Ejemplo 1.3.18. Sean X un conjunto y R_1 la relación de X en $\mathscr{P}(X)$ con regla de correspondencia $R_1 = \{(x, y) \mid x \in y\}$ y R_2 la relación de $\mathscr{P}(X)$ en $\mathscr{P}(\mathscr{P}(X))$ dada por $R_2 = \{(z, w) \mid w = \{z\}\}$.

$$R_2 \circ R_1 = \left\{(x, z) \mid \text{existe } y \in \mathscr{P}(X) \text{ tal que } x \in y \text{ y } z = \{y\}\right\}.$$

§ 1.4. Funciones

Una *función* es una relación binaria sujeta a ciertas condiciones y es uno de los conceptos más importantes en la matemática. Las funciones nos permiten conocer propiedades de conjuntos a través de otros. Un primer ejemplo de esto es la identificación de los elementos de $(A \times B) \times C$ con los de $A \times (B \times C)$ mencionada en la página 37.

Definición 1.4.1. *Sean X y Y conjuntos. Una* **función** *de X en Y es una relación f de X en Y que satisface las siguientes condiciones*
(1) $Dom(f) = X$.
(2) Si $(x, y), (x, y') \in f$, entonces $y = y'$.
El conjunto Y se llama **codominio o contradominio** *de f y lo denotaremos por $cod(f)$.*

En palabras, una función f de X en Y es una correspondencia entre elementos de X y elementos de Y tal que a cada elemento de X le debe corresponder un único elemento de Y.

Ejemplo 1.4.2. (*i*) Sean $X = \{a, b, c, d\}$, $Y = \{1, 2, 3, 4, 5\}$. $f = \{(a, 2), (b, 3), (c, 1), (d, 5)\}$ es una función de X en Y ya que $Dom(f) = X$ y cada elemento de X aparece una única vez como primera coordenada de un elemento de f.
(*ii*) Con los mismos conjuntos X y Y de (*i*), $h = \{(a, 1), (b, 3), (c, 2), (d, 2)\}$ es también una función. Nótese que en esta función, a diferencia de la de (*i*), hay dos elementos de X, que son c y d que aparecen con la misma segunda coordenada en h.

Para simplificar un poco los comentarios en las siguientes figuras llamamos a $y \in Y$ un compañero de $x \in X$ si y está en la imagen de x bajo la relación. Esto es, $y \in Y$ es un compañero de x si y sólo si $y \in R[\{x\}]$.

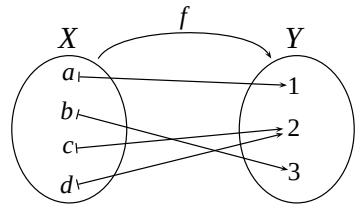


FIGURA 11. La relación f es una función porque cada elemento de X tiene un único compañero en Y.

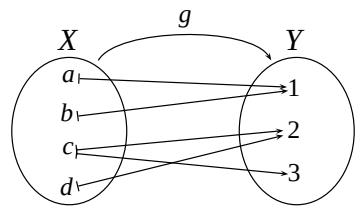


FIGURA 12. La relación g no es una función ya que $c \in X$ tiene dos compañeros en Y que son 2 y 3.

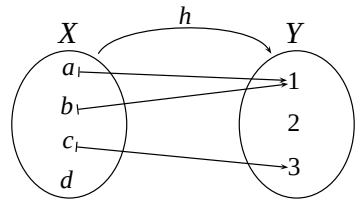


FIGURA 13. La relación h no es una función ya que $d \in X$ no tiene ningún compañero en Y.

Entonces para que una relación f sea función, cada elemento de su dominio debe aparecer una y sólo una vez como primera coordenada de los elementos de f, sin importar si hay elementos diferentes en f que tengan la misma segunda coordenada.

Ejemplo 1.4.3. Existe una única función de $\emptyset$ en cualquier conjunto Y a la que llamamos ***función vacía en Y***. En el caso en que $X \neq \emptyset$ no existe ninguna función de X a $\emptyset$. ¿Por qué?

Ejemplo 1.4.4. Para cada conjunto X, $\Delta_X = \{(x, x) \mid x \in X\}$ es una función de X en X, llamada ***función identidad*** en X y a la que denotaremos 1_X.

Ejemplo 1.4.5. Sean X y Y conjuntos y $y_0 \in Y$ un elemento fijo. $f = \{(x, y_0) \mid x \in X\}$ es una función de X en Y llamada ***función constante*** igual a y_0.

Ejemplo 1.4.6. Sean X y Y conjuntos no vacíos. $\pi_1 = \{((x, y), x) \mid x \in X, y \in Y\}$ es una función de $X \times Y$ en X, llamada ***proyección de $X \times Y$ en X***. De manera análoga, $\pi_2 = \{((x, y), y) \mid x \in X, y \in Y\}$ se llama ***la proyección de $X \times Y$ en Y***.

Notación 1.4.7. *Dada una función f de X en Y y dado una elemento $x \in X$, al único elemento $y \in Y$ tal que $(x, y) \in f$ lo denotaremos por* $\boldsymbol{f(x)}$ *y lo llamamos* **la imagen de x bajo la función f**. *Así pues la función queda determinada por X (dominio), Y (codominio) y el valor de $f(x)$ para cada $x \in X$. Usaremos de aquí en adelante la notación* $\boldsymbol{f : X \longrightarrow Y}$ *y llamaremos a $f(x)$ la* **regla de correspondencia**.

Otra notación usual es

$$X \xrightarrow{f} Y$$

Veamos con la notación introducida cuándo dos funciones son iguales. A partir de aquí las funciones consideradas serán no vacías, lo que significa que $X \neq \emptyset$ y por lo tanto $Y \neq \emptyset$. (véase ejercicio 1.4.5)

Teorema 1.4.8. *Las funciones $f : X \longrightarrow Y$ y $g : X' \longrightarrow Y'$ son iguales si y sólo si $X = X', Y = Y'$ y $f(x) = g(x)$ para todo $x \in X$.*

Este teorema es consecuencia inmediata del teorema 1.3.2. (véase ejercicio 1.4.7) Resumiendo, una función consiste de tres datos que son el dominio, el codominio y lo que hemos llamado la regla de correspondencia, que es, para cada x del dominio debemos decir quién es $f(x)$.

Ejemplo 1.4.9. Con la nueva notación, en los ejemplos 1.4.4, 1.4.5 y 1.4.6 tenemos respectivamente que
(a) $1_X : X \longrightarrow X$, $1_X(x) = x$ para toda $x \in X$.
(b) $f : X \longrightarrow Y$, $f(x) = y_0$ para toda $x \in X$.
(c) $\pi_X : X \times Y \longrightarrow X$, $\pi_X(x, y) = x$; $\pi_Y : X \times Y \longrightarrow Y$, $\pi_Y(x, y) = y$.

Observación 1.4.10. Respecto al ejemplo anterior, en realidad debimos haber escrito $\pi_X((x,y)) = x$ y $\pi_Y((x,y)) = y$. Sin embargo por comodidad lo escribimos $\pi_X(x,y) = x$ y $\pi_Y(x,y) = y$.

Ejemplo 1.4.11. Sean $f : X \longrightarrow Y$ una función, $X' \subseteq X$ y $g : X' \longrightarrow Y$ con regla de correspondencia $g(x) = f(x)$ para toda $x \in X'$. g es una función que se llama ***la restricción de f a X'*** y se denota por $f|_{X'}$. En particular a la restricción de 1_X en X, $\mathbf{1_X|_{X'} : X' \longrightarrow X}$ se le llama ***función inclusión*** de X' en X.

Ejemplo 1.4.12. Sea $\mathbb{N}$ el conjunto de los números naturales y $\mathbb{Z}$ el conjunto de los números enteros. Definimos $f : \mathbb{N} \longrightarrow \mathbb{Z}$ por $f(x) = x - x^2$.
Veamos quién es $f(x)$ para algunos valores de x:

$$f(0) = 0 - 0^2 = 0; \quad f(1) = 1 - 1^2 = 1 - 1 = 0; \quad f(2) = 2 - 2^2 = -2;$$

$$f(7) = 7 - 7^2 = -42.$$

Observación 1.4.13. Cuando construyamos una función debemos tener cuidado en que ésta esté bien definida, es decir, a cada x en el dominio no sólo le debe corresponder un único elemento sino que éste pertenezca efectivamente al codominio.

Ejemplo 1.4.14. Si f es la relación de $\mathbb{N}$ en $\mathbb{Z}$ cuya regla de correspondencia está dada $f(x) = x - x^2$, f no es una función de $\mathbb{Z}$ en $\mathbb{N}$ ya que $f(2) = 2 - 2^2 = -2$ y en este caso -2 no pertenece al codominio que es $\mathbb{N}$.

Ejemplo 1.4.15. Sean $A = \{0, 1, 4, 9, 16\}$ y $B = \{-2, -1, 0, 1, 2, 3, 4\}$ y consideremos la relación f de A en B definida por $(x,y) \in f$ si y sólo si $x = y^2$. Esta relación no es una función de A en B ya que por ejemplo, según la definición de f, $(4,2) \in f$ y $(4,-2) \in f$.

***Definición 1.4.16**. Sea $f : X \longrightarrow Y$ una función. La* **imagen de f** *es la imagen de la relación f, es decir,*

$$Im(f) = \{y \in Y \mid \textit{existe } x \in X \textit{ tal que } f(x) = y\}.$$

Esto es, $y \in Im(f) \iff \exists\, x \in X$ $y = f(x)$.

También podemos describir la imagen de f como

$$\mathbf{Im(f)} = \{f(x) \mid x \in X\}$$

Ejemplo 1.4.17. $Im(1_X) = X$ ya que para cada $x \in X$, $1_X(x) = x$.

Ejemplo 1.4.18. Sea $f : \mathbb{N} \longrightarrow \mathbb{N}$ dada por $f(x) = x + 1$. $Im(f) = \mathbb{N} - \{0\}$. Para demostrar la igualdad es suficiente probar que $\mathbb{N} - \{0\} \subseteq Im(f)$. ¿Por qué?
Si $x \in \mathbb{N} - \{0\}$, entonces $x \neq 0$ y por lo tanto $x - 1 \in \mathbb{N}$, así que $f(x - 1) = (x - 1) + 1 = x$ y por lo tanto $x \in Im(f)$.

Como las funciones son relaciones, como tales podemos componerlas en los casos en que esto se pueda hacer, es decir, con el lenguaje de funciones, se pueden componer dos funciones cuando el codominio de la primera coincide con el dominio de la segunda y en estos términos tenemos:

Definición 1.4.19. *Sean $f : X \longrightarrow Y$ y $g : Y \longrightarrow Z$ funciones. La* ***composición de f con g*** *es la función $h : X \longrightarrow Z$ dada por $h(x) = g(f(x))$, para cada $x \in X$. A esta función h la denotamos por $\boldsymbol{g \circ f}$. En diagrama*

$$\begin{array}{ccccc} & & g\circ f & & \\ & \overset{f}{\curvearrowright} & & \overset{g}{\curvearrowright} & \\ X & \longrightarrow & Y & \longrightarrow & Z \\ \cup & & \cup & & \cup \\ x & \longmapsto & f(x) & \longmapsto & g(f(x)) \end{array}$$

Ejemplo 1.4.20. Sean $X = \{a, b, c\}$, $Y = \{2, 5, 7, 9\}$ y $Z = \{a, b, 1, 2\}$. Definamos $f : X \longrightarrow Y$ por $f(a) = 5$, $f(b) = 9$, $f(c) = 5$ y $g : Y \longrightarrow Z$ por $g(2) = 1$, $g(5) = 1$, $g(7) = a$ y $g(9) = b$. Entonces la regla de correspondencia de $g \circ f$ está dada por

$$(g \circ f)(a) = g(f(a)) = g(5) = 1.$$
$$(g \circ f)(b) = g(f(b)) = g(9) = b.$$
$$(g \circ f)(c) = g(f(c)) = g(5) = 1.$$

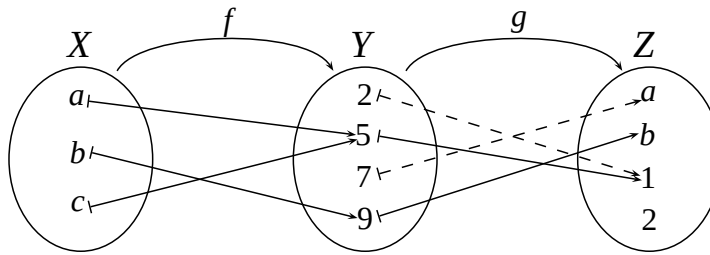


FIGURA 14. $g \circ f$

Nota 1.4.21. Al hacer la composición $g \circ f$, g solamente toma valores en $Im(f)$ y teniendo en cuenta esto se puede definir la composición de manera más general:

si $f : X \to Y$ es una función y $g : Z \to W$ es una función tal que $Im(f) \subseteq Z$. Entonces $g \circ f$ es una función de X a W.

Ejemplo 1.4.22. Sean $f : \mathbb{N} \longrightarrow \mathbb{N}$ y $g : \mathbb{N} \longrightarrow \mathbb{Z}$ funciones dadas por $f(x) = x + 1$ y $g(x) = x - x^2$ respectivamente. Entonces $g \circ f : \mathbb{N} \longrightarrow \mathbb{Z}$ está dada por

$$(g \circ f)(x) = g(f(x)) = g(x + 1) = (x + 1) - (x + 1)^2 = -x^2 - x.$$

Ejemplo 1.4.23. Sean X y Y conjuntos no vacíos, $x_0 \in X$ y $y_0 \in Y$ elementos fijos en X y Y respectivamente. Defínase $i_1 : X \longrightarrow X \times Y$ e $i_2 : Y \longrightarrow X \times Y$ como $i_1(x) = (x, y_0)$ e $i_2(y) = (x_0, y)$. Considerando las funciones π_1 y π_2 del ejemplo 1.4.6 tenemos que

$$\begin{array}{lll}
\pi_1 \circ i_1 : X \longrightarrow X & \text{y} & (\pi_1 \circ i_1)(x) = \pi_1(i_1(x)) = \pi_1(x, y_0) = x. \\
\pi_2 \circ i_2 : Y \longrightarrow Y & \text{y} & (\pi_2 \circ i_2)(y) = \pi_2(i_2(y)) = \pi_2(x_0, y) = y. \\
\pi_1 \circ i_2 : Y \longrightarrow X & \text{y} & (\pi_1 \circ i_2)(y) = \pi_1(i_2(y)) = \pi_1(x_0, y) = x_0. \\
\pi_2 \circ i_1 : X \longrightarrow Y & \text{y} & (\pi_2 \circ i_1)(x) = \pi_2(i_1(x)) = \pi_2(x, y_0) = y_0.
\end{array}$$

Entonces se tienen las siguientes igualdades de funciones debido a que tienen el mismo dominio, mismo codominio y misma regla de correspondencia

$$\begin{array}{l}
\pi_1 \circ i_1 = 1_X; \quad \pi_2 \circ i_2 = 1_Y \\
\pi_1 \circ i_2 = \text{función constante igual a } x_0. \\
\pi_2 \circ i_1 = \text{función constante igual a } y_0.
\end{array}$$

También podemos considerar las siguientes composiciones cuando $X = Y$ y $x_0 = y_0$:

$$\begin{array}{lll}
i_1 \circ \pi_1 : X \times X \longrightarrow X \times X & \text{y} & (i_1 \circ \pi_1)(x, y) = i_1(\pi_1(x, y)) = i_1(x) = (x, x_0). \\
i_2 \circ \pi_2 : X \times X \longrightarrow X \times X & \text{y} & (i_2 \circ \pi_2)(x, y) = i_2(\pi_2(x, y)) = i_2(y) = (x_0, y). \\
i_1 \circ \pi_2 : X \times X \longrightarrow X \times X & \text{y} & (i_1 \circ \pi_2)(x, y) = i_1(\pi_2(x, y)) = i_1(y) = (y, x_0). \\
i_2 \circ \pi_1 : X \times X \longrightarrow X \times X & \text{y} & (i_2 \circ \pi_1)(x, y) = i_2(\pi_1(x, y)) = i_2(x) = (x_0, y).
\end{array}$$

Proposición 1.4.24. *Sea $f : X \longrightarrow Y$ una función. Entonces*

(1) $f \circ 1_X = f$,
(2) $1_Y \circ f = f$.

La demostración se deja como el ejercicio 1.4.15.

Teorema 1.4.25. *Sean $f : X \longrightarrow Y$, $g : Y \longrightarrow Z$ y $h : Z \longrightarrow W$ funciones. Entonces $(h \circ g) \circ f = h \circ (g \circ f)$. Esto es, la composición de funciones es asociativa.*

Demostración. Como $(h \circ g) \circ f$ y $h \circ (g \circ f)$ tienen el mismo dominio y el mismo contradominio sólo es necesario demostrar que tienen la misma regla de correspondencia.
Sea $x \in X$. Entonces

$$[(h \circ g) \circ f](x) = (h \circ g)(f(x)) = h(g(f(x))) = h((g \circ f)(x)) = [h \circ (g \circ f)](x)$$

Por lo tanto $(h \circ g) \circ f = h \circ (g \circ f)$. ∎

Es importante hacer notar que en caso de que se pueda realizar la composición $g \circ f$, no necesariamente se puede hacer la composición $f \circ g$. Para que existan ambas composiciones debemos tener que el codominio de f debe ser igual al dominio de g y el codominio de g debe ser igual al dominio de f. Sin embargo aún en estos casos sucede generalmente que ambas composiciones no son iguales, es decir en general $g \circ f \neq f \circ g$.

Ejemplo 1.4.26. Sean $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ dada por $f(x) = x - 2$ y $g : \mathbb{Z} \longrightarrow \mathbb{Z}$ dada por $g(x) = x^2$. Podemos formar ambas composiciones:

$$g \circ f : \mathbb{Z} \to \mathbb{Z}, (g \circ f)(x) = g(f(x)) = g(x-2) = (x-2)^2 = x^2 - 4x + 4,$$
$$f \circ g : \mathbb{Z} \to \mathbb{Z}, (f \circ g)(x) = f(g(x)) = f(x^2) = x^2 - 2.$$

Aún cuando $g \circ f$ y $f \circ g$ tienen el mismo dominio y el mismo codominio, evidentemente tiene distintas regla de correspondencia, por ejemplo, $(g \circ f)(0) = 4$ y $(f \circ g)(0) = -2$. Luego $g \circ f \neq f \circ g$.

Definición 1.4.27*. Sean $f : X \longrightarrow Y$ una función, $A \subseteq X$ y $B \subseteq Y$.*
(1) La **imagen directa** *de A bajo f es el conjunto*

$$\boldsymbol{f[A]} = \{f(x) \mid x \in A\} (\subseteq Y)$$

(imagen de A bajo la relación f, pag.40)
(2) La **imagen inversa** *de B bajo f es el conjunto*

$$\boldsymbol{f^{-1}[B]} = \{x \in X \mid f(x) \in B\} (\subseteq X)$$

(imagen inversa de B bajo la relación f, pag.40)

Entonces, para cada $x \in X$ y $y \in Y$ tenemos

$$y \in f[A] \iff \exists\, x \in A\ f(x) = y; \qquad x \in f^{-1}[B] \iff f(x) \in B.$$

La negación de ambas sería, respectivamente

$$y \notin f[A] \iff \forall\, x \in A\ f(x) \neq y; \qquad x \notin f^{-1}[B] \iff f(x) \notin B.$$

Ejemplo 1.4.28. Sean X y Y conjuntos no vacíos.

(1) Consideremos la función identidad $1_X : X \to X$ y sea $A \subseteq X$. Entonces $1_X[A] = A$ y $1_X^{-1}[A] = A$.
(2) Sean $y_0 \in Y$ y $g : X \to Y$ la función constante igual a y_0. Para todo subconjunto $A \neq \emptyset$ de X, $g[A] = \{y_0\}$ y si $B \subseteq Y$, entonces

$$f^{-1}[B] = \begin{cases} X \text{ si } y_0 \in B \\ \emptyset \text{ si } y_0 \notin B \end{cases}.$$

(3) Sea $h : X \to Y$ la función del ejemplo 1.4.2 (*ii*) y sea $A = \{a, c\}$ y $B = \{2, 3, 4\}$. Entonces $h[A] = \{1, 2\}$ y $h^{-1}[B] = \{b, c, d\}$. Si $C = \{5\}$, entonces $h^{-1}[C] = \emptyset$.

Nota 1.4.29. En la definición de imagen directa y de imagen inversa hemos usado paréntesis de corchetes para evitar confusiones, debido a que un subconjunto A de X bien podría ser también elemento de X y en ese caso $f(A)$ denota la imagen del elemento A de X, mientras que $f[A]$ es el conjunto de imágenes de los elementos de A.

Ejemplo 1.4.30. Sean $X = \{a, b, \{a, b\}, c, d, \{a, b, c\}\}$, $Y = \{1, 2, 3, \{1, 2, 3\}, 4\}$ conjuntos y $f : X \longrightarrow Y$ definida por $f(a) = 1$, $f(b) = \{1, 2, 3\}$, $f(\{a, b\}) = 4$, $f(c) = 2$, $f(d) = 1$ y $f(\{a, b, c\}) = \{1, 2, 3\}$. $A = \{a, b\}$ es tanto elemento de X como subconjunto de él, así que como elemento de X tenemos que $f(A) = f(\{a, b\}) = 4$, mientras que como subconjunto de X, tenemos que $f[A] = f[\{a, b\}] = \{f(a), f(b)\} = \{1, \{1, 2, 3\}\}$. El conjunto $B = \{1, 2, 3\}$ es tanto elemento como subconjunto de Y, así que hay que tener cuidado con B ya que $f^{-1}[B]$ denota la imagen inversa de B como subconjunto de Y y si queremos encontrar la imagen inversa de B, ésta es $f^{-1}[\{B\}]$. Así pues $f^{-1}[B] = \{a, c, d\}$ y $f^{-1}[\{B\}] = \{b, \{a, b, c\}\}$.

Teorema 1.4.31. *Sea $f : X \longrightarrow Y$ una función, $A_1, A_2 \subseteq X$ y $B_1, B_2 \subseteq Y$. Entonces*
(1) $A_1 \subseteq A_2$ *implica* $f[A_1] \subseteq f[A_2]$,
(2) $f[A_1 \cup A_2] = f[A_1] \cup f[A_2]$,
(3) $f[A_1 \cap A_2] \subseteq f[A_1] \cap f[A_2]$,
(4) $f[A_1 - A_2] \supseteq f[A_1] - f[A_2]$,
(5) $B_1 \subseteq B_2$ *implica* $f^{-1}[B_1] \subseteq f^{-1}[B_2]$,
(6) $f^{-1}[B_1 \cup B_2] = f^{-1}[B_1] \cup f^{-1}[B_2]$,
(7) $f^{-1}[B_1 \cap B_2] = f^{-1}[B_1] \cap f^{-1}[B_2]$,
(8) $f^{-1}[B_1 - B_2] = f^{-1}[B_1] - f^{-1}[B_2]$,
(9) $f^{-1}[f[A_1]] \supseteq A_1$,
(10) $f[f^{-1}[B_1]] \subseteq B_1$.

Demostración. Demostraremos (1), (3), (4), (6), (8) y (10) y dejamos como ejercicio la demostración de los restantes. (véase ejercicio 1.4.34)

(1) Supongamos que $A_1 \subseteq A_2$ y sea $y \in f[A_1]$. Entonces, por definición, existe $x \in A_1$ tal que $f(x) = y$. Pero por hipótesis $A_1 \subseteq A_2$ así que $x \in A_2$. Por lo tanto $f(x) = y \in f[A_2]$.

(3) Como $A_1 \cap A_2 \subseteq A_1$ y $A_1 \cap A_2 \subseteq A_2$, por el inciso (1) $f[A_1 \cap A_2] \subseteq f[A_1]$ y $f[A_1 \cap A_2] \subseteq f[A_2]$ y por lo tanto $f[A_1 \cap A_2] \subseteq f[A_1] \cap f[A_2]$.

(4) Sea $y \in f[A_1] - f[A_2]$. Entonces $y \in f[A_1]$ y $y \notin f[A_2]$, lo que significa que $y = f(x)$ para alguna $x \in A_1$ y $y \neq f(z)$ para todo $z \in A_2$. luego $x \notin A_2$ por lo que $x \in A_1 - A_2$ y por lo tanto $y = f(x) \in f[A_1 - A_2]$.

(6) $f^{-1}[B_1 \cup B_2] = f^{-1}[B_1] \cup f^{-1}[B_2]$

$\subseteq$) $f^{-1}[B_1 \cup B_2] \subseteq f^{-1}[B_1] \cup f^{-1}[B_2]$. Si $x \in f^{-1}[B_1 \cup B_2]$, entonces $f(x) \in B_1 \cup B_2$ y por lo tanto $f(x) \in B_1$ o $f(x) \in B_2$.

i) Si $f(x) \in B_1$, entonces $x \in f^{-1}[B_1]$, de aquí concluimos que $x \in f^{-1}[B_1] \cup f^{-1}[B_2]$.

ii) Si $f(x) \in B_2$, se tiene que $x \in f^{-1}[B_2]$ y así $x \in f^{-1}[B_1] \cup f^{-1}[B_2]$.

En ambos casos $x \in f^{-1}[B_1] \cup f^{-1}[B_2]$.

$\supseteq$) $f^{-1}[B_1] \cup f^{-1}[B_2] \subseteq f^{-1}[B_1 \cup B_2]$.
Por (5) $B_1 \subseteq B_1 \cup B_2$ y $B_2 \subseteq B_1 \cup B_2$, implican $f^{-1}[B_1] \subseteq f^{-1}[B_1 \cup B_2]$ y $f^{-1}[B_2] \subseteq f^{-1}[B_1 \cup B_2]$. Por lo tanto $f^{-1}[B_1] \cup f^{-1}[B_2] \subseteq f^{-1}[B_1 \cup B_2]$.

(8) $f^{-1}[B_1 - B_2] = f^{-1}[B_1] - f^{-1}[B_2]$

$\subseteq$) $f^{-1}[B_1 - B_2] \subseteq f^{-1}[B_1] - f^{-1}[B_2]$.
Sea $x \in f^{-1}[B_1 - B_2]$. Entonces $f(x) \in B_1 - B_2$ y así $f(x) \in B_1$ y $f(x) \notin B_2$. Pero esto último implica que $x \in f^{-1}[B_1]$ y $x \notin f^{-1}[B_2]$. Por lo tanto $x \in f^{-1}[B_1] - f^{-1}[B_2]$.

$\supseteq$) $f^{-1}[B_1] - f^{-1}[B_2] \subseteq f^{-1}[B_1 - B_2]$.
Si $x \in f^{-1}[B_1] - f^{-1}[B_2]$, entonces $x \in f^{-1}[B_1]$ y $x \notin f^{-1}[B_2]$ y por lo tanto $f(x) \in B_1$ y $f(x) \notin B_2$, que es, $f(x) \in B_1 - B_2$ y esto último implica que $x \in f^{-1}[B_1 - B_2]$.

(10) $f[f^{-1}[B_1]] \subseteq B_1$.
$y \in f[f^{-1}[B_1]]$ implica que existe $x \in f^{-1}[B_1]$ tal que $y = f(x)$. Pero si $x \in f^{-1}[B_1]$, entonces $f(x) \in B_1$, esto es $y \in B_1$. ∎

En los incisos (3), (4), (9) y (10) del teorema 1.4.31 en general no se da la igualdad como lo muestran los siguientes ejemplos.

Ejemplo 1.4.32. Sea $f : \mathbb{N} \longrightarrow \mathbb{N}$, dada por $f(x) = 1$ para todo $x \in \mathbb{N}$ y sean $A_1 = \{1, 2, 3\}$ y $A_2 = \{4, 5, 6\}$.

(1) $f[A_1 \cap A_2] = f[\varnothing] = \varnothing$ y $f[A_1] \cap f[A_2] = \{1\} \cap \{1\} = \{1\}$. Por lo tanto $f[A_1 \cap A_2] \subsetneq f[A_1] \cap f[A_2]$.
(2) En cuanto a la diferencia, $f[A_1 - A_2] = f[A_1] = \{1\}$ y $f[A_1] - f[A_2] = \{1\} - \{1\} = \varnothing$. En este caso también $f[A_1] - f[A_2] \subsetneq f[A_1 - A_2]$.
(3) Para la imagen inversa, $f^{-1}[f[A_1]] = f^{-1}[f[\{1, 2, 3\}]] = f^{-1}[\{1\}] = \mathbb{N}$. Luego $A_1 \subsetneq f^{-1}[f[A_1]] = \mathbb{N}$.
(4) Por último si consideramos $B = \{2\}$, entonces $f[f^{-1}[B]] = f[\varnothing] = \varnothing$ y así $f[f^{-1}[B]] = f[\varnothing] \subsetneq B$.

Ejemplo 1.4.33. Sea $f : \mathbb{Z} \longrightarrow \mathbb{N}$ definida por $f(x) = x^2$ y sean $A_1 = \{1, -1, -3, -2, 6\}$ y $A_2 = \{-1, -3, 2, 5\}$.

(1) $f[A_1 \cap A_2] = f[\{-1, -3\}] = \{1, 9\}$, $f[A_1] = \{1, 4, 9, 36\}$, $f[A_2] = \{1, 4, 9, 25\}$, por lo que $\{1, 9\} = f[A_1 \cap A_2] \subsetneq f[A_1] \cap f[A_2] = \{1, 4, 9\}$.
(2) En cuanto a la diferencia,

$$\{36\} = f[A_1] - f[A_2] \subsetneq f[A_1 - A_2] = f[\{1, -2, 6\}] = \{1, 4, 36\}.$$

(3) Si $A = \{-1, 4\}$, entonces $f^{-1}[f[A]] = \{1, -1, 4, -4\}$ y así $A \subsetneq f^{-1}[f[A]]$.
(4) Para $B = \{4, 5\}$, $f[f^{-1}[B]] = \{4\}$ por lo que $\{4\} = f[f^{-1}[B]] \subsetneq B = \{4, 5\}$.

§ 1.5. Funciones inyectivas y funciones suprayectivas

La pregunta que uno podría hacerse es si existe una función, donde la igualdad se dé en los incisos (3) y (4) del teorema 1.4.31 sin importar quiénes sean A_1 y A_2 o que la igualdad se dé siempre en el inciso (9) para cualquier subconjunto B del codominio. Observando los ejemplos 1.4.32 y 1.4.33 en ambos podemos ver que el hecho de que existan elementos distintos en el dominio con la misma imagen nos permitió construir los conjuntos A_1 y A_2, y en el caso de la imagen inversa, el subconjunto B contenía un elemento que no pertenece a la imagen como lo es 2 en el ejemplo 1.4.32. Como más adelante veremos, si no existen elementos distintos en el dominio de una función que tengan la misma imagen, entonces siempre se dará la igualdad en los incisos (3), (4) y (9) y si cada elemento del codominio de f pertenece a $Im(f)$, entonces la igualdad deberá darse en (10). Funciones que

satisfacen estas propiedades son de suma importancia, por lo que les daremos un nombre especial.

Definición 1.5.1. *Se dice que una función $f : X \longrightarrow Y$ es* ***inyectiva*** *si para cada pareja de elementos $x_1, x_2 \in X$, si $x_1 \neq x_2$, entonces $f(x_1) \neq f(x_2)$.*

De manera equivalente, una función $f : X \longrightarrow Y$ es inyectiva si y sólo si para cualesquiera $x_1, x_2 \in X$, $f(x_1) = f(x_2)$ implica $x_1 = x_2$.
Entonces según la definición, para mostrar que una función f no es inyectiva basta mostrar una pareja de elementos x_1 y x_2 en el dominio de f tales que $x_1 \neq x_2$ y $f(x_1) = f(x_2)$.

Ejemplo 1.5.2. Sea $f : \mathbb{Z} \longrightarrow \mathbb{Z}$, dada por $f(x) = x^2$. f no es inyectiva ya que $1 \neq -1$ y $f(1) = 1 = f(-1)$.

Ejemplo 1.5.3. Sea $g : \mathbb{N} \longrightarrow \mathbb{Z}$, dada por $g(x) = x^2$. g es inyectiva porque si $g(x_1) = g(x_2)$, con $x_1, x_2 \in \mathbb{N}$, entonces $x_1^2 = x_2^2$. Por lo tanto $x_1 = x_2$ o $x_1 = -x_2$. Si $x_2 = 0$, entonces $x_1 = -x_2 = 0$ y en caso de que ambos sea distintos de cero como $x_1, x_2 \in \mathbb{N}$, no puede suceder que sea $x_1 = -x_2$ por lo que debe ser $x_1 = x_2$.

Si el lector se fija en las funciones f y g de los ejemplos 1.5.2 y 1.5.3, podrá apreciar que ambos tiene la misma regla de correspondencia y sin embargo g es inyectiva y f no lo es. Esto se debe a que sus dominios son distintos, lo que muestra la importancia de cada uno de los datos que definen a una función.

Teorema 1.5.4. *Sean $f : X \longrightarrow Y$ y $g : Y \longrightarrow Z$ funciones.*
(1) *Si f y g son inyectivas, entonces $g \circ f$ es inyectiva.*
(2) *Si $g \circ f$ es inyectiva, entonces f es inyectiva.*

Demostración.

(1) Supongamos que f y g son inyectivas y supongamos que $(g \circ f)(x_1) = (g \circ f)(x_2)$. Entonces $g(f(x_1)) = g(f(x_2))$. Por ser g inyectiva se tiene que $f(x_1) = f(x_2)$ y por ser f inyectiva, debe ser $x_1 = x_2$. Hemos demostrado entonces que $(g \circ f)(x_1) = (g \circ f)(x_2)$ implica $x_1 = x_2$. Por lo tanto $g \circ f$ es inyectiva.
(2) Si $g \circ f$ es inyectiva y $f(x_1) = f(x_2)$, entonces $g(f(x_1)) = g(f(x_2))$, es decir, $(g \circ f)(x_1) = (g \circ f)(x_2)$. Pero como $g \circ f$ es inyectiva, podemos afirmar que $x_1 = x_2$. Así pues que $f(x_1) = f(x_2)$ implica $x_1 = x_2$. Por lo tanto f es inyectiva.

■

A continuación daremos un ejemplo de dos funciones f y g tales que $g \circ f$ es inyectiva pero g no lo es, lo que muestra que la afirmación inversa de (1) del teorema 1.5.4, no es verdadera.

Ejemplo 1.5.5. Sean $f : \mathbb{N} \longrightarrow \mathbb{Z}$ dada por $f(x) = x + 1$ y $g : \mathbb{Z} \longrightarrow \mathbb{Z}$ dada por $g(x) = x^2$. $g \circ f : \mathbb{N} \longrightarrow \mathbb{Z}$ está definida por $(g \circ f)(x) = (x + 1)^2$. $g \circ f$ es inyectiva (véase ejemplo 1.5.3) y por lo tanto, por (2) del teorema 1.5.4, f lo es. Sin embargo g no es inyectiva (véase ejemplo 1.5.2).

Definición 1.5.6. *Una función $f : X \longrightarrow Y$ es* ***suprayectiva*** *o* ***sobre*** *si $Im(f) = Y$.*

Debido a que para cualquier función $f : X \longrightarrow Y$ siempre se tiene que $Im(f) \subseteq Y$, para que una función $f : X \longrightarrow Y$ sea suprayectiva bastará ver que $Y \subseteq Im(f)$, es decir, para toda $y \in Y$, debe existir $x \in X$ tal que $f(x) = y$.
Para mostrar que una función $f : X \longrightarrow Y$ no es suprayectiva, basta exhibir un elemento $y \in Y$ tal que $f(x) \neq y$ para toda $x \in X$.

Ejemplo 1.5.7. $f : \mathbb{Z} \longrightarrow \mathbb{N}$ dada por $f(x) = x^2$ no es suprayectiva ya que, por ejemplo, $3 \in \mathbb{N}$ y no existe $x \in \mathbb{Z}$ tal que $f(x) = x^2 = 3$ (3 no es el cuadrado de ningún número entero). Aquí $Im(f) = \{0, 1, 4, 9, 16, \ldots\}$.

Ejemplo 1.5.8. $f : \mathbb{N} \longrightarrow \mathbb{Z}$ dada por $f(x) = x+1$ no es suprayectiva ya que $0 \in \mathbb{Z}$ y no existe $x \in \mathbb{N}$ tal que $f(x) = x+1 = 0$. Es más $Im(f) = \{1, 2, 3, 4, \ldots\} = \mathbb{N}-\{0\}$.

Ejemplo 1.5.9. $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ dada por $f(x) = x + 1$ es una función suprayectiva. Para cualquier $y \in \mathbb{Z}$, debemos exhibir $x \in \mathbb{Z}$ tal que $f(x) = x + 1 = y$. Si consideramos $x = y - 1$, que sabemos es un entero, tenemos que $f(x) = f(y-1) = (y - 1) + 1 = y$. Por lo tanto $Im(f) = \mathbb{Z}$.

Nuevamente aquí podemos observar que las funciones de estos dos últimos ejemplos en lo único que difieren es en su dominio con lo cual se tiene que una sea suprayectiva y la otra no. Por otro lado, en general, si $f : A \longrightarrow B$ es una función suprayectiva y C es un conjunto tal que $B \subsetneq C$, entonces la función $g : A \longrightarrow C$ definida por $g(x) = f(x)$ es una función que difiere de f en el codominio y por supuesto g no es suprayectiva ya que $Im(g) = Im(f) = B \neq C$.

Teorema 1.5.10. *Sean $f : X \longrightarrow Y$ y $g : Y \longrightarrow Z$ funciones.*
(1) *Si f y g son suprayectivas, entonces $g \circ f$ es suprayectiva.*
(2) *Si $g \circ f$ es suprayectiva, entonces g es suprayectiva.*

Demostración.

(1) Supongamos que f y g son suprayectivas y sea $z \in Z$. Por ser g suprayectiva, existe $y \in Y$ tal que $g(y) = z$. Pero para esta $y \in Y$, ya que f suprayectiva, existe $x \in X$ tal que $f(x) = y$. Entonces $(g \circ f)(x) = g(f(x)) = g(y) = z$ y por lo tanto $g \circ f$ es suprayectiva.
(2) Supongamos que $g \circ f$ es suprayectiva y sea $z \in Z$. Como $g \circ f$ es suprayectiva, existe $x \in X$ tal que $(g \circ f)(x) = z$, es decir, $g(f(x)) = z$. Entonces $f(x)$ es el elemento de Y que buscamos pues $y = f(x)$ es tal que $g(y) = z$. ∎

En los siguientes ejemplos de las funciones f y g, se muestra que la composición $g \circ f$ es suprayectiva y f no lo es, lo que significa que el inverso de (1) del teorema 1.5.10 no es verdadero.

Ejemplo 1.5.11. Sean $f : \mathbb{N} \to \mathbb{Z}$ definida por $f(x) = -x$ y $g : \mathbb{Z} \to \{0, 1, 4, 9, 16, \ldots\}$ dada por $g(x) = x^2$. Entonces $g \circ f : \mathbb{N} \to \{0, 1, 4, 9, 16, \ldots\}$ es suprayectiva, porque todo elemento en $\{0, 1, 4, 9, 16, \ldots\}$ es de la forma a^2 con $a \in \mathbb{N}$, así para $a^2 \in \{0, 1, 4, 9, 16, \ldots\}$ se tiene que $(g \circ f)(a) = g(f(a)) = g(-a) = a^2$. Sin embargo f no es suprayectiva ya que $2 \notin Im(f)$.

Definición 1.5.12. *Una función $f : X \longrightarrow Y$ es* ***biyectiva*** *si es inyectiva y suprayectiva.*

El siguiente resultado es consecuencia inmediata de los teoremas 1.5.4 y 1.5.10

Corolario 1.5.13. *Sean $f : X \longrightarrow Y$ y $g : Y \longrightarrow Z$ funciones.*
(1) *Si f y g son biyectivas, entonces $g \circ f$ es biyectiva.*
(2) *Si $g \circ f$ es biyectiva, entonces f es inyectiva y g es suprayectiva.*

Ejemplo 1.5.14. Para cada conjunto X, la función identidad $1_X : X \longrightarrow X$ es biyectiva.

Ejemplo 1.5.15. La función $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ definida por $f(x) = x + 1$ es biyectiva. Es inyectiva: si $f(x) = f(x')$, entonces $x + 1 = x' + 1$ y por lo tanto $x = x'$. En el ejemplo 1.5.9 se demostró que f es suprayectiva.

Hagamos un paréntesis aquí, para ayudarnos a comprender los conceptos de esta sección, dibujando los diagramas de algunos ejemplos.

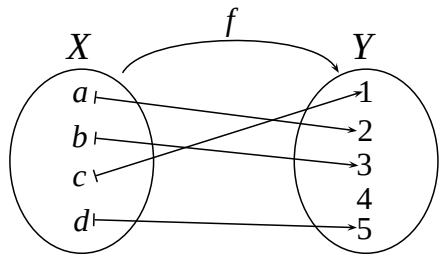


FIGURA 15. f es una función inyectiva ya que cualesquiera dos elementos distintos de X tienen compañeros distintos en Y.

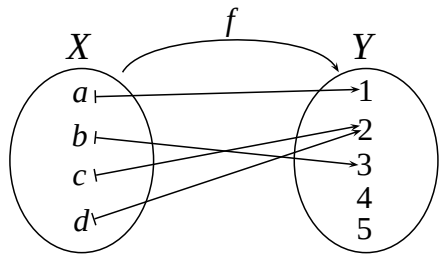


FIGURA 16. f es una función que no es inyectiva porque c y d son elementos distintos de X que tienen el mismo compañero, que es 2, en Y, es decir, $c \neq d$ y $f(c) = 2 = f(d)$.

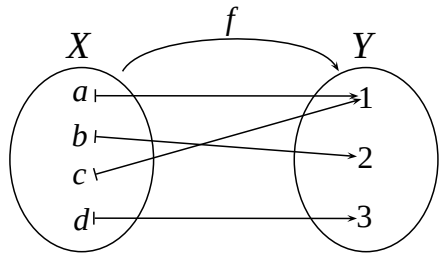


FIGURA 17. f es una función suprayectiva porque todo elemento de Y es compañero de al menos un elemento de X. Esto es $1 = f(a)$, $2 = f(b)$ y $3 = f(d)$.

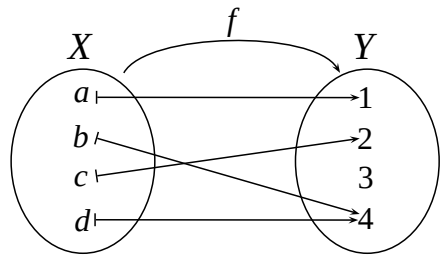


FIGURA 18. f es una función que no es suprayectiva, ya que no todo elemento de Y es compañero de algún un elemento de X. Esto es, 3 no es compañero de ningún elemento de X ya que $f(x) \neq 3$ para todo $x \in X$,.

Nos proponemos ahora dar algunas propiedades equivalentes para las funciones inyectivas y para las funciones suprayectivas, pero antes discutamos algunos ejemplos para ilustrar algunas de estas propiedades.

Considerando el ejemplo que aparece en la figura 15 de la página 55: $X = \{a, b, c, d\}$, $Y = \{1, 2, 3, 4, 5\}$ y $f : X \longrightarrow Y$ está definida por $f(a) = 2$, $f(b) = 3$, $f(c) = 1$ y $f(d) = 5$. En este ejemplo, $Im(f) = \{1, 2, 3, 5\} \subsetneq Y$.

Ahora, definimos la función $g : Y \longrightarrow X$ de la siguiente manera: $g(1) = c$, $g(2) = a$, $g(3) = b$, $g(4) = a$ y $g(5) = d$. Con esta regla de correspondencia resulta que g es función. Al hacer la composición $g \circ f : X \longrightarrow X$ obtenemos $(g \circ f)(a) = g(f(a)) = g(2) = a; (g \circ f)(b) = g(f(b)) = g(3) = b; (g \circ f)(c) = g(f(c)) = g(1) = c; (g \circ f)(d) = g(f(d)) = g(5) = d$, es decir, $(g \circ f)(a) = a, (g \circ f)(b) = b, (g \circ f)(c) = c$ y $(g \circ f)(d) = d$. De aquí concluimos que $g \circ f = 1_X$.

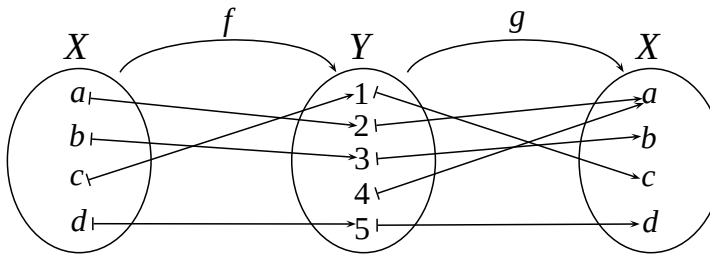


FIGURA 19. $g \circ f = 1_X$.

Es importante hacer notar que la imagen de 4 bajo g es irrelevante en la composición $g \circ f$ y puede ser cualquier elemento de X (Explique por qué es esto, véase ejercicio 1.5.30). Analicemos ahora el ejemplo que aparece en la figura 16 de la página 55 donde

$$f : X = \{a, b, c, d\} \longrightarrow Y = \{1, 2, 3, 4, 5\}$$

está dada por $f(a) = 1$, $f(b) = 3$, $f(c) = 2$ y $f(d) = 2$.
Si quisiéramos hacer lo mismo que hemos hecho anteriormente, es decir, definir una función $h : Y \longrightarrow X$ tal que $(h \circ f)(x) = x$ para toda $x \in X$ se nos presenta un problema al tratar de definir $h(2)$, ya que $f(c) = 2 = f(d)$. ¿Qué valor escogemos para $h(2)$? ¿$h(2) = c$ o $h(2) = d$? Probemos y definamos $h(2) = c$. Entonces $h(1) = a$, $h(2) = c$, $h(3) = b$, $h(4) = a$ y $h(5) = b$. Veamos qué pasa con la composición $h \circ f : X \longrightarrow X$.

$$\begin{array}{ll} (h \circ f)(a) = h(f(a)) = h(1) = a; & (h \circ f)(b) = h(f(b)) = h(3) = b; \\ (h \circ f)(c) = h(f(c)) = h(2) = c\,; & (h \circ f)(d) = h(f(d)) = h(2) = c. \end{array}$$

Esto es, $(h \circ f)(a) = a$, $(h \circ f)(b) = b$, $(h \circ f)(c) = c$ y/ $(h \circ f)(d) = c$. Luego $h \circ f \neq 1_X$
Ahora si definiéramos $h(2) = d$ se tendría $(h \circ f)(c) = h(f(c)) = h(2) = d$ y entonces también $h \circ f \neq 1_X$ (verifíquelo). ¿Qué propiedad tiene f para que en los dos ejemplos que hemos dado, en uno se puede definir g tal que $g \circ f = 1_X$ y en el otro no? En el primer caso cada elemento de $Im(f)$ es imagen de un único elemento del dominio y en el segundo no es así. Esto es, en el primero la función es inyectiva y en el segundo no lo es.
Sigamos analizando ejemplos y consideremos ahora el ejemplo que aparece en la Figura 17 de la página 55, $f : X \longrightarrow Y$, donde $X = \{a, b, c, d\}$, $Y = \{1, 2, 3\}$ y $f(a) = 1$, $f(b) = 2$, $f(c) = 1$ y $f(d) = 3$.
Definamos $g : Y \longrightarrow X$ por $g(1) = a$, $g(2) = b$, $g(3) = d$. De esta manera, $f \circ g : Y \longrightarrow Y$ está definida como sigue:

$$\begin{array}{ll} (f \circ g)(1) = f(g(1)) = f(a) = 1; & (f \circ g)(2) = f(g(2)) = f(b) = 2; \\ (f \circ g)(3) = f(g(3)) = f(d) = 3; & \end{array}$$

Es decir, $(f \circ g)(1) = 1, (f \circ g)(2) = 2, (f \circ g)(3) = 3$. Así tenemos que $f \circ g = 1_Y$.

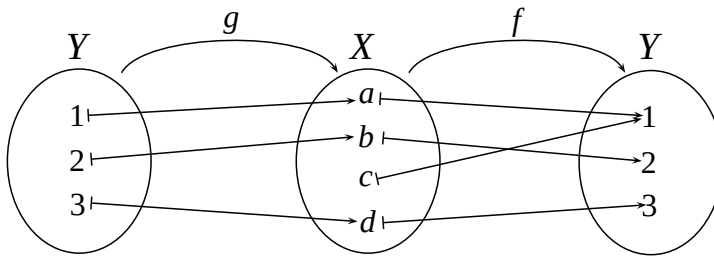


FIGURA 20. $f \circ g = 1_Y$.

Si hubiéramos escogido $g(1) = c$ habríamos llegado a la misma conclusión (verifíquelo).

Tratemos de hacer lo mismo, ahora para el ejemplo que aparece en la figura 18 de la página 56. $X = \{a, b, c, d\}$, $Y = \{1, 2, 3, 4\}$ y $f : X \longrightarrow Y$, definida por $f(a) = 1$, $f(b) = 4$, $f(c) = 2$ y $f(d) = 4$.

Definamos $g : Y \longrightarrow X$ por $g(1) = a$, $g(2) = c$, $g(3) = a$, $g(4) = d$. $f \circ g : Y \longrightarrow Y$ tiene regla de correspondencia:

$$(f \circ g)(1) = f(g(1)) = f(a) = 1; \quad (f \circ g)(2) = f(g(2)) = f(c) = 2;$$
$$(f \circ g)(3) = f(g(3)) = f(a) = 1; \quad (f \circ g)(4) = f(g(4)) = f(d) = 4.$$

Es decir, $(f \circ g)(1) = 1$, $(f \circ g)(2) = 2$, $(f \circ g)(3) = 1$, $(f \circ g)(4) = 4$. Se tiene entonces que $f \circ g \neq 1_Y$ ya que $(f \circ g)(3) \neq 1_Y(3)$. Uno podría pensar que esto se debe a la elección de $g(3)$. Sin embargo, si el lector considera todos los posibles valores que se puede dar a $g(3)$ (¡hágalo!), siempre vamos a tener que $f \circ g \neq 1_Y$. Pero ¿qué diferencia hay con el ejemplo anterior para que en ese caso sí se puede encontrar $g : Y \longrightarrow X$ tal que $f \circ g = 1_Y$ y en el otro no? La diferencia es que en la primera función $Im(f) = Y$ y en la segunda, $Im(f) \subsetneq Y$, es decir, en la primera f es suprayectiva y en la segunda f no lo es. Esta es la razón por la cual no importa qué valores le demos a $g(3)$, para cualquier g siempre se tendrá que $(f \circ g)(3) \neq 3$ pues tendría que existir un elemento $x \in X$ tal que $f(x) = 3$ y esto no es posible debido a que $3 \notin Im(f)$.

Antes de dar las equivalencias que mencionamos en el párrafo inmediato posterior al ejemplo 1.5.15 de la página 54, daremos unas definiciones.

Definición 1.5.16. *Sea $f : X \longrightarrow Y$ una función.*
(1) Una función $g : Y \longrightarrow X$ se llama un ***inverso izquierdo*** *de f si*

$$g \circ f = 1_X.$$

(2) Una función $g : Y \longrightarrow X$ se llama un **inverso derecho** *de f si*

$$f \circ g = 1_Y.$$

Como se puede concluir de los ejemplos discutidos en las páginas 56 y 58, una función puede tener más de un inverso izquierdo y más de un inverso derecho. Veamos ahora las equivalencias mencionadas.

Teorema 1.5.17. *Sea $f : X \longrightarrow Y$ una función. Entonces*
(1) *f es inyectiva si y sólo si f tiene un inverso izquierdo.*
(2) *f es suprayectiva si y sólo si f tiene un inverso derecho.*

Demostración.

(1) f es inyectiva si y sólo si f tiene un inverso izquierdo.

$\Longrightarrow$) Supongamos que f es inyectiva. Queremos demostrar la existencia de una función $g : Y \longrightarrow X$ tal que $g \circ f = 1_X$. Como se puede apreciar, lo importante para definir g es su actuación sobre $Im(f)$ ya que lo que nos lo importante es que $g(f(x)) = x$ para cada $x \in X$. Así pues dividimos al conjunto Y en dos subconjuntos ajenos, $Im(f)$ y $Y - Im(f)$ y sea $x_0 \in X$. Definimos $g : Y \longrightarrow X$ como sigue

$$g(y) = \begin{cases} x & \text{si} \quad y \in Im(f) \text{ y } f(x) = y \\ \\ x_0 & \text{si} \quad y \in Y - Im(f) \end{cases}$$

Observemos que en el caso que $y \in Im(f)$, el elemento $x \in X$ tal que $f(x) = y$ es único, pues f es inyectiva por hipótesis y como $Im(f)$ y $Y - Im(f)$ son conjuntos ajenos, g está bien definida (véase ejercicio 1.4.33).

Veamos que $g \circ f = 1_X$. Sea $x \in X$ y $f(x) = y$. Entonces $(g \circ f)(x) = g(f(x)) = g(y) = x$. Como $g \circ f$ y 1_X tiene el mismo dominio, el mismo codominio y la misma regla de correspondencia, entonces $g \circ f = 1_X$ y por lo tanto g es un inverso izquierdo para f.

$\Longleftarrow$) Si f tiene inverso izquierdo $g : Y \longrightarrow X$. $g \circ f = 1_X$ ya que 1_X es inyectiva, por (2) del teorema 1.5.4 debe ser f inyectiva.

(2) f es suprayectiva si y sólo si f tiene un inverso derecho.

$\Longrightarrow$) Supongamos que f es suprayectiva. Queremos demostrar la existencia de una función $g : Y \longrightarrow X$ tal que $f \circ g = 1_Y$. Para hacer esto fijémonos que g debe estar definida de tal manera que para cada $y \in Y$, $f(g(y)) = y$. Dado $y \in Y$, como f es suprayectiva ($Im(f) = Y$), existe $x \in X$ (no necesariamente única) tal que $f(x) = y$, esto es, para cada $y \in Y$, $f^{-1}[\{y\}]) \neq \emptyset$, así que para

cada $y \in Y$ escojamos $x_y \in f^{-1}[\{y\}]$. Definimos $g : Y \longrightarrow X$ por $g(y) = x_y$ (recordemos que x_y satisface $f(x_y) = y$). Veamos que $f \circ g = 1_Y$. $(f \circ g)(y) = f(g(y)) = f(x_y) = y$ y como $f \circ g$ y 1_Y tiene el mismo dominio, el mismo contradominio y la misma regla de correspondencia, se tiene que $f \circ g = 1_Y$.

$\Longleftarrow$) Supongamos que f tiene inverso derecho, es decir, existe $g : Y \longrightarrow X$ tal que $f \circ g = 1_Y$. Como 1_Y es una función suprayectiva, por (2) del teorema 1.5.10, f debe ser suprayectiva. ∎

Corolario 1.5.18. *Una función $f : X \longrightarrow Y$ es biyectiva si y sólo si f tiene inverso izquierdo y derecho.*

Demostración. Si f es biyectiva, entonces f es inyectiva y es suprayectiva, por lo que, por el teorema 1.5.17, f tiene inverso izquierdo y f tiene inverso derecho. ∎

Queda claro de la demostración del último teorema que una función puede tener varios inversos izquierdos o varios inversos derechos, pero ¿existirá alguna función que tenga un único inverso izquierdo o un único inverso derecho? y si es así ¿qué propiedad tiene la función? el siguiente teorema responde a estas preguntas.

Teorema 1.5.19. *Si $f : X \longrightarrow Y$ es una función biyectiva, entonces cualquier inverso izquierdo de f es igual a cualquier inverso derecho de f. Esto es, existe una única función $g : Y \to X$ tal que $g \circ f = 1_X$ y también tal que $f \circ g = 1_Y$.*

Demostración. Como f es biyectiva, el teorema 1.5.17 nos dice que f tiene inverso izquierdo y tiene inverso derecho. Sean $g : Y \longrightarrow X$ y $h : Y \longrightarrow X$ tales que $g \circ f = 1_X$ y $f \circ h = 1_Y$. Entonces

$$\begin{aligned} g &= g \circ 1_Y && \text{(Proposición 1.4.24)} \\ &= g \circ (f \circ h) && \text{(hipótesis)} \\ &= (g \circ f) \circ h && \text{(Teorema 1.4.25)} \\ &= 1_X \circ h && \text{(hipótesis)} \\ &= h && \text{(Proposición 1.4.24)} \end{aligned}$$ ∎

Hemos demostrado, en el caso de que f sea una función biyectiva, que cualquier inverso izquierdo es igual a cualquier inverso derecho, lo que significa que f tiene un único inverso izquierdo y un único inverso derecho que además deben se iguales.

A la función única del teorema anterior la denotamos por $\boldsymbol{f^{-1}}$ y la llamamos ***función inversa*** de f y diremos que f es una función ***invertible***.

Observación 1.5.20. Es importante hacer notar que cuando hablamos de la imagen inversa de un subconjunto B del codominio de una función f y que hemos denotado por $f^{-1}[B]$, ésta es una simple notación y no debe interpretarse como si fuera la función inversa, pues como acabamos de ver, ésta sólo existe cuando f es biyectiva.

Ejemplo 1.5.21. Sea $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ definida por $f(x) = x + 1$. Como f es biyectiva (ejemplo 1.5.15) debe existir su función inversa f^{-1}. Para saber cuál es la regla de correspondencia de f^{-1} basta ver que f^{-1} debe ser tal que $f^{-1}(f(x)) = x$, es decir, $f^{-1}(x+1) = x$. Entonces debe ser $f^{-1}(x) = x-1$ para toda $x \in \mathbb{Z}$. Comprobémoslo.

$$(f^{-1} \circ f)(x) = f^{-1}(f(x)) = f^{-1}(x + 1) = (x + 1) - 1 = x$$

y

$$(f \circ f^{-1})(x) = f(f^{-1}(x)) = f(x - 1) = (x - 1) + 1 = x.$$

Veamos otra equivalencia para funciones inyectivas y para funciones suprayectivas.

Teorema 1.5.22. *Sea $f : X \longrightarrow Y$ una función.*

(1) *f es inyectiva si y sólo si para cualquier conjunto Z y cualesquiera funciones $g : Z \to X$ y $h : Z \to X$, si $f \circ g = f \circ h$, entonces $g = h$.*
(2) *f es una función suprayectiva si y sólo si para cualquier conjunto Z y cualesquiera funciones $g : Y \to Z$ y $h : Y \to Z$, si $g \circ f = h \circ f$, entonces $g = h$.*

Demostración.

(1) f es inyectiva si y sólo si para cualquier conjunto Z y cualesquiera funciones $g : Z \to X$ y $h : Z \to X$, si $f \circ g = f \circ h$, entonces $g = h$.

$\Longrightarrow$) Supongamos que f es inyectiva y supongamos que $g : Z \to X$ y $h : Z \to X$ son funciones tales que $f \circ g = f \circ h$. Como g y h tienen el mismo dominio y el mismo codominio, para demostrar que $g = h$ basta mostrar que tienen la misma regla de correspondencia. Consideremos entonces $z \in Z$, luego, por hipótesis, $f(g(z)) = f(h(z))$ y ya que f es inyectiva, debe ser que $g(z) = h(z)$ para todo $z \in Z$. Por lo tanto $g = h$.

$\Longleftarrow$) Supongamos que para cualquier conjunto Z y cualesquiera funciones $g : Z \to X$ y $h : Z \to X$, si $f \circ g = f \circ h$, entonces $g = h$ y supongamos que f no es inyectiva. Luego existen $x_0, x_1 \in X$, $x_0 \neq x_1$ tales que $f(x_0) = f(x_1)$. Ahora consideremos $Z = X$. Definamos $g, h : X \to X$ por $g(x) = x_0$ y $h(x) = x_1$ para

todo $x \in X$. Entonces

$$(f \circ g)(x) = f(g(x)) = f(x_0) = f(x_1) = f(h(x)) = (f \circ h)(x),$$

para todo $x \in X$. Esto implica, por hipótesis que $x_0 = g(x) = h(x) = x_1$ para todo $x \in X$ lo que contradice que $x_0 \neq x_1$. Por lo tanto debe ser f inyectiva.

(2) f es una función suprayectiva si y sólo si para cualquier conjunto Z y cualesquiera funciones $g : Y \to Z$ y $h : Y \to Z$, si $g \circ f = h \circ f$, entonces $g = h$.

$\Longrightarrow$) Sea f suprayectiva y $g : Y \to Z$ y $h : Y \to Z$ tales que $g \circ f = h \circ f$. Tomemos cualquier elemento $y \in Y$. Entonces, por hipótesis, existe $x \in X$ tal que $f(x) = y$. Luego $g(y) = g(f(x)) = h(f(x)) = h(y)$ y por lo tanto $g = h$.

$\Longleftarrow$) Supongamos que si $g : Y \to Z$ y $h : Y \to Z$ son funciones tales que $g \circ f = h \circ f$, entonces $g = h$ y supongamos que f no es suprayectiva, esto es, $Y - Im(f) \neq \emptyset$. Definamos $g, h : Y \to Y$ por

$$g(y) = \begin{cases} y & si\ y \in Im(f) \\ y_0 & si\ y \notin Im(f) \end{cases}, \quad y \quad h(y) = \begin{cases} y & si\ y \in Im(f) \\ y_1 & si\ y \notin Im(f) \end{cases},$$

donde y_0 y y_1 son elementos fijos en Y y $y_0 \neq y_1$. Entonces

$$(g \circ f)(x) = g(f(x)) = f(x) = h(f(x)) = (h \circ f)(x),$$

para toda $x \in X$. Por lo tanto, por hipótesis, $g = h$ lo cual es una contradicción ya que para $y \in Y - Im(f)$ $g(y) = y_0$ y $h(y) = y_1$ con $y_0 \neq y_1$. Concluimos entonces que f es suprayectiva. ∎

En muchas ocasiones es muy cómodo trabajar con conjuntos distinguiendo a sus elementos por subíndices, especialmente cuando se trata de conjuntos cuyos elementos son conjuntos. Con el concepto de función podemos formalizar esta idea: Sea C un conjunto y $\varphi : I \longrightarrow C$ una función suprayectiva, donde I es un conjunto que actuará como el conjunto de índices. Podemos denotar a los elementos de C de la manera siguiente: si denotamos por A_i a la imagen de i bajo φ, es decir, $\varphi(i) = A_i$. Entonces C puede describirse como $C = \{A_i \mid i \in I\}$ o más simplemente como $C = \{A_i\}_{i \in I}$ y decimos que C es un ***conjunto*** (**o familia**) ***indicado(a)***, donde I es el conjunto de índices. Cabe mencionar que de la función φ no se ha pedido que sea inyectiva, y no existe problema alguno si no lo es, pues en este caso, simplemente para elementos distintos $i, j \in I$ tales que $\varphi(i) = \varphi(j)$ se tendrá $A_i = A_j$. Si queremos ser más específicos y describir los elementos de C tal que $A_i \neq A_j$ si $i \neq j$, basta considerar I tal que $\varphi : I \longrightarrow C$ es biyectiva.

Resumiendo, por $C = \{A_i\}_{i \in I}$ entenderemos que está dada una función suprayectiva (o en su caso biyectiva) $\varphi : I \longrightarrow C$ tal que $\varphi(i) = A_i$.

Ejemplo 1.5.23.
(*i*) Sea $I = \{a, b, c, d\}$. Entonces $C = \{A_i\}_{i \in I}$ es el conjunto $C = \{A_a, A_b, A_c, A_d\}$.
(*ii*) Si $I = \mathbb{N}$ y $\varphi : I \longrightarrow C$ es biyectiva, describimos los elementos de C como $C = \{A_i\}_{i \in \mathbb{N}} = \{A_0, A_1, A_2, \ldots\}$, donde $A_i \neq A_j$ si $i \neq j$.

§ 1.6. Relaciones de equivalencia

En esta sección estudiamos otro tipo de relación binaria, llamada *relación de equivalencia*. Como se verá más adelante, las relaciones de equivalencia aparecen frecuentemente en matemáticas.

***Definición 1.6.1**. Sea X un conjunto y R una relación de X en X. Decimos que R es una **relación de equivalencia** en X si satisface las siguientes propiedades:*

(1) $(x, x) \in R$ *para toda* $x \in X$ *(Propiedad reflexiva)*
(2) *Si* $(x, y) \in R$, *entonces* $(y, x) \in R$ *(Propiedad simétrica)*
(3) *Si* $(x, y) \in R$ *y* $(y, z) \in R$ *entonces* $(x, z) \in R$ *(Propiedad transitiva)*

Es inmediato de la definición que si R es una relación de equivalencia, entonces $Dom(R) = X$ e $Im(R) = X$.
Introducimos una notación para las relaciones de equivalencia que resulta más ilustrativa y de más fácil manejo.

***Notación 1.6.2**. Sea R una relación de equivalencia en X. Por $\boldsymbol{x \underset{R}{\sim} y}$ entenderemos que $(x, y) \in R$ y cuando no pueda haber confusión omitiremos R, es decir, simplemente escribiremos $x \sim y$, y diremos que $\underset{R}{\sim}$ o $\sim$ es una relación de equivalencia. En el caso en que $(x, y) \notin R$ escribiremos $\boldsymbol{x \underset{R}{\nsim} y}$ o $\boldsymbol{x \nsim y}$. Si $x \sim y$, diremos que x está relacionado con y (según R).*

Con esta nueva notación tenemos que

$\underset{R}{\sim}$ es una relación de equivalencia si y sólo si

$$\begin{cases} (1)\ x \underset{R}{\sim} x \text{ para toda } x \in X & \text{(reflexiva)} \\ (2)\ \text{Si } x \underset{R}{\sim} y, \text{ entonces } y \underset{R}{\sim} x & \text{(simétrica)} \\ (3)\ \text{Si } x \underset{R}{\sim} y \text{ y } y \underset{R}{\sim} z, \text{ entonces } x \underset{R}{\sim} z. & \text{(transitiva)} \end{cases}$$

Ejemplo 1.6.3. Sea X cualquier conjunto. $\Delta_X = \{(x,x) \mid x \in X\}$ y $X \times X$ son relaciones de equivalencia en X. Con la notación $\underset{R}{\sim}$ respectivamente se tiene: para $x, y \in X$ $x \underset{R}{\sim} y$ si y sólo si $x = y$ y, si denotamos por $\sim$ a $X \times X$, $x \sim y$ para todo $x, y \in X$.

Ejemplo 1.6.4. Si $X = \{a\}$, la única relación de equivalencia en X es $\Delta_X = \{(a,a)\} = X \times X$.

Ejemplo 1.6.5. Sea $X = \{a, b, c, d\}$
(1) $R = \{(a,a),(a,b),(b,b),(b,a),(c,c),(d,d)\}$ es una relación de equivalencia en X.
(1') Otra forma de describir R sería: $a \sim a$, $a \sim b$, $b \sim b$,$b \sim a$, $c \sim c$, $d \sim d$.
(2) $S = \{(a,a),(b,b),(d,d)\}$ no es una relación de equivalencia por que $(c,c) \notin S$, es decir S no es reflexiva.
(3) $T = \{(a,a),(b,b),(a,b),(b,a),(c,c),(d,d),(c,d)\}$ no es una relación de equivalencia ya que $(c,d) \in T$ pero $(d,c) \notin T$, es decir T no es simétrica.
(4) $U = \{(a,a),(b,b),(a,b),(b,a),(c,c),(d,d),(a,d),(d,a)\}$ no es una relación de equivalencia ya que $(d,a) \in U$ y $(a,b) \in U$ pero $(d,b) \notin U$, es decir, no es transitiva.

Definición 1.6.6. *Sea R una relación de equivalencia en un conjunto X y $a \in X$. La* ***clase de equivalencia*** *de a respecto a R (o la R-clase de equivalencia de a), es el subconjunto de X, denotado por $[a]_R$ (o simplemente $[a]$), definido por*

$$[a]_R = \left\{ x \in X \mid a \underset{R}{\sim} x \right\}$$

Debido a que $a \underset{R}{\sim} a$ para todo $a \in X$, para una relación de equivalencia $\underset{R}{\sim}$, se tiene que $a \in [a]_R$ y por lo tanto $[a]_R \neq \emptyset$ para toda $a \in X$.
Dada una relación de equivalencia $\sim$, en un conjunto X, estamos asociando a cada elemento $a \in X$ un subconjunto $[a]$ de X que es su clase de equivalencia. En lo que sigue vamos a ver que esta familia $\{[a]\}_{a \in X}$ de subconjuntos de X tiene propiedades muy especiales. Comencemos viendo la relación que puede haber entre dos clases de equivalencia $[a]$ y $[b]$.

Teorema 1.6.7. *Sea $\sim$ una relación de equivalencia en X y sean $a, b \in X$. Las siguientes propiedades son equivalentes*

(1) $a \sim b$,
(2) $[a] = [b]$,

(3) $[a] \cap [b] \neq \emptyset$.

Demostración.

(1)⇒(2) Probaremos que $[a] = [b]$.

$\subseteq$) Sea $x \in [a]$. Entonces $a \sim x$ y por ser $\sim$ simétrica, $x \sim a$. Como $a \sim b$, por ser $\sim$ transitiva, se tiene que $x \sim b$. Lo que implica $x \in [b]$.

$\supseteq$) Análogamente se demuestra que $[b] \subseteq [a]$.

Por lo tanto $[a] = [b]$.

(2)⇒(3) Como $[a] = [b]$ y $[a] \neq \emptyset$ para toda $a \in X$, entonces $[a] \cap [b] = [a] \neq \emptyset$.

(3)⇒(1) Supongamos que $[a] \cap [b] \neq \emptyset$ y sea $x \in [a] \cap [b]$. Entonces $x \in [a]$ y $x \in [b]$, es decir $a \sim x$ y $b \sim x$. Por ser $\sim$ simétrica se tiene que $x \sim b$, así que $a \sim x$ y $x \sim b$, y de la transitividad de $\sim$, obtenemos $a \sim b$. ■

Corolario 1.6.8. *Sea R una relación de equivalencia en X. Si $a, b \in X$, entonces* $[a] = [b]$ *o* $[a] \cap [b] = \emptyset$.

Demostración. Si $[a] \neq [b]$, entonces no puede ser que $[a] \cap [b] \neq \emptyset$ ya que esto implica, por el teorema 1.6.7, que $[a] = [b]$. ■

Notación 1.6.9. *Sea R una relación de equivalencia en X. Denotamos por* $\boldsymbol{P_R}$ *al conjunto de las clases de equivalencia.*

Dada una relación de equivalencia en X y $a \in X$, a cualquier elemento $x \in [a]$ se le llama un **representante** de la clase de equivalencia $[a]$. Esto significa que una clase de equivalencia tiene tantos representantes como elementos. Podemos indicar el conjunto P_R de las clases de equivalencia teniendo a X como conjunto de índices,[1] mediante la función

$$f : X \to P_R, \text{ dada por } f(x) = [x];$$

obsérvese que f es suprayectiva y en general, cuando la relación no sea Δ_X (del ejemplo 1.4.4 y ejemplo 1.6.3), f no es inyectiva, pues si $x \sim y$, entonces $f(x) = [x] = [y] = f(y)$. Sin embargo, si por cada clase de equivalencia consideramos un representante y al conjunto de estos lo denotamos por S, entonces podemos indicar los elementos de P_R usando la función biyectiva $g : S \to P_R$ dada por $g(x) = [x]$ para toda $x \in S$.

[1] véase la definición de familia indicada, página 62.

A pesar de no haber introducido aún la unión arbitraria de una familia de conjuntos, la usaremos en el siguiente definición; en la sección 1.8.1 pueden verse los detalles. Ahí se define, para una familia arbitraria de conjuntos $\{A_i\}_{i\in I}$ su unión que es: $\bigcup_{i\in I} A_i = \{x \mid x \in A_i \text{ para alguna } i \in I\}$. Así pues, $\bigcup_{a\in S}[a] = \{x \mid x \in [a] \text{ para alguna } a \in S\}$. A partir de esto último podemos introducir la siguiente

Definición 1.6.10. *Sea R una relación de equivalencia en un conjunto X. Un subconjunto S de X es un* ***conjunto completo de representantes*** *respecto a R, si*
(1) Para cualesquiera $a, b \in S$; $[a] \cap [b] = \varnothing$ si $a \neq b$.
(2) $\bigcup_{a\in S}[a] = X$.

Efectivamente , el conjunto S dado en el párrafo anterior a la definición 1.6.10, es un conjunto completo de representantes:

(i) para cualesquiera $a, b \in S$, si $a \neq b$, entonces a y b pertenecen a distintas clases (recuérdese que hemos tomado un representante por cada clase), luego por el teorema 1.6.7, $[a] \cap [b] = \varnothing$.

(ii) $X = \bigcup_{a\in S}[a]$ ya que dado $x \in X$, algún $a \in S$ es representante de $[x]$, luego $[a] = [x]$ y entonces $x \in [a]$. Por lo tanto $x \in \bigcup_{a\in S}[a]$.

Cada relación de equivalencia en X determina una familia de subconjuntos de X cuyas propiedades satisfacen las dadas en la siguiente

Definición 1.6.11. *Sea X un conjunto no vacío y $P = \{X_i\}_{i\in I}$ una familia de subconjuntos de X. Decimos que P es una* ***partición*** *de X si satisface*
(1) $X_i \neq \varnothing$ para toda $i \in I$,
(2) Para toda $i, j \in I$, $X_i \neq X_j$ implica $X_i \cap X_j = \varnothing$,
(3) $\bigcup_{i\in I} X_i = X$.

Nota 1.6.12. Si de antemano sabemos que $P = \{X_i\}_{i\in I}$ es una familia de subconjuntos de X y todo los conjuntos X_i son distintos entre sí, para verificar que P es una partición de X la condición (2) de la definición 1.6.11 se puede sustituir por $X_i \cap X_j = \varnothing$ si $i \neq j$. Así se tiene la definición alterna:

Definición 1.6.13. *Sea X un conjunto no vacío y $P = \{X_i\}_{i\in I}$ una familia de subconjuntos de X distintos dos a dos. Decimos que P es una* ***partición*** *de X si satisface*
(1) $X_i \neq \varnothing$ para toda $i \in I$,

(2) $X_i \cap X_j = \emptyset$ *si* $i \neq j$,
(3) $\bigcup_{i \in I} X_i = X$.

Ejemplo 1.6.14. Para cada conjunto $X \neq \emptyset$, $P = \{X\}$ y $P' = \{\{x\} \mid x \in X\}$ son particiones de X.

Ejemplo 1.6.15. Sean $X = \{a, b, c, d\}$, $X_1 = \{a, b\}$, $X_2 = \{c\}$, $X_3 = \{d\}$. $\{X_1, X_2, X_3\}$ es una partición de X.

Ejemplo 1.6.16. Sean $X = \{1, 2, 3, 4, 5\}$, $X_1 = \{1\}$, $X_2 = \{2, 4\}$, $X_3 = \{1, 3, 5\}$. Aún cuando $X = X_1 \cup X_2 \cup X_3$, $\{X_1, X_2, X_3\}$ no es una partición de X ya que $X_1 \cap X_3 = \{1\} \neq \emptyset$ y $X_1 \neq X_3$.

Ejemplo 1.6.17. Sean $\mathbb{N}$ el conjunto de los números naturales, $X_1 = \{x \in \mathbb{N} \mid x \text{ es par}\}$ y $X_2 = \{x \in \mathbb{N} \mid x \text{ es impar}\}$. $P = \{X_1, X_2\}$ es una partición de X.

Teorema 1.6.18. *Sea X un conjunto no vacío, R una relación de equivalencia en X y S un conjunto completo de representantes de X respecto a R. Entonces $P_R = \{[a]_R \mid a \in S\}$ es una partición de X.*

Demostración.

(*i*) $[a] \neq \emptyset$ para toda $a \in S$ ya que, por ser R una relación de equivalencia, $a \in [a]$. Ya hemos visto, en el párrafo anterior de la definición 1.6.11, que para S un conjunto completo de representantes se satisfacen:
(*ii*) $[a] \cap [b] = \emptyset$ si $a \neq b$,
(*iii*) $X = \bigcup_{a \in S} [a]$. ∎

Veamos ahora que cada partición en X induce a su vez una relación de equivalencia en X.

Teorema 1.6.19. *Sean X un conjunto no vacío y $P = \{X_i\}_{i \in I}$ una partición en X donde $X_i \neq X_j$ si $i \neq j$. Entonces la relación definida en X por: "$x \underset{R_P}{\sim} y$ si y sólo si existe $i \in I$ tal que $x, y \in X_i$" es de equivalencia en X.*

Demostración. Verifiquemos que $\underset{R_P}{\sim}$ satisface las condiciones de la definición de relación de equivalencia.

(1) Dada cualquier $x \in X$, como $\bigcup_{i \in I} X_i = X$ por ser $\{X_i\}_{i \in I}$ una partición, entonces $x \in X_i$ para alguna $i \in I$. Por lo tanto $x \underset{R_P}{\sim} x$ para toda $x \in X$.

(2) Supongamos que $x \underset{R_P}{\sim} y$. Entonces por la definición de $\underset{R_P}{\sim}$, existe $i \in I$ tal que $x, y \in X_i$, o lo que es lo mismo, $y, x \in X_i$ y por lo tanto $y \underset{R_P}{\sim} x$.

(3) Sean $x, y, z \in X$ y supongamos que $x \underset{R_P}{\sim} y$ y $y \underset{R_P}{\sim} z$. Entonces por la definición de $\underset{R_P}{\sim}$, existe $i \in I$ tal que $x, y \in X_i$ y existe $j \in I$ tal que $y, z \in X_j$, luego $y \in X_i \cap X_j$. Esto último implica que $i = j$, ya que para $i \neq j$, por ser $\{X_i\}_{i \in I}$ una partición de X, debe ser $X_i \cap X_j = \emptyset$. Entonces $x, z \in X_i$ y por lo tanto $x \underset{R_P}{\sim} z$. ∎

Nota 1.6.20. Es importante mencionar que puede haber más de un conjunto de representantes para una relación de equivalencia R en X y en este sentido se podrá pensar que la partición dada en el teorema 1.6.18 depende del conjunto de representantes dados. Sin embargo esto no es así pues si S y S' son dos conjunto de representantes y P_R y $\widehat{P}_R$ son las particiones correspondientes definidas en el teorema 1.6.18, se puede demostrar que son iguales (véase ejercicio 1.6.34) de tal manera que esta correspondencia define una función del conjunto de relaciones de equivalencia en X en el conjunto de particiones de X.

Si X es un conjunto no vacío, denotemos por

$$\mathscr{R} = \{\text{relaciones de equivalencia en } X\}$$

y por

$$\mathscr{P} = \{\text{particiones de } X\},$$

y sean $\mu : \mathscr{R} \longrightarrow \mathscr{P}$ y $\nu : \mathscr{P} \longrightarrow \mathscr{R}$ definidas, respectivamente, por $\mu(R) = P_R$, donde la partición P_R está definida como en el teorema 1.6.18 y $\nu(P) = R_P$, donde R_P está definida como en el teorema 1.6.19.

Teorema 1.6.21. *Sea X un conjunto no vacío, entonces las funciones $\mu : \mathscr{R} \longrightarrow \mathscr{P}$ y $\nu : \mathscr{P} \longrightarrow \mathscr{R}$ definidas por $\mu(R) = P_R$ y $\nu(P) = R_P$ satisfacen $\nu \circ \mu = 1_{\mathscr{R}}$ y $\mu \circ \nu = 1_{\mathscr{P}}$.*

Demostración.

$1^\circ/$ $\nu \circ \mu = 1_{\mathscr{R}}$.

Sea R una relación de equivalencia en X y S un conjunto completo de representantes.

Para mostrar que R_{P_R} y R son relaciones de equivalencia iguales, debemos ver que para cualesquiera $x, y \in X$, $(x, y) \in R$ si y sólo si $(x, y) \in R_{P_R}$ o usando la notación $\sim$, $x \underset{R}{\sim} y$ si y sólo si $x \underset{R_{P_R}}{\sim} y$.

Sea $x \in X$. Por ser S un conjunto completo de representantes, $x \in [a]$ para alguna $a \in S$. Entonces $x \underset{R}{\sim} y$ si y sólo si $x, y \in [a]$ y esto último es si y sólo si $x \underset{R_{P_R}}{\sim} y$. Luego $\nu \circ \mu = 1_{\mathscr{R}}$.

$2^\circ /$ $\mu \circ \nu = 1_{\mathscr{P}}$

Sea $P = \{X_i\}_{i \in I}$ una partición de X. Debemos demostrar que $P_{R_P} = P$.

$\subseteq$) Sea $[a]_{R_P} \in P_{R_P}$. Por un lado, puesto que P es una partición, dada $a \in X$, existe una $j \in I$ tal que $a \in X_j$. Mostraremos que $[a]_{R_P} = X_j$

$$x \in [a]_{R_P} \text{ si y sólo si } x \underset{R_P}{\sim} a$$
$$x \underset{R_P}{\sim} a \quad \text{si y sólo si } x \in X_j \text{ (porque } a \in X_j)$$

Por lo tanto $[a]_{R_P} = X_j \in P$. Con lo que se tiene $P_{R_P} \subseteq P$.

$\supseteq$) Ahora sean $X_j \in P$ y $a \in X_j$. Se sigue de la definición de R_P, $[a]_{R_P} = X_j$ y de aquí se tiene que $X_j \in P_{R_P}$. Por lo tanto $P \subseteq P_{R_P}$.

Concluímos entonces que $P_{R_P} = P$, es decir, $\mu \circ \nu = 1_{\mathscr{P}}$. ∎

Dada una relación de equivalencia R ($\sim$) en X, es usual denotar al conjunto P_R de clases de equivalencia por $\boldsymbol{X/R}$ ($\boldsymbol{X/\sim}$) y lo llamaremos el **conjunto cociente** de X respecto a R ($\sim$). Existe una función "natural", llamada **función canónica**, de X en X/R que asocia a cada elemento $a \in X$ su clase $[a]$.

Teorema 1.6.22. *Sea R una relación de equivalencia en X. La función canónica* $\varphi : X \longrightarrow X/R$ *definida por* $\varphi(a) = [a]_R$ *es suprayectiva. Además* $\varphi(a) = \varphi(b)$ *si y sólo si* $a \underset{R}{\sim} b$.

Demostración. Claramente φ es suprayectiva, pues si $[a]_R \in X/R$, $\varphi(a) = [a]$. Por otro lado $\varphi(a) = \varphi(b)$ si y sólo si $[a]_R = [b]_R$. Pero esta última igualdad se da, por el teorema 1.6.7, si y sólo si $a \underset{R}{\sim} b$. ∎

§ 1.7. Relaciones de orden

El tercer tipo de relación que introducimos en este capítulo es el de relación de orden en un conjunto.

Definición 1.7.1. *Sea X un conjunto y S una relación en X* ($S \subseteq X \times X$). *S se llama* ***orden parcial*** *en X si satisface*

(1) $(x, x) \notin S$ *para toda* $x \in X$,

(2) Si $(x, y) \in S$ *y* $(y, z) \in S$, *entonces* $(x, z) \in S$. *(propiedad transitiva)*

Así como usamos el símbolo $\sim$ para las relaciones de equivalencia, para un orden parcial usaremos el símbolo $<$. Esto es, si S es un orden parcial y $(a,b) \in S$, lo escribimos $\boldsymbol{a < b}$ y lo leemos "$\boldsymbol{a}$ **menor que** $\boldsymbol{b}$". En el caso en que $(a,b) \notin S$, escribiremos $a \not< b$.
Con esta nueva notación tenemos

$<$ es un orden parcial en X si y sólo si

$$\begin{cases} (1)\ a \not< a \text{ para toda } a \in X, \\ \\ (2)\ \text{Si } a < b \text{ y } b < c, \text{ entonces } a < c. \end{cases}$$

Si $<$ es un orden parcial en un conjunto X, diremos que $(X,<)$ es un ***conjunto parcialmente ordenado***.
Diremos que $\boldsymbol{x > y}$, $\boldsymbol{x}$ **es mayor que** $\boldsymbol{y}$, si $y < x$.

Definición 1.7.2*. Dado un orden parcial $<$ sobre un conjunto X y $x, y \in X$, diremos que x y y son comparables respecto a $<$, si $x < y$ o $y < x$ o $x = y$.*

Ejemplo 1.7.3. Sea $X = \{a,b\}$ donde $a \neq b$. $S = \{(a,b)\}$ es un orden parcial en X.

Ejemplo 1.7.4. Sea Y un conjunto y $X = \mathscr{P}(Y)$. El conjunto $S = \{(A,B) \in X \times X \mid A \subsetneq B\}$ es un orden parcial en X. En el caso en que se trabaje con una familia de conjuntos y el orden parcial esté dado a través de $\subsetneq$, lo denotamos directamente $(X,\subset)$ en alusión a que el orden parcial está definido por la inclusión. Más generalmente, dada cualquier familia de conjuntos X, $(X,\subset)$ es un conjunto parcialmente ordenado.

En un conjunto X se pueden tener definidos distintos órdenes parciales y si trabajamos en el conjunto con más de uno, deberemos denotarlos de manera distinta, por ejemplo, $<, <', <'', \ldots$ etc o bien $<_1, <_2, <_3, \ldots$ etc.
Existen ciertos tipos de órdenes parciales que aparecen con frecuencia en matemáticas y que son de gran interés.

Definición 1.7.5*. Un orden parcial $<$ en X se llama* ***total*** *(o lineal) si cualesquiera elementos $x, y \in X$ satisfacen una de las siguientes*

$$x < y, \quad x = y \quad \acute{o} \quad y < x,$$

y en este caso diremos que $(X,<)$ es un ***conjunto totalmente ordenado*** *o que $(X,<)$ es un conjunto linealmente ordenado.*

Esto es $<$ es total si cualesquiera dos elementos de X son comparables.

Lema 1.7.6. *Si $(X, <)$ es un conjunto totalmente ordenado, entonces cada pareja de elementos $x, y \in X$ satisface una y sólo una de las propiedades de la definición 1.7.5.*

Demostración. Suponer que se satisfacen al mismo tiempo cualesquiera dos de las propiedades de la definición 1.7.5, en cualquier caso esto nos lleva a que $x < x$, verifíquelo (ejercicio 1.7.9), lo que es imposible en un orden parcial. ∎

Ejemplo 1.7.7. El orden del ejemplo 1.7.3 es un orden total.

Ejemplo 1.7.8. El orden del ejemplo 1.7.4 en general no es total. Es más, el orden $\subset$ será total si y sólo si Y tiene a lo más un elemento (véase ejercicio 1.7.8). Más adelante, cuando se introduzcan los sistemas numéricos tendremos más ejemplos de orden total.

Sea $(X, <)$ un conjunto parcialmente ordenado. Por $\boldsymbol{x \leq y}$ entenderemos que $x < y$ o $x = y$ y es este caso se leerá "***x* es menor o igual a *y***".

Proposición 1.7.9. *Sea $(X, <)$ un conjunto parcialmente ordenado. Entonces*
(1) *$x \leq x$ para toda $x \in X$.*
(2) *Si $x \leq y$ y $y \leq x$, entonces $x = y$.* [2]
(3) *Si $x \leq y$ y $y \leq z$, entonces $x \leq z$.*

Demostración.

(1) Como $x = x$ para toda $x \in X$, por la definición de $\leq$, $x \leq x$ para toda $x \in X$.
(2) No puede suceder que $x \neq y$, ya que en este caso tendríamos que $x < y$ y $y < x$, que por ser $<$ un orden parcial, nos llevaría a que $x < x$ lo que es imposible. Por lo tanto debe ser $x = y$.
(3) Es inmediato por el hecho de que tanto $<$ como $=$ son transitivos. ∎

Por otro lado, cualquier relación en un conjunto X que satisfaga las propiedades de la proposición 1.7.9, induce un orden parcial en X.

Proposición 1.7.10. *Sea R una relación en el conjunto X que satisface:*
(1) $(x, x) \in R$,

[2] Se conoce como la propiedad antrisimétrica.

(2) *Si* $(x,y) \in R$ *y* $(y,x) \in R$, *entonces* $x = y$,
(3) *Si* $(x,y) \in R$ *y* $(y,z) \in R$, *entonces* $(x,z) \in R$.
Entonces R induce un orden parcial en X definido por: $x < y$ *si y sólo si* $(x,y) \in R$ *y* $x \neq y$.

Demostración. Es inmediata. ∎

Debido a las proposiciones 1.7.9 y 1.7.10, en un conjunto parcialmente ordenado, se puede trabajar indistintamente con $<$ o con $\leq$. Si se da una relación en X que satisfaga las propiedades de la proposición 1.7.10, sin ningún problema podemos usar la notación $\leq$, en el sentido de que $<$, definido como en la proposición 1.7.10, será un orden parcial, así pues podemos también decir que $(X, \leq)$ es un conjunto parcialmente ordenado. Esto es, si queremos dar un orden parcial, podemos hacerlo dando una relación que satisfaga la definición 1.7.1 o dando una relación que satisfaga las tres condiciones de la proposición 1.7.10, ya que, como hemos visto, cada una se obtiene de la otra.

Definición 1.7.11. *Sea* $(X, <)$ *un conjunto parcialmente ordenado y* $a \in X$.
(1) a se llama ***maximal (minimal)*** *en X si no existe* $x \in X$ *tal que*

$$a < x \ (x < a).$$

(2) a se llama ***máximo (mínimo)*** *en X si* $x \leq a$ $(a \leq x)$ *para todo* $x \in X$.

Un elemento que es máximo (mínimo), claramente es maximal (minimal). Sin embargo el inverso en general no es cierto, es decir, un elemento puede ser maximal (minimal) pero no máximo (mínimo). Un elemento máximo (mínimo) es comparable, mediante el orden, con todos los elementos del conjunto, mientras que un maximal (minimal) no necesariamente es comparable con todos los elementos del conjunto, es más, podría ser que no sea comparable con ningún elemento. Además un conjunto parcialmente ordenado puede tener varios maximales mientras que si un conjunto tiene máximo (mínimo), éste deberá ser único como lo muestra la siguiente

Proposición 1.7.12. *Si un conjunto parcialmente ordenado tiene máximo (mínimo), entonces es único.*

Demostración. Si $(X, <)$ es un conjunto parcialmente ordenado y x_0 y x_1 son máximos, entonces aplicando la definición, se tiene que $x \leq x_0$ para toda $x \in X$ y en particular $x_1 \leq x_0$. De la misma manera, como x_1 es máximo, se debe tener

que $x_0 \leq x_1$. Por lo tanto $x_0 = x_1$. Análogamente se demuestra la unicidad del mínimo. ∎

Ejemplo 1.7.13. Sea Y un conjunto con al menos dos elementos y sea $X = \mathscr{P}(Y) - \{Y\}$. Ya hemos visto que $(X, \subset)$ es un conjunto parcialmente ordenado. Sean $a, b \in Y$ con $a \neq b$ y sean $A = Y - \{a\}$ y $B = Y - \{b\}$. A y B son maximales en X pero no máximos pues $\{a\} \nsubseteq A$ y $\{b\} \nsubseteq B$. Evidentemente X no tiene máximo pero sí tiene mínimo que es $\varnothing$.

***Proposición 1.7.14**. En un conjunto totalmente ordenado un elemento es maximal (minimal) si y sólo si es máximo (mínimo).*

Demostración. Ya hemos comentado que un elemento máximo (mínimo) es maximal (minimal). Inversamente si un elemento a es maximal (minimal), como el conjunto es totalmente ordenado, entonces dado $x \in X$ se debe tener que $x \leq a$ ($a \leq x$) ya que cualesquiera dos elementos son comparables mediante el orden y por definición de maximal (minimal) no puede ser $a < x$ ($x < a$). Por lo tanto a es máximo (mínimo). ∎

***Definición 1.7.15**. Sea $(X, <)$ un conjunto parcialmente ordenado, $Y \subseteq X$ y $a \in X$. (1) a se llama **cota superior (inferior)** de Y en X si $y \leq a$ ($a \leq y$) para toda $y \in Y$. (2) Si el conjunto de las cotas superiores (inferiores) de Y en X tiene elemento mínimo (máximo) b, a b se le llama el **supremo (ínfimo)** de Y en X.*

En otras palabras, el supremo de un conjunto es la mínima cota superior y el ínfimo de un conjunto es la máxima cota inferior.
Un conjunto que tiene cota superior (inferior) se le llama ***acotado superiormente*** (***inferiormente***).

Ejemplo 1.7.16. Sea $X = \mathbb{Z}$ y $Y = \{x \in \mathbb{Z} \mid -5 \leq x < 5\}$. Y es un conjunto acotado superiormente e inferiormente: $y \in \mathbb{Z}$ es cota superior de Y si y sólo si $5 \leq y$ y $z \in \mathbb{Z}$ es cota inferior de Y si y sólo si $z \leq -5$ y en este caso 5 es e supremo de Y y -5 es el ínfimo de Y. Observe que 4 el máximo de Y y -5 es el mínimo de Y.

Ejemplo 1.7.17. Sea $A = \{x \in \mathbb{Z} \mid 0 \leq x \text{ y } x \text{ es par}\} \subseteq \mathbb{Z}$, A no está acotado superiormente pero sí inferiormente y el conjunto de cotas inferiores es $\{y \in \mathbb{Z} \mid y \leq 0\}$ y 0 es el ínfimo de A (que en este caso es mínimo porque pertenece al conjunto).

Definición 1.7.18. *Un orden parcial $<$ en X se llama* ***buen orden*** *si cada subconjunto no vacío de X tiene elemento mínimo y en este caso se dice que $(X, <)$ es un* ***conjunto bien ordenado***.

Más adelante cuando introduzcamos los números naturales con el orden, veremos que $(\mathbb{N}, <)$ es un conjunto bien ordenado.
El hecho de que cada subconjunto no vacío de un conjunto bien ordenado tenga mínimo, hace que este buen orden sea total.

Proposición 1.7.19. *Sea $<$ un orden parcial. Si $<$ es un buen orden en X, entonces $<$ es un orden total.*

Demostración. Debemos demostrar que cualesquiera dos elementos de X son comparables mediante el orden.
Sean $a, b \in X$ tales que $a \neq b$. El conjunto $A = \{a, b\}$ es un subconjunto no vacío de X y por ser $<$ un buen orden, entonces tiene mínimo que debe ser a o b, en cuyo caso $a \leq b$ o $b \leq a$,
respectivamente. ∎

§ 1.8. Sobre algunos axiomas de la teoría de conjuntos

La teoría de conjuntos se desarrolla partiendo de ciertos axiomas. Es a través de ellos que se construyen los conjuntos. Como ya hemos mencionado en el texto, hay que tener cuidado cuando se quiere construir un conjunto pues el resultado puede que no lo sea. La teoría de conjuntos fue desarrollada por Cantor a fines del siglo XIX. Sin embargo el aceptar que una colección de objetos definidos mediante una propiedad es un conjunto llevó a contradicciones. La famosa **paradoja de Russel** es un un ejemplo de esto: Sea U el conjunto de aquellos conjuntos que no se pertenecen a sí mismos, es decir, $U = \{x \mid x \notin x\}$. Luego

$$\forall x \; x \in U \Leftrightarrow x \notin x.$$

Considerando $x = U$ y al preguntarnos si U es un elemento de sí mismo, obtenemos

$$U \in U \Leftrightarrow U \notin U$$

lo cual es un absurdo.
Para evitar estas contradicciones Ernest Zermelo presentó un sistema axiomático donde la paradoja de Russel no tiene cabida. Concretamente el axioma de especificación dice lo siguiente:

> **Axioma de especificación**. *Dado un conjunto X y una proposición $p(x)$, la colección*
>
> $$A = \{x \in X \mid p(x) \text{ es verdadera}\}$$
>
> *es un conjunto.*

Teorema 1.8.1. *No existe un conjunto que tenga como sus elementos a todos los conjuntos*

Demostración. Supongamos que existe un conjunto $\mathscr{U}$ tal que $A \in \mathscr{U}$ para cualquier conjunto A. Usando el axioma de especificación construimos el siguiente conjunto:

$$\mathscr{C} = \{x \in \mathscr{U} \mid x \notin x\}.$$

Entonces por el axioma de especificación, $\mathscr{C} \in \mathscr{U}$. Debe ser verdadera una de las siguientes dos afirmaciones $\mathscr{C} \in \mathscr{C}$ o $\mathscr{C} \notin \mathscr{C}$. Sin embargo ninguna de ellas lo es ya que

(1) Si $\mathscr{C} \in \mathscr{C}$, por la definición de $\mathscr{C}$, tendríamos que $\mathscr{C} \notin \mathscr{C}$.
(2) Si $\mathscr{C} \notin \mathscr{C}$, como $\mathscr{C} \in \mathscr{U}$, entonces $\mathscr{C} \in \mathscr{C}$.

Como en ambos casos llegamos a una contradicción concluimos que $\mathscr{U}$ no puede ser un conjunto. ∎

Otra manera de enunciar el teorema 1.8.1 es

Teorema 1.8.2. *Dado un conjunto X, existe un conjunto A tal que $A \notin X$.*

Es importante mencionar otro de los axiomas de la teoría de conjuntos; el llamado *axioma de elección*. En este usamos nuevamente $\bigcup_{i \in I} A_i$ (véase definición 1.8.3).

> **Axioma de elección**. *Dada una familia no vacía de conjuntos no vacíos $\{A_i\}_{i \in I}$ existe una función*
>
> $$\varphi : \{A_i\}_{i \in I} \to \bigcup_{i \in I} A_i$$
>
> *tal que $\varphi(A_i) \in A_i$ para todo $i \in I$.*

A cualquier función como la mencionada en el axioma de elección se le llama una **función de selección** para la familia $\{A_i\}_{i \in I}$ y lo que está diciendo este axioma es que dada una familia no vacía de conjuntos no vacíos, podemos tomar simultáneamente un elemento de cada uno de los conjuntos que pertenece a la familia. En realidad ya hemos usado este axioma, un ejemplo de esto se puede ver cuando consideramos un conjunto completo de representantes (véase definición 6.10).

Ahí tomamos un elemento por cada clase de equivalencia. Más concretamente dada una relación de equivalencia R en X y P el conjunto de sus clases de equivalencia, si indicamos los elementos de P mediante una función biyectiva $f : I \to P$, esto es $P = \{A_i\}_{i\in I}$, un conjunto completo de representantes será una función de selección $\varphi : P = \{A_i\}_{i\in I} \to \bigcup_{i\in I} A_i$ ya que para cada $i \in I$, $\varphi(A_i) \in A_i$, esto es, estamos determinando un elemento y sólo uno por cada clase de equivalencia.
Sea $f : X \longrightarrow Y$ una función suprayectiva. Para construir un inverso derecho de f, consideramos, para cada $y \in Y$, el conjunto $f^{-1}(y) = f^{-1}(\{y\})$ que sabemos es no vacío. Tomamos la familia no vacía de conjuntos $\{f^{-1}(y)\}_{y\in Y}$ (lo estamos indicando a través de Y), existe una función $\varphi : \left\{ f^{-1}(y) \right\}_{y\in Y} \longrightarrow \bigcup_{y\in Y} f^{-1}(y)$ tal que $\varphi\left(f^{-1}(y)\right) \in f^{-1}(y)$. Si denotamos a este elemento por x_y, tendremos, entonces que $f(x_y) = y$.

§ §1.8.1. Operaciones con una familia arbitraria de conjuntos

Otro ejemplo donde usamos el axioma de elección es el siguiente:
Las definiciones de unión e intersección de dos conjuntos pueden extenderse a cualquier familia de conjuntos:

Definición 1.8.3*. Sea $\{A_i\}_{i\in I}$ una familia arbitraria de conjuntos. La unión $\bigcup_{i\in I} A_i$ de $\{A_i\}_{i\in I}$ es el conjunto*

$$\bigcup_{i\in I} A_i = \left\{ x \mid x \in A_i \text{ para alguna } i \in I \right\}.$$

Definición 1.8.4*. Sea $\{A_i\}_{i\in I}$ una familia arbitraria no vacía de conjuntos. La intersección $\bigcap_{i\in I} A_i$ de $\{A_i\}_{i\in I}$ es el conjunto*

$$\bigcap_{i\in I} A_i = \left\{ x \mid x \in A_i \text{ para todo } i \in I \right\}.$$

Luego, según la definiciones tenemos que

$$(1)\ x \in \bigcup_{i\in I} A_i \iff \exists i \in I \text{ tal que } x \in A_i.$$

$$(2)\ x \in \bigcap_{i\in I} A_i \iff \forall i \in I\ x \in A_i.$$

De aquí tenemos que

$$(1)\ x \notin \bigcup_{i\in I} A_i \iff \forall i \in I\ (x \notin A_i).$$

$$(2)\ x \notin \bigcap_{i\in I} A_i \iff \exists i \in I\ \ (x \notin A_i).$$

Nota 1.8.5. La razón por la cual, en la intersección, se pide que la familia $\{A_i\}_{i\in I}$ sea no vacía es por lo siguiente: si fuera $I = \varnothing$, entonces cada conjunto B pertenecería a $\bigcap_{i\in I} A_i$ puesto que si existiera B tal que $B \notin \bigcap_{i\in I} A_i$, esto significa que existe A_i para algún $i \in I$ tal que $B \notin A_i$, lo cual es imposible porque $I = \varnothing$. Conclusión: cada conjunto B debe pertenecer a $\bigcap_{i\in I} A_i$ cuando $I = \varnothing$, sin embargo ya hemos visto que no existe un conjunto que contenga a todos los conjuntos (véase teorema 1.8.1).

Teorema 1.8.6. *Sea $\{A_i\}_{i\in I}$ es una familia de conjuntos. Entonces*

(1) $A_j \subseteq \bigcup_{i\in I} A_i$ *para toda* $j \in I$.
(2) Si $I \neq \varnothing$, *entonces* $\bigcap_{i\in I} A_i \subseteq A_j$ *para toda* $j \in I$.

La demostración queda como ejercicio. (véase ejercicio 1.8.1)

Teorema 1.8.7. *Sea $\{A_i\}_{i\in I}$ una familia de conjuntos y X cualquier conjunto. Entonces*

(1) $X \cap \left(\bigcup_{i\in I} A_i\right) = \bigcup_{i\in I}(X \cap A_i)$.
(2) $X - \left(\bigcup_{i\in I} A_i\right) = \bigcap_{i\in I}(X - A_i)$, *donde* $I \neq \varnothing$.

Demostración.

(1) $X \cap \left(\bigcup_{i\in I} A_i\right) \subseteq \bigcup_{i\in I}(X \cap A_i)$.

$\subseteq)$ $x \in X \cap \left(\bigcup_{i\in I} A_i\right)$ implica que $x \in X$ y $x \in \bigcup_{i\in I} A_i$. Como $x \in \bigcup_{i\in I} A_i$, entonces $x \in A_j$ para alguna $j \in I$. Luego $x \in X \cap A_j$ y por ser $\left(X \cap A_j\right) \subseteq \bigcup_{i\in I}(X \cap A_i)$ (teorema 1.8.6) se tiene que $x \in \bigcup_{i\in I}(X \cap A_i)$.

$X \cap \left(\bigcup_{i\in I} A_i\right) \supseteq \bigcup_{i\in I}(X \cap A_i)$.

$\supseteq)$ $x \in \bigcup_{i\in I}(X \cap A_i)$ implica que $x \in X \cap A_j$ para alguna $j \in I$ y por lo tanto $x \in X$ y $x \in A_j$. Como $x \in A_j$ para alguna $j \in I$, entonces $x \in \bigcup_{i\in I} A_i$ y de aquí se tiene que $x \in X \cap \left(\bigcup_{i\in I} A_i\right)$.

Por lo tanto $X \cap \left(\bigcup_{i\in I} A_i\right) = \bigcup_{i\in I}(X \cap A_i)$.

(2) $X - \left(\bigcup_{i\in I} A_i\right) \subseteq \bigcap_{i\in I}(X - A_i)$.

$\subseteq)$ $x \in X - \left(\bigcup_{i\in I} A_i\right)$ implica que $x \in X$ y $x \notin \bigcup_{i\in I} A_i$. Pero si $x \notin \bigcup_{i\in I} A_i$, entonces $x \notin A_i$ para toda $i \in I$ y de aquí, $x \in X - A_i$ para toda $i \in I$. Lo que significa que $x \in \bigcap_{i\in I}(X - A_i)$.

$X - \left(\bigcup_{i\in I} A_i\right) \supseteq \bigcap_{i\in I}(X - A_i)$.

$\supseteq)$ $x \in \bigcap_{i\in I}(X - A_i)$ implica que $x \in (X - A_i)$ para toda $i \in I$, lo que a su vez implica que $x \in X$ y $x \notin A_i$ para toda $i \in I$. Pero si $x \notin A_i$ para toda $i \in I$, entonces $x \notin \bigcup_{i\in I} A_i$.

Luego $x \in X - \left(\bigcup_{i\in I} A_i\right)$.

Por lo tanto $X - \left(\bigcup_{i\in I} A_i\right) = \bigcap_{i\in I}(X - A_i)$. ∎

Teorema 1.8.8. *Sean $\{A_i\}_{i\in I}$ una familia no vacía de conjuntos y X un conjunto. Entonces*

(1) $X \cup \left(\bigcap_{i\in I} A_i\right) = \bigcap_{i\in I}(X \cup A_i)$.

(2) $X - \left(\bigcap_{i\in I} A_i\right) = \bigcup_{i\in I}(X - A_i)$.

Demostración.

(1) $X \cup \left(\bigcap_{i\in I} A_i\right) \subseteq \bigcap_{i\in I}(X \cup A_i)$.

$\subseteq)$ $x \in X \cup \left(\bigcap_{i\in I} A_i\right)$ implica que $x \in X$ o $x \in \bigcap_{i\in I} A_i$.

i) Si $x \in X$, se tiene que $x \in X \cup A_i$ para toda $i \in I$ y por lo tanto $x \in \bigcap_{i\in I}(X \cup A_i)$.

ii) Si $x \in \bigcap_{i\in I} A_i$, se tiene que $x \in A_i$ para toda $i \in I$ y por lo tanto $x \in X \cup A_i$ para toda $i \in I$. Luego $x \in \bigcap_{i\in I}(X \cup A_i)$.

$X \cup \left(\bigcap_{i\in I} A_i\right) \supseteq \bigcap_{i\in I}(X \cup A_i)$.

$\supseteq$) $x \in \bigcap_{i\in I}(X \cup A_i)$ implica que $x \in X \cup A_i$ para toda $i \in I$. Pueden suceder dos casos; $x \in X$ o $x \notin X$.

i) Si $x \in X$, entonces $x \in X \cup \left(\bigcap_{i\in I} A_i\right)$.

ii) En el caso en que $x \notin X$, como $x \in X \cup A_i$ para todo $i \in I$, entonces se debe tener $x \in A_i$ para toda $i \in I$ y por lo tanto $x \in \bigcap_{i\in I} A_i$ y de aquí se tiene que $x \in X \cup \left(\bigcap_{i\in I} A_i\right)$.

Por lo tanto $X \cup \left(\bigcap_{i\in I} A_i\right) = \bigcap_{i\in I}(X \cup A_i)$.

(2) $X - \left(\bigcap_{i\in I} A_i\right) \subseteq \bigcup_{i\in I}(X - A_i)$.

$\subseteq$) $x \in X - \left(\bigcap_{i\in I} A_i\right)$ implica que $x \in X$ y $x \notin \bigcap_{i\in I} A_i$. Pero $x \notin \bigcap_{i\in I} A_i$ significa que $x \notin A_j$ para algún $j \in I$ lo que significa que para esta $j \in I$, $x \in X - A_j$ y esto último implica que $x \in \bigcup_{i\in I}(X - A_i)$.

$X - \left(\bigcap_{i\in I} A_i\right) \supseteq \bigcup_{i\in I}(X - A_i)$.

$\supseteq$) $x \in \bigcup_{i\in I}(X - A_i)$ implica que $x \in X - A_j$ para alguna $j \in I$ y entonces $x \in X$ y $x \notin A_j$. Pero si $x \notin A_j$ para alguna $j \in I$, entonces $x \notin \bigcap_{i\in I} A_i$ y así $x \in X - \left(\bigcap_{i\in I} A_i\right)$.

Por lo tanto $X - \left(\bigcap_{i\in I} A_i\right) = \bigcup_{i\in I}(X - A_i)$. ∎

Pasaremos ahora a la definición del producto cartesiano de una familia arbitraria no vacía de conjuntos. Si nos fijamos en las definiciones de unión e intersección

de una familia arbitraria de conjuntos que acabamos de dar, podemos observar que cuando la familia consta únicamente de dos conjuntos, la unión e intersección de ellos coincide plenamente con la que hemos dado en la sección 2. Sin embargo, la definición que daremos para el producto cartesiano de una familia arbitraria no vacía de conjuntos difiere de la que dimos anteriormente en la sección 2, en el sentido de que si la familia dada contiene únicamente dos conjuntos, el producto cartesiano de ellos que resulta usando esta nueva definición no coincide formalmente con la dada en la sección 2. No obstante se pueden identificar ambos conjuntos mediante una función biyectiva que resulta bastante natural.

Definición 1.8.9. *Dada una familia no vacía de conjuntos* $\{A_i\}_{i\in I}$*, su producto cartesiano, denotado por* $\bigtimes_{i\in I} A_i$*, es el conjunto*

$$\bigtimes_{i\in I} A_i = \left\{ f : \{A_i\}_{i\in I} \longrightarrow \bigcup_{i\in I} A_i \mid f(A_i) \in A_i \text{ para toda } i \in I \right\}.$$

Esto es, $\bigtimes_{i\in I} A_i$ es el conjunto de funciones de selección para la familia $\{A_i\}_{i\in I}$.
Es claro que si $A_i = \varnothing$ para algún $i \in I$, $\bigtimes_{i\in I} A_i = \varnothing$.
Teniendo en cuenta el axioma de elección obtenemos el siguiente

Teorema 1.8.10. *Si* $\{A_i\}_{i\in I}$ *es una familia no vacía de conjuntos no vacíos, entonces* $\bigtimes_{i\in I} A_i \neq \varnothing$.

Demostración. Por el axioma de elección, existe al menos una función de selección y por to tanto $\bigtimes_{i\in I} A_i \neq \varnothing$. ∎

En las condiciones del Teorema 1.8.10, es claro que los elementos de $\bigtimes_{i\in I} A_i$ son las funciones de selección y en realidad este último teorema es equivalente al axioma de elección y como cada función $f \in \bigtimes_{i\in I} A_i$ queda determinada por los valores que toma en cada A_i ($i \in I$), a f la podemos denotar por $(a_i)_{i\in I}$, donde $f(A_i) = a_i$ para toda $i \in I$ y con esta notación se tiene que dados $(a_i)_{i\in I}, (b_i)_{i\in I} \in \bigtimes_{i\in I} A_i$ $(a_i)_{i\in I} = (b_i)_{i\in I}$ si y sólo si $a_i = b_i$ para toda $i \in I$.

§§ Ejercicios sección 1.1.

1.1.1. Demuestre el teorema 1.1.11. (pág. 22.)

1.1.2. Encuentre una proposición adecuada para describir a cada uno de los siguientes conjuntos.

(1) $A = \{0, 2, 4, 6, 8, 10\}$
(2) $B = \{1, 3, 5, 7, 9, 11\}$
(3) $C = \{30, 31, 32, \ldots\}$
(4) $D = \{1, 4, 9, 16, 25, 36, \ldots\}$
(5) $E = \{-1, 2, -3, 4, -5, 6, -7, \ldots\}$
(6) $F = \{-1, 3, -5, 7, -9, 11, \ldots\}$
(7) $G = \{\frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \frac{1}{6}, \ldots\}$

1.1.3. Describa los siguientes conjuntos listando todos sus elementos.

(1) $\{x \in \mathbb{Z} \mid x^2 + x = 6\}$
(2) $\{n + \frac{1}{n} \mid n \in \{1, 2, 3, 5, 7\}\}$
(3) $\{x \in \mathbb{N} \mid x \text{ es número par y } x^2 \leq 50\}$
(4) $\{1 + (-1)^n \mid n \in \mathbb{N}\}$
(5) $\{x \in \mathbb{N} \mid x^2 - 3x = 0\}$
(6) $\{n^3 + n^2 \mid n \in \{0, 1, 2, 3, 4\}\}$
(7) $\{\frac{1}{n^2+n} \mid n \text{ es un entero positivo impar y } n \in \{1, 2, 3, 5, 7\}\}$

1.1.4. Determine cuáles de los siguientes conjuntos son iguales.

1) $A = \{c, e, r, o\}$ 2) $B = \{1, 2, 3\}$
3) $C = \{a, r, o, m, a\}$ 4) $D = \{5, 2, 3, 4, 5\}$
5) $E = \{x \in \mathbb{N} \mid 1 < x \leq 5\}$ 6) $F = \{x \in \mathbb{Z} \mid x^2 + 1 = 0\}$
7) $G = \{1, 2, 2\}$ 8) $H = \{e, s, p, o, n, j, a\}$
9) $I = \{1, 2, 2, 3\}$ 10) $J = \{x \in \mathbb{N} \mid x^2 + 2 = 3x\}$
11) $K = \{0\}$ 12) $L = \{a, m, o, r\}$
13) $M = \{j, a, p, o, n, e, s\}$ 14) $N = \varnothing$

1.1.5. Si $A = \{x \in \mathbb{Z} \mid \exists y \in \mathbb{Z}(x = 2y)\}$ y $B = \{a \in \mathbb{Z} \mid \exists b, c \in \mathbb{Z}(a = 6b + 10c)\}$, demuestre que $A = B$.

1.1.6. Demuestre que:

(*a*) $x \in A$ si y sólo si $\{x\} \subseteq A$.
(*b*) $A \subseteq \varnothing$ si y sólo si $A = \varnothing$.
(*c*) Si $A \neq \varnothing$ entonces $\varnothing \subsetneq A$.
(*d*) $\{a\} = \{b, c\}$ si y sólo si $a = b = c$.
(*e*) Si $\{c, a\} = \{c, b\}$ entonces $a = b$.
(*f*) Si $A \subseteq B$, $B \subseteq C$ y $C \subseteq A$, entonces $A = B = C$.

1.1.7. Demuestre la verdad o falsedad (con un contraejemplo) de los siguientes enunciados:

(*a*) Si $A \subseteq B$ y $B \not\subseteq C$ entonces $A \not\subseteq C$.
(*b*) Si $A \notin B$ y $B \notin C$ entonces $A \notin C$.
(*c*) Si $A \neq B$ y $B \neq C$ entonces $A \neq C$.
(*d*) Si $A \in B$ y $B \not\subseteq C$ entonces $A \notin C$.
(*e*) Si $A \subsetneq B$ y $B \subseteq C$ entonces $A \not\subseteq C$.
(*f*) Si $A \subseteq B$ y $B \in C$ entonces $A \notin C$.
(*g*) Si $A \not\subseteq B$ y $B \not\subseteq C$ entonces $A \not\subseteq C$.

1.1.8.

(1) Dé un ejemplo de tres conjuntos A, B y C tales que $A \in B$ y $B \in C$ pero $A \notin C$
(2) Dé un ejemplo de conjuntos A, B, C, D y E que satisfacen simultáneamente la siguiente condición: $A \subsetneq B$, $B \in C$, $C \subsetneq D$ y $D \subsetneq E$.

1.1.9. Sea $A = \{1, 2, \{2\}\}$. ¿Cuáles de las siguientes proposiciones son verdaderas y cuáles falsas?

1) $1 \in A$. 2) $\{1\} \in A$. 3) $\{1\} \subseteq A$. 4) $\{\{1\}\} \subseteq A$. 5) $\{2\} \in A$.
6) $\{2\} \subseteq A$. 7) $\{\{2\}\} \subseteq A$. 8) $\{\{2\}\} \subsetneq A$.

1.1.10. ¿Cuáles de las siguientes proposiciones son verdaderas y cuáles falsas? Justifique cada una de sus respuestas.

1) $\varnothing \in \varnothing$. 2) $\varnothing \notin \varnothing$. 3) $\varnothing \subseteq \varnothing$.
4) $\varnothing \subsetneq \varnothing$. 5) $\varnothing \in \{\varnothing\}$. 6) $\varnothing \notin \{\varnothing\}$.
7) $\varnothing \subsetneq \{\varnothing\}$. 8) $\varnothing \subseteq \{\varnothing\}$. 9) $\varnothing = \{\{\varnothing\}\}$.
10) $\{\{\varnothing\}\} \subseteq \{\{\varnothing\}, \varnothing\}$. 11) $\varnothing = \{0\}$. 12) $\{\{\varnothing\}, \varnothing\} \subseteq \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}\}$.
13)$\{\{\varnothing\}, \varnothing\} \in \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}\}$.

1.1.11. Considere los siguientes conjuntos:
$P = \{r, s, t, u, v, w\}$; $Q = \{u, v, w, x, y, z\}$; $R = \{s, u, y, z\}$;
$S = \{u, v\}$; $T = \varnothing$.
Determine cuál de estos conjuntos:

(1) es subconjunto de P y de Q únicamente.
(2) es subconjunto de R pero no de Q.
(3) no es subconjunto de P ni de R.
(4) no es subconjunto de R pero si de Q.
(5) es subconjunto de todos.

1. 1.12. Dé un ejemplo de un conjunto X con más de dos elementos y con la propiedad de que todo elemento de X es subconjunto de X.

1.1.13. Para el conjunto $A = \{1, 2, 3, 4\}$ determine

(1) los subconjuntos que no tienen ningún elemento.
(2) los subconjuntos que tienen un único elemento.
(3) los subconjuntos que tienen dos elementos.
(4) los subconjuntos que tienen tres elementos.
(5) los subconjuntos que tienen cuatro elementos.
(6) los subconjuntos que tienen cinco elementos.

¿Cuántos subconjuntos tiene A? ¿Cuántos subconjuntos propios tiene A?

1.1.14. Sea $X = \{1, \{1\}, 2, \{1, 2\}\}$.

(1) Determine todos los subconjuntos A de X tales que: $\{1\} \subseteq A$ y $\{1\} \in A$.
(2) Determine todos los subconjuntos B de X tales que: $2 \notin B$ y $\{1, 2\} \in B$.
(3) Determine todos los subconjuntos C de X tales que: $\{1, 2\} \subsetneq C$.
(4) Determine todos los subconjuntos D de X tales que: $\{1, 2\} \nsubseteq D$ y $\{1\} \in D$.

§ § Ejercicios sección 1.2.

1. 2.1. Considere los siguientes conjuntos $A = \{a, b, c, d, 1, 2, 5\}$, $B = \{a, c, 1, 3\}$, $C = \{a, b, c\}$, $D = \{b, c, d, 1, 2\}$ y $E = \{c, d\}$. Realice las siguientes operaciones:

1) $A \cap B$	2) $C \cup B$	3) $C \cup D$
4) $A \cap C$	5) $A \cap C$	6) $A - B$
7) $B - D$	8) $(A - B) \cap (B - D)$	9) $(A - B) \cap D$
10) $B \cup (C \cap D)$	11) $C \cap (B \cup D)$	12) $[C \cap (A - D)] \cup B$
13) $[(A - B) \cup (A - C)] \cup D$	14) $[A - (D \cup (B - C))] \cap C$	15) $[C \cap (A - D)] \cup B$
16) $[C - (D \cap (B - C))] \cup (A - D)$	17) $\mathscr{P}(C) - \mathscr{P}(E)$	18) $\mathscr{P}(C - E)$
19) $B \times C$	20) $(B \cap D) \times C$	

1.2.2. Sean $A = \{1, 2, a, c\}$, $B = \{2, 3, 4, a, b\}$ y $C = \{1, a\}$. ¿Cuáles de las siguientes proposiciones son verdaderas y cuáles falsas?

1) $c \in A \cup B$	2) $2 \in A \cap B$	3) $\{3, a\} \subseteq A \cup B$	4) $\{3, a\} \nsubseteq A \cup C$
5) $\{a, c\} \nsubseteq A \cup B$	6) $a \notin A - B$	7) $\{4, b\} \subseteq B - A$	8) $\{1, 3, a\} \in \mathscr{P}(B \cup C)$
9) $\{a, c\} \in \mathscr{P}(A)$	10) $\{\varnothing\} \subseteq \mathscr{P}(C)$		

1.2.3. Sean A y B conjuntos. Demuestre $A \cup (A \cap B) = A$ y $A \cap (A \cup B) = A$.

1.2.4. Si $A \cup B = A \cup C$ ¿Es cierto que $B = C$? Justifique se respuesta.

1.2.5. [3] Sean A, B conjuntos. Demuestre que $A \cup B = B \cup A$.

1.2.6. [4] Sean A, B conjuntos. Demuestre que

(1) $A \cap B \subseteq A$; $A \cap B \subseteq B$.
(2) $A \cap A = A$.
(3) $A \cap B = B \cap A$.

1.2.7. [5] Sean A, B y C conjuntos. Demuestre que

(1) Si $A \subseteq B$, entonces $A \cap C \subseteq B \cap C$ para cualquier conjunto C.
(2) Si $C \subseteq A$ y $C \subseteq B$, entonces $C \subseteq A \cap B$.

1.2.8. [6] Sean A, B y C conjuntos. Demuestre que $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

1.2.9. [7] Sean A, B y C conjuntos. Demuestre que $C = A \cap B$ si y sólo si C satisface las siguientes dos condiciones

(i) $C \subseteq A$ y $C \subseteq B$.
(ii) Si D es un conjunto tal que $D \subseteq A$ y $D \subseteq B$, entonces $D \subseteq C$.

1.2.10. [8] Sean A y B conjuntos. Demuestre que

(1) $A - A = \varnothing$; $A - \varnothing = A$.
(2) $A - B \subseteq A$.

1.2.11. [9] Sean A y B conjuntos. Entonces $A - (B \cap C) = (A - B) \cup (A - C)$.

1.2.12. Sean A, B, C y D conjuntos tales que $A \subseteq B$ y $C \subseteq D$. Demuestre que $A \cup C \subseteq B \cup D$ y que $A \cap C \subseteq B \cap D$.

1.2.13. Sean A, B y C conjuntos tales que $A \subseteq B$. Demuestre que $A - C \subseteq B - C$.

1.2.14. Demuestre que $A \cap B = (A \cup B) - [(A - B) \cup (B - A)]$.

1.2.15. Sean A, B y C conjuntos. Demuestre que

(1) $A - B = A - (A \cap B)$.

---

[3] Parte del teorema 1.2.4 pág. 25.
[4] Parte del teorema 1.2.8 pág. 27.
[5] Parte del teorema 1.2.9 pág. 28.
[6] Parte del teorema 1.2.10 pág. 28.
[7] Parte del teorema 1.2.11. pág. 29
[8] Parte del teorema 1.2.15 pág. 31
[9] Parte del teorema 1.2.18 pág. 32

(2) $A - B = (A \cup B) - B$.
(3) $A = (A \cap B) \cup (A - B)$.
(4) $A \cap (B - C) = (A \cap B) \cup C$.
(5) $(A \cap B) - C = (A - C) \cap (B - C)$.
(6) $(A \cup B) - C = (A - C) \cup (B - C)$.
(7) $(A - B) - C = (A - C) - (B - C)$.
(8) $A - (B - C) = (A - B) \cup (A \cap C)$.
(9) $A - (B - C) = (A - B) \cup (A \cap C)$.
(10) $(A - C) - (B - C) = (A - B) - C$.
(11) $(A - B) - (A - C) = A \cup (B - C)$.
(12) $A - (B - C) \supseteq (A - B) - C$.

1.2.16. Sean A y B conjuntos. Demuestre que

(1) si $A \subseteq B$, entonces $(A - C) \subseteq (B - C)$. ¿Es cierta la igualdad?
(2) si $A \subseteq B$, entonces $(C - B) \subseteq (C - A)$. ¿Es cierta la igualdad?

1.2.17. Sean conjuntos A, B, C. Demuestre que $(A-B) \subseteq C$ si y sólo si $(A-C) \subseteq B$.

1.2.18. Sean A, B y C conjuntos. Demuestre lo siguiente:

(1) Si $A \cup B = \emptyset$, entonces $A = \emptyset$ y $B = \emptyset$.
(2) $A = B$ si y sólo si $A \cap B = A \cup B$.
(3) $A = B$ si y sólo si $C \cap A = C \cap B$ y $C \cup A = C \cup B$.
(4) $A - (B - C) = (A - B) - C$ si y sólo si $A \cap C = \emptyset$.

1.2.19. ¿Existen conjuntos A, B y C tales que $A \cap B \neq \emptyset$, $A \cap C = \emptyset$ y $(A \cap B) - C = \emptyset$?

1.2.20. Sean $A, B \subseteq X$. Considérese A^c y B^c los complementos relativos de A y B en X, respectivamente. Demuestre lo siguiente:

(1) $(A^c)^c = A$.
(2) $A \cup A^c = X$ y $A \cap A^c = \emptyset$.
(3) $A - B = A \cap B^c$.
(4) $A \subseteq B$ si y sólo si $B^c \subseteq A^c$.
(5) $A = B$ si y sólo si $B^c = A^c$.
(6) $A = (A \cap B) \cup (A \cap B^c)$.
(7) $A \cup B = X$ si y sólo si $A^c \subseteq B$.
(8) $A \subseteq B^c$ si y sólo si $A \cap B = \emptyset$.
(9) $A \cup B = X$ y $A \cap B = \emptyset$ si y sólo si $B = A^c$.

(10) $A^c - B^c = A - B$.
(11) Si $A^c \subsetneq B$, entonces $A \cap B \neq \emptyset$. ¿Es cierto el recíproco?
(12) Si $B \subsetneq A^c$, entonces $A \cup B \neq X$.

1.2.21. Proporcione la justificación (a partir del ejercicio 2.20 y de las operaciones de la teoría de conjuntos) de los pasos necesarios para simplificar el conjunto $(A \cap B) \cup [B \cap ((C \cap D) \cup (C \cap D^c))]$ donde $A, B, C, D \subseteq X$.

$$\begin{aligned}(A \cap B) \cup [B \cap ((C \cap D) \cup (C \cap D^c))] &= (A \cap B) \cup [B \cap (C \cap (D \cup D^c))] \\ &= (A \cap B) \cup [B \cap (C \cap X)] \\ &= (A \cap B) \cup (B \cap C) \\ &= (B \cap A) \cup (B \cap C) \\ &= B \cap (A \cup C)\end{aligned}$$

1.2.22. Utilice el ejercicio 2.20 y las reglas de esta sección para simplificar las siguientes expresiones:

(1) $A \cap (B - A)$
(2) $(A \cap B) \cup (A \cap B \cap C^c \cap D) \cup (A^c \cap B)$
(3) $(A - B) \cup (A \cap B)$
(4) $A^c \cup B^c \cup (A \cap B \cap D^c)$
(5) $A^c \cup (A \cap B^c) \cup (A \cap B \cap C^c) \cup (A \cap B \cap C \cap D^c)$
(6) $[(A \cup B \cup C) \cap (A \cup B)] - [(A \cup (B - C)) \cap A]$

1.2.23. Sean $A, B \subseteq X$. Exprese $(A - B)^c$ en términos de $\cup$ y $-$.

1.2.24. Dé un contraejemplo para demostrar la falsedad de los siguientes enunciados:

(1) $A \subseteq A \cap B$.
(2) $A \cup B \subseteq A$.
(3) $A \subseteq B \cup C \implies [(A \subseteq B) \vee (A \subseteq C)]$.
(4) $B \cap C \subseteq A \implies [(B \subseteq A) \vee (C \subseteq A)]$.
(5) $A - (B - C) \subseteq (A - B) - C$.
(6) $A - B = B - A$.
(7) $A \cup C \subseteq B \cup C \implies A \subseteq B$.
(8) $A \cap C \subseteq B \cap C \implies A \subseteq B$.
(9) $A = C - B \implies (A \cap B = \emptyset \wedge A \cup B = C)$.
(10) $\mathscr{P}(A \cup B) \subseteq \mathscr{P}(A) \cup \mathscr{P}(B)$.

1.2.25. Demuestre lo siguiente:

(*a*) $A \subseteq B \iff \mathscr{P}(A) \subseteq \mathscr{P}(B)$.
(*b*) $A = B \iff \mathscr{P}(A) = \mathscr{P}(B)$.
(*c*) $\mathscr{P}(A \cap B) = \mathscr{P}(A) \cap \mathscr{P}(B)$.
(*d*) $A \cap B = \varnothing \implies \mathscr{P}(A - B) = \mathscr{P}(A) - \mathscr{P}(B)$ si $B \neq \varnothing$.
(*e*) $\mathscr{P}(A \cup B) = \mathscr{P}(A) \cap \mathscr{P}(B) \implies A = B$.
(*f*) $\mathscr{P}(A \cap B) = \mathscr{P}(A) \cup \mathscr{P}(B) \implies A = B$.

Definición. Si A y B son conjuntos se define la **diferencia simétrica** de A y B, denotada como $\boldsymbol{A \bigtriangleup B}$, por

$$A \bigtriangleup B = (A - B) \cup (B - A).$$

1.2.26. Sean A y B conjuntos. Demuestre que $A \bigtriangleup B = (A \cup B) - (A \cap B)$.

1. 2.27. Para los conjuntos $A = \{1, 2, 3, 4\}$, $B = \{2, 4, a, b\}$ y $C = \{a, \{c\}, 1, 5\}$ encontrar:
(1) $A \bigtriangleup B$
(2) $B \bigtriangleup C$
(3) $A \cap (B \bigtriangleup C)$
(4) $B \bigtriangleup A$
(5) $A \bigtriangleup A$
(6) $A \bigtriangleup (B \bigtriangleup C)$
(7) $A \bigtriangleup \varnothing$

1.2.28. Demuestre que para conjuntos A, B y C se tiene:
(1) $A \bigtriangleup (B \bigtriangleup C) = (A \bigtriangleup B) \bigtriangleup C$
(2) $A \bigtriangleup B = B \bigtriangleup A$
(3) $A \bigtriangleup \varnothing = A$; $A \bigtriangleup A = A$.
(4) $A \cap (B \bigtriangleup C) = (A \cap B) \bigtriangleup (A \cap C)$
(5) Si $A \bigtriangleup B = A \bigtriangleup C$ entonces $B = C$
(6) $A \cup B = A \bigtriangleup B \bigtriangleup (A \cap B)$; $A - B = A \bigtriangleup (A \cap B)$. Así las operaciones $\cup$ y $-$ pueden ser expresadas en términos de $\bigtriangleup$ y $\cap$.
(7) $A \triangle B = \varnothing \iff A = B$
(8) A y B son ajenos si y sólo si $A \cup B = A \bigtriangleup B$

1.2.29. Exprese las operaciones $\cup$, $\cap$ y $-$ en términos de:
(1) $\bigtriangleup$ y $\cap$,
(2) $\bigtriangleup$ y $\cup$,
(3) $-$ y $\bigtriangleup$.

1.2.30. Demuestre que:

(1) $-$ no se puede expresar en términos de $\cap$ y $\cup$,
(2) $\cup$ no se puede expresar en términos de $\cap$ y $-$.

1.2.31. Encuentre números enteros x, y, z tales que:

(1) $(2x, x+y) = (6, 2)$,
(2) $(y^2, x+y) = (9, 5)$,
(3) $(x^2 + x - y + 2, 8) = (2, y)$,
(4) $(2x, x+y, x+y+z) = (8, 2, 7)$.

1.2.32. Considere las siguientes posibles definiciones de par ordenado de a y b

$$(a, b) = \{\{a, \varnothing\}, \{b, \varnothing\}\}$$
$$(a, b) = \{\{\{a\}, \varnothing\}, \{\{b\}\}\}.$$

Demuestre que éstas satisfacen la condición $*$ de la página 34.

1.2.33. Demuestre utilizando la definición 1.2.23, de par ordenado, que: $A \times B \subseteq \mathscr{P}(\mathscr{P}(A \cup B))$.

1.2.34. Sean A, B, C conjuntos no vacíos, demuestre que $A \times (B \times C) \neq (A \times B) \times C$.

1.2.35. Sean A y B son conjuntos no vacíos y $(A \times B) \cup (B \times A) = C \times C$. Demuestre que $A = B = C$.

1.2.36. Sean A, B y C conjuntos. Demuestre que si $C \times A = C \times B$ y $C \neq \varnothing$, entonces $A = B$.

1.2.37. Sean A, B, C y D conjuntos. Demuestre que:

(1) $A \times A = B \times B$ si y sólo si $A = B$.
(2) $A \times B = \varnothing$ si y sólo si $A = \varnothing$ y $B = \varnothing$,
(3) Supongamos que $C \times D \neq \varnothing$. Entonces $C \times D \subseteq A \times B$ si y sólo si $C \subseteq A$ y $D \subseteq B$.

1.2.38. [10] Sean A, B y C conjuntos. Demuestre

(1) $(A \cup B) \times C = (A \times C) \cup (B \times C)$.
(2) $A \times (B \cap C) = (A \times B) \cap (A \times C)$.
(3) $(A - B) \times C = (A \times C) - (B \times C)$.

1.2.39. Sean A, B y C conjuntos. Demuestre

[10] Parte del teorema 1.2.33 pág. 36.

(1) $A \times (B \bigtriangleup C) = (A \times B) \bigtriangleup (A \times C)$.
(2) $(A \bigtriangleup B) \times C = (A \times C) \bigtriangleup (B \times C)$

1.2.40. Sean A y B conjuntos.

(1) Demuestre que $\{S \times T \mid (S,T) \in \mathscr{P}(A) \times \mathscr{P}(B)\} \subseteq \mathscr{P}(A \times B)$.
(2) ¿Es cierto que todo subconjunto de $A \times B$ es de la forma $S \times T$, con $S \subseteq A$ y $T \subseteq B$? (justifica tu respuesta).

1.2.41. Sean $A, B \subseteq X$ y $C, D \subseteq Y$. Demuestre que:

(1) $(A \times C) \cap (B \times D) = (A \cap B) \times (C \cap D)$.
(2) $(A \times C) \cup (B \times D) \subseteq (A \cup B) \times (C \cup D)$. Dé un ejemplo en el que no se cumple la igualdad.
(3) $(A \cup B) \times (C \cup D) = (A \times C) \cup (B \times D) \cup (A \times D) \cup (B \times C)$.
(4) $(X \times Y) - (B \times C) = ((X - B) \times Y) \cup (X \times (Y - C))$.

1. 2.42. Si se intenta generalizar la definición para una terna ordenada (a, b, c) como

$$(a, b, c) = \{\{a\}, \{a, b\}, \{a, b, c\}\}$$

no se tendrá éxito, pues fracasa la idea de ordenado. Dé un contraejemplo para esto.

§ § Ejercicios sección 1.3.

1.3.1. [11] Demuestre el teorema 1.3.2.

1.3.2. Sean $A = \{1, 2, 3\}$ y $B = \{a, b\}$.

(1) Encuentre las relaciones R de A en B tales que $Dom(R) = A$ y $Im(R) = \{b\}$.
(2) Encuentre las relaciones R de A en B tales que $Im(R) = \emptyset$.
(3) Encuentre las relaciones R de A en B tales que $(1, a) \in R$ y $(1, b), (3, a) \notin R$.
(4) Encuentre las relaciones R de A en B tales que $3 \notin Dom(R)$ y $a \notin Im(R)$.

1.3.3. Considere las siguientes relaciones definidas en el conjunto $X = \{1, 2, 3, 4\}$. (Esto es, relaciones de X en X).

(1) $r = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 3), (3, 4)\}$.
(2) $s = \{(2, 3), (3, 4), (2, 4), (4, 3), (3, 2), (4, 2), (2, 2), (3, 3), (4, 4)\}$.
(3) $t = \{(2, 3), (3, 4), (2, 4), (4, 3), (3, 2), (4, 2)\}$.
(4) $u = \{(1, 2), (2, 3)\}$.

[11] Teorema 1.3.2 pág. 38.

(5) $v = \{(1,1),(2,2),(3,3),(4,4)\}$.
(6) $w = \{(1,2),(2,3),(1,3),(3,3),(3,2),(2,2)\}$.
(7) $x = \{(1,1),(2,2),(3,3),(4,4),(1,3),(3,1),(3,4),(4,3)\}$.
(8) $y = \{(1,1),(1,2),(1,3),(1,4)\}$.
(9) $X \times X$.
(10) $z = \{(1,1),(2,2),(3,3),(4,4),(1,2),(2,3),(1,3),(1,4)\}$.
(11) $X \times \varnothing$

Encuentre el dominio e imagen de cada relación.

1.3.4. Para las siguientes relaciones binarias de $A = \{-3,-1,0,1,4,9\}$ en $B = \{0,1,2,3,4,5,6,7\}$, encuentra su dominio e imagen.

1) $R = \{(x,y) \in A \times B \mid x = y\}$
2) $S = \{(x,y) \in A \times B \mid x \neq y\}$
3) $T = \{(x,y) \in A \times B \mid y \leq x\}$
4) $U = \{(x,y) \in A \times B \mid x < y\}$
5) $V = \{(x,y) \in A \times B \mid y + 2x = 4\}$
6) $W = \{(x,y) \in A \times B \mid |x| - y = 4\}$
7) $X = \{(x,y) \in A \times B \mid x^2 + y^2 \leq 10\}$
8) $Y = \{(x,y) \in A \times B \mid x^2 = y^2\}$
9) $Z = \{(x,y) \in A \times B \mid x - 2 \leq y \leq x + 1\}$
10) $L = \{(x,y) \in A \times B \mid x = y^2\}$

1.3.5. Sean $A = \{1,2\}$ y $B = \{a,b,c\}$.

(1) Encuentre las relaciones R de A en B tales que $2 \notin Dom(R)$ y $a, c \notin Im(R)$.
(2) Encuentre las relaciones R de A en B tales que $Dom(R) = A$ e $Im(R) = \{b\}$.
(3) Encuentre las relaciones R de A en B tales que $(1,a) \in R$ y $(1,b),(3,a) \notin R$.

1.3.6. Sea $A = \{a,b,c\}$ y sean R y S las relaciones de A en A dadas por

$$R = \{(a,a),(a,b),(b,c),(c,a),(c,c)\} \quad y \quad S = \{(a,b),(a,c),(b,a),(c,c)\}.$$

Encuentre:
1) $R \cap S$, 2) $R \cup S$, 3) $(A \times A) - R$, 4) $R \circ S$, 5) $S^2 = S \circ S$,
6) R^{-1}, 7) S^{-1}, 8) $(R \circ S)^{-1}$.

1.3.7. Sean $A = \{1,2,3,4,5\}$, $B = \{6,7,8,9\}$, $C = \{a,b,c,d\}$ y $D = \{e,f,g,h\}$. Sean $R \subseteq A \times B$, $S \subseteq B \times C$ y $T \subseteq C \times D$ definidas por

$$R = \{(1,7),(4,6),(5,6),(2,8)\}, \qquad S = \{(6,a),(6,b),(7,a),(8,d)\},$$
$$T = \{(b,f),(a,f),(d,h),(c,e),(d,g)\}.$$

Encuentre:

1) R^{-1}	2) S^{-1}	3) $S \circ R$	4) $S \circ S^{-1}$
5) $S^{-1} \circ S$	6) $R^{-1} \circ S^{-1}$	7) $T \circ S$	8) $T \circ (S \circ R)$
9) $(T \circ S)^{-1}$	10) $(R^{-1} \circ S^{-1}) \circ T^{-1}$	11) $R[\{4,5,3\}]$	12) $S[\{6,8\}]$
13) $T[\{a,c,b\}]$	14) $R^{-1}[\{6,9\}]$	15) $S^{-1}[\{a,b\}]$	16) $T^{-1}[\{e,f,h\}]$

1.3.8. Sea R una relación de X en Y, y sean $A, B \subseteq X$. Pruebe:

(1) $R[A \cup B] = R[A] \cup R[B]$.
(2) $R[A \cap B] \subseteq R[A] \cap R[B]$.
(3) $R[A - B] \supseteq R[A] - R[B]$.
(4) Por medio de ejemplos muestre que $\subseteq$ y $\supseteq$ en (2) y (3) no pueden remplazarse por $=$.
(5) Pruebe los incisos (1), . . . , (4) con R^{-1} en vez de R.

1.3.9. ¿Es cierto que $R = Dom(R) \times Im(R)$? (justifica tu respuesta).

1.3.10. Sea R una relación de X en Y. Pruebe:

(1) $R \subseteq Dom(R) \times Im(R)$.
(2) $R[X] = Im(R)$ y $R^{-1}[Y] = Dom(R)$.
(3) Si $a \notin Dom(R)$ entonces $R[\{a\}] = \emptyset$; si $b \notin Im(R)$ entonces $R^{-1}[\{b\}] = \emptyset$.
(4) $Dom(R) = Im(R^{-1})$; $Im(R) = Dom(R^{-1})$.
(5) $(R^{-1})^{-1} = R$.
(6) $R^{-1} \circ R \supseteq \Delta_{Dom(R)}$, $R \circ R^{-1} \supseteq \Delta_{Im(R)}$. Dar un ejemplo de una relación R tal que $R^{-1} \circ R \neq \Delta_{Dom(R)}$ y $R \circ R^{-1} \neq \Delta_{Im(R)}$.

1.3.11. Demuestre que si $Im(R) \cap Dom(S) = \emptyset$ entonces $R \circ S$ es la relación vacía.

1.3.12. Sea R una relación de X en Y. Demuestre que $R \circ \Delta_X = R = \Delta_Y \circ R$.

1.3.13. Pruebe que para tres relaciones $R \subseteq A \times B$, $S \subseteq B \times C$ y $T \subseteq C \times D$:

$$T \circ (S \circ R) = (T \circ S) \circ R.$$

(La operación $\circ$ es asociativa.)

1.3.14. Pruebe que para tres relaciones R, S y T:

(1) $(R \circ S)^{-1} = S^{-1} \circ R^{-1}$,
(2) $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$,
(3) ¿Cómo se compara $(R \cup S)^{-1}$ y $R^{-1} \cup S^{-1}$?,
(4) $(R \cup S) \circ T = (R \circ T) \cup (S \circ T)$; $R \circ (S \cup T) = (R \circ S) \cup (R \circ T)$,
(5) $(R \cap S) \circ T \subseteq (R \circ T) \cap (S \circ T)$; $R \circ (S \cap T) \subseteq (R \circ S) \cap (R \circ T)$,

(6) Por medio de ejemplos muestre que $\subseteq$ en (5) no puede remplazarse por $=$.

1.3.15. Halle una relación R en el conjunto $X = \{1, 2, 3, 4, 5\}$ tal que $R \circ R^{-1} = \Delta_A$ y $R^{-1} \circ R$ conste de una solo elemento.

1.3.16. Halle una relación R tal que $R \circ R \neq \emptyset$ pero $R \circ (R \circ R) = \emptyset$.

1.3.17. Demuestre que $Im(R) \cap Dom(S) = \emptyset$ si y sólo si $R \circ S$ es la relación vacía.

1.3.18. Sea R una relación de X a Y. Muestre que $R \circ \Delta_X = R = \Delta_Y \circ R$.

1.3.19. Dado un conjunto X, considere $S \subseteq X$. Definimos

$$R_S = \{(A, B) \in \mathcal{P}(X) \times \mathcal{P}(X) \mid A \cup B^c \subseteq S\}.^{12}$$

(1) ¿Qué conjunto es $Dom(R_S)$? ¿e $Im(R_S)$?
(2) Muestre que si $R_S \circ R_S \neq \emptyset$, entonces $S = X$.
(3) Dados $S, T \subseteq X$, ¿cómo se comparan $R_{S \cap T}$ y $R_S \cap R_T$?.
(4) Dados $S, T \subseteq X$, ¿cómo se comparan $R_{S \cup T}$ y $R_S \cup R_T$?.

1.3.20. Consideremos las siguientes relaciones S, F y M de X en X, donde $X = \{seres\ humanos\}$.

$$(x, y) \in S \iff x \text{ es hermana de } y;$$
$$(x, y) \in P \iff x \text{ es el padre de } y;$$
$$(x, y) \in M \iff x \text{ es la madre de } y.$$

¿Qué relación es $S \circ F$? ¿Qué relación es $M \circ F$?

1.3.21. Sea X un conjunto y sean R y S relaciones de X en X. Demuestre que si $R \subseteq S$ entonces

(1) $T \circ R \subseteq T \circ S$; $R \circ T \subseteq S \circ T$.
(2) $S^{-1} \subseteq R^{-1}$.

Relaciones reflexivas, simétricas, antisimétricas, y transitivas

1.3.22. Sea $X = \{a, b, c, d, e\}$ y sean R, S, T y U relaciones en X donde

$R = \{(a, a), (a, b), (b, c), (b, d), (c, e), (e, d), (c, a)\}$,
$S = \{(a, b), (b, a), (b, c), (b, d), (e, e), (d, e), (c, b)\}$,
$T = \{(a, b), (a, a), (b, c), (b, b), (e, e), (b, a), (c, b), (c, c), (d, d), (a, c), (c, a)\}$,
$U = \{(a, b), (b, c), (b, b), (e, e), (b, a), (c, b), (d, d), (a, c), (c, a)\}$.

(1) ¿Cuáles de las relaciones son simétricas?

[12] Recuerde que B^c es el compelmento de B en X, véase página 33

(2) ¿Cuáles son reflexivas?
(3) ¿Cuáles son irreflexivas?
(4) ¿Cuáles son transitivas?
(5) ¿Cuáles son antisimétricas?[13]

1.3.23. Sea $A = \{a, b, c, d, e\}$.

(1) Construye una relación en A que sea: reflexiva, pero no transitiva ni simétrica.
(2) Construye una relación en A que sea: simétrica, pero no transitiva ni reflexiva.
(3) Construye una relación en A que sea: transitiva, pero no reflexiva ni simétrica.
(4) Construye una relación en A que sea: reflexiva y simétrica, pero no transitiva.
(5) Construye una relación en A que sea: reflexiva y antisimétrica, pero no transitiva.
(6) Construye una relación en A que sea: reflexiva y transitiva, pero no simétrica.
(7) Construye una relación en A que sea: antisimétrica y transitiva, pero no reflexiva.

1.3.24. Sea R la relación binaria en $\mathbb{Z}$ definida por $(a, b) \in R \iff a^2 + a = b^2 + b$. Determine si es reflexiva, antisimétrica, simétrica, antisimétrica, transitiva.

1.3.25. Demuestre que:

(1) R es simétrica si y sólo si $R^{-1} \subseteq R$.
(2) R es transitiva si y sólo si $R \circ R \subseteq R$.
(3) R es transitiva y simétrica si y sólo si $R^{-1} \circ R = R$.

1.3.26. Demuestre que si las relaciones R_1 y R_2 son reflexivas, entonces las relaciones $R_1 \cup R_2$, $R_1 \cap R_2$, R_1^{-1}, $R_1 \circ R_2$ son también reflexivas.

1. 3.27. Demuestre que si las relaciones R_1 y R_2 son irreflexivas, entonces las relaciones $R_1 \cup R_2$, $R_1 \cap R_2$, R_1^{-1} son también irreflexivas. Demuestre que la composición $R_1 \circ R_2$ de dos relaciones irreflexivas puede no ser irreflexiva.

1.3.28. Demuestre que si las relaciones R_1 y R_2 son simétricas, entonces las relaciones $R_1 \cup R_2$, $R_1 \cap R_2$, R_1^{-1} son también simétricas.

1.3.29. Demuestre que la composición $R_1 \circ R_2$ de dos relaciones simétricas R_1 y R_2 es simétrica si y sólo si $R_1 \circ R_2 = R_2 \circ R_1$.

1.3.30. Demuestre que:

[13] Una relación R es antisimétrica si $(a, b), (b, a) \in R$ implica $a = b$.

(1) Si las relaciones R_1 y R_2 son antisimétricas, entonces $R_1 \cap R_2$ y R_1^{-1} son también antisimétricas.
(2) La unión $R_1 \cup R_2$ de dos relaciones antisimétricas R_1 y R_2 en A es antisimétrica si y sólo si $R_1 \circ R_2^{-1} \subseteq \Delta_A$.

1.3.31. Demuestre que cualquier relación R que es simétrica y antisimétrica es transitiva.

§§ Ejercicios sección 1.4.

1.4.1. Sean $X = \{a, b, c, d\}$ y $Y = \{1, 2, 3, 4\}$. Decide cuál de los siguientes conjuntos de pares ordenados son funciones de X en Y. Si sí es función haga un diagrama de ella y encuentre su imagen.

(1) $f = \{(a, 1), (b, 1), (c, 3), (d, 4)\}$.
(2) $g = \{(a, 3), (b, 1), (c, 2), (d, 3), (b, 4)\}$.
(3) $h = \{(a, 3), (b, 4), (c, 1), (d, 2)\}$.
(4) $i = \{(a, 4), (b, 4), (d, 1)\}$.
(5) $j = \{(a, 2), (b, 2), (c, 2), (d, 2)\}$.
(6) $k = \{(a, 1), (b, 2), (c, 3), (d, 5)\}$.

1.4.2. Decide cuál de los siguientes conjuntos de pares ordenados son funciones de $\mathbb{Z}$ en $\mathbb{Z}$. Si sí es función encuentre su imagen.

(1) $F = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x^2 \leq y\}$
(2) $G = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x - 2 \leq y \leq x + 1\}$
(3) $H = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid 4x + 2y = 6\}$
(4) $I = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid y = x^2\}$
(5) $J = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x = y\}$
(6) $K = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x^2 = y^2\}$

1.4.3. Sean $A = \{1, 2, 3\}$ y $B = \{a, b, c\}$.

(1) Determine todas las funciones f de A en B tales que $f(1) = a$.
(2) Determine todas las funciones f de A en B tales que $f(2) = f(3)$.
(3) Determine todas las funciones f de A en B tales que $f(2) \neq f(3)$ y $f(1) = c$.

1.4.4. Sean X y Y conjuntos. Demuestre que:

(1) Si $X = \emptyset$ entonces existe una única función de X a Y;
(2) Si $X \neq \emptyset$ y $Y = \emptyset$, entonces no existe ninguna función de X a Y.

1.4.5. Sean A y B conjuntos y $f : A \to B$ una función. Demuestre que $A \neq \emptyset$ implica que $B \neq \emptyset$.

1.4.6. Sea X un conjunto no vacío, justifique el hecho de que no existe ninguna función de X en $\emptyset$.

1.4.7. [14] Sean $f : X \longrightarrow Y$ y $g : X' \longrightarrow Y'$ dos funciones. Demuestre que f y g son iguales si y sólo si $X = X', Y = Y'$ y $f(x) = g(x)$ para todo $x \in X$.

1.4.8. [15] Diga por que en el ejemplo 1.4.18 (página 46) es suficiente demostrar que
$\mathbb{N} - \{0\} \subseteq Im(f)$ para verificar que $Im(f) = \mathbb{N} - \{0\}$.

1.4.9. Explique por qué cada una de las siguientes "*funciones*" está mal definida.
(1) $f : \mathbb{N} \longrightarrow \mathbb{Z}$ como $f(x) = \frac{x}{2} - 1$ para todo $x \in \mathbb{Z}$.
(2) $g : \mathbb{R} \longrightarrow \mathbb{R}$ como $g(x) = \frac{1}{x+1}$ para todo $x \in \mathbb{R}$.
(3) $h : \mathbb{Q} \longrightarrow \mathbb{Z}$ como $h(\frac{a}{b}) = a$ para todo $a, b \in \mathbb{Z}$ con $b \neq 0$.
(4) $i : \mathbb{Z} \longrightarrow \mathbb{Z}$ como

$$i(x) = \begin{cases} -x^2 & \text{si } x > -1 \\ x & \text{si } x \leq 1. \end{cases}$$

(5) $j : \mathbb{Z} \longrightarrow \mathbb{Z}$ como

$$j(x) = \begin{cases} x + 3 & \text{si } x > 1 \\ 2x & \text{si } x \leq 0. \end{cases}$$

1.4.10. Sea $X = X_1 \cup X_2$, $f : X_1 \longrightarrow Y$ y $g : X_2 \longrightarrow Y$ funciones. Demuestre que la relación dada por

$$h(x) = \begin{cases} f(x) & \text{si } x \in X_1 \\ \\ g(x) & \text{si } x \in X_2 \end{cases}$$

es función de X en Y si y sólo si $g(x) = f(x)$ para toda $x \in X_1 \cap X_2$.

1.4.11. Las funciones f y g son llamadas **compatibles** si $f(x) = g(x)$ para todo $x \in Dom(f) \cap Dom(g)$.
Muestre que:
(1) f y g son compatibles si y sólo si $f \cup g$ es una función.
(2) f y g son compatibles si y sólo si $f\,|_{Dom(f)\cap Dom(g)} = g\,|_{Dom(f)\cap Dom(g)}$.

[14] teorema 1.4.8 pág. 44.
[15] Parte del ejercicio 1.4.18 pág. 46.

1.4.12.

(1) Definimos $f : \mathbb{N} \longrightarrow \mathbb{Z}$ como $f(n) = -n^3 + n + 2$ para todo $n \in \mathbb{N}$. Encuentre $f(1)$, $f(0)$ y $f(2)$.

(2) Definimos $g : \mathbb{Z} \longrightarrow \mathbb{Q}$ como $g(x) = \frac{x^2+2}{3}$ para todo $x \in \mathbb{Z}$. Encuentre $g(5)$, $g(-1)$, $g(0)$ y $g(1)$.

(3) Definimos $h : \mathbb{N} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ como $h(x, y) = y - 3x$ para todo $x \in \mathbb{N}$ y $y \in \mathbb{Z}$. Encuentre $h(1, 2)$, $h(1, -1)$, $h(2, 1)$ y $h(2, -3)$.

(4) Se define la función **parte entera** o **función suelo** $\lfloor\ \rfloor : \mathbb{R} \longrightarrow \mathbb{Z}$ como:

$$\lfloor x \rfloor = \text{el mayor entero menor o igual que } x,$$

es decir, $\lfloor x \rfloor$ es el entero inmediato a la izquierda de x en la recta real. Calcule $\left\lfloor \sqrt{2} \right\rfloor$, $\left\lfloor \frac{15}{17} \right\rfloor$, $\lfloor \pi \rfloor$, $\lfloor -2 \rfloor$, $\left\lfloor -\frac{18}{7} \right\rfloor$.

(5) Se define la **función techo** $\lceil\ \rceil : \mathbb{R} \longrightarrow \mathbb{Z}$ como:

$$\lceil x \rceil = \text{el menor entero mayor o igual que } x,$$

es decir, $\lceil x \rceil$ es el entero inmediato a la derecha de x en la recta real. Calcule $\left\lceil -\sqrt{2} \right\rceil$, $\left\lceil \frac{5}{2} \right\rceil$, $\lceil 2\pi \rceil$ y $\lceil 5 \rceil$.

(6) Se define la **función signo** $sgn : \mathbb{R} \longrightarrow \{-1, 0, 1\}$ como

$$sgn(x) = \begin{cases} 1 & \text{si } x > 1 \\ 0 & \text{si } x = 0 \\ -1 & \text{si } x < 0. \end{cases}$$

Calcule $sgn(-2)$, $sgn(7)$, $sgn(-4) + sgn(2)$ y $sgn(-4 + 2)$.

(7) Se define la **función valor absoluto** $|\ | : \mathbb{R} \longrightarrow \mathbb{R}$ como

$$|x| = \begin{cases} x & \text{si } x \geq 0 \\ -x & \text{si } x < 0. \end{cases}$$

Calcule $|3|$, $|-5|$, $|2-5|$, $|2| + |-5|$ y $|-4| - |3|$.

(8) Definimos $j : \mathbb{Z} \longrightarrow \mathbb{R}$ como

$$j(x) = \begin{cases} -x^2 & \text{si } x > 0 \\ x + 1 & \text{si } -3 \leq x \leq 0 \\ x + x^2 & \text{si } x < -3. \end{cases}$$

Calcule $j(2)$, $j(1)$, $j(-1)$ y $j(-3)$.

(9) Sean $A = \{1, 2, 3, \{1, 2\}\}$ y $B = \{1, \{1\}, 2, \{1, 2\}\}$. Definimos $F : \mathscr{P}(A) \longrightarrow \mathscr{P}(B)$ como $F(X) = B - (A - X)$ para todo $X \subseteq A$. Encuentre $F(\varnothing)$, $F(\{1\})$, $F(\{1, 2\})$ y $F(A)$.

(10) Sean $C = \{1, 2, 3, 4, 5, 7\}$ y $D = \{2, 4, 5, 7, 8\}$. Definimos $G : \mathscr{P}(C) \longrightarrow \mathscr{P}(D)$ como $f(X) = D \cap X$ para todo $X \subseteq C$. Encuentre $G(\{1, 2, 3\})$, $G(\{2, 3, 5, 7\})$ y $G(C)$.

1.4.13. Para cada pareja de funciones diga si son iguales o no (justifique su respuesta).

(1) $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ y $g : \mathbb{N} \longrightarrow \mathbb{Z}$ dadas por

$$f(x) = 2x^2 - 1 \qquad \text{y} \qquad g(x) = 2x^2 - 1.$$

(2) Sea $X = \{-1, 0, 1\}$, y sean $f : X \longrightarrow \mathbb{Z}$ y $g : X \longrightarrow \mathbb{Z}$ dadas por

$$f(x) = x \qquad \text{y} \qquad g(x) = x^3.$$

(3) $f : \mathbb{Z} \longrightarrow \mathbb{R}$ y $g : \mathbb{Z} \longrightarrow \mathbb{R}$ dadas por

$$f(x) = x^2 + 2x \qquad \text{y} \qquad g(x) = x^2 - 2x.$$

(4) Sea $Y = \{-2, 0, 1\}$, y sean $f : Y \longrightarrow \mathbb{Z}$ y $g : Y \longrightarrow \mathbb{Z}$ dadas por

$$f(x) = x^2(x + 1) \qquad \text{y} \qquad g(x) = 2x.$$

(5) Sea $W = \{-1, 0, 1, 3\}$, y sean $f : W \longrightarrow \mathbb{Z}$ y $g : W \longrightarrow \mathbb{Z}$ dadas por

$$f(x) = x^3(x - 1) \qquad \text{y} \qquad g(x) = 3x(x^2 - 1).$$

(6) Sean $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ y $g : \mathbb{Z} \longrightarrow \mathbb{Z}$ dadas por

$$f(x) = x^3(x - 1) \qquad \text{y} \qquad g(x) = 3x(x^2 - 1).$$

(7) $f : \mathbb{Z} \longrightarrow \mathbb{Q}$ y $g : \mathbb{Z} \longrightarrow \mathbb{R}$ dadas por

$$f(x) = \frac{x}{2} + 1 \qquad \text{y} \qquad g(x) = \frac{x}{2} + 1.$$

(8) Sean $f : \mathbb{N} \longrightarrow \mathbb{Q}$ y $g : \mathbb{N} \longrightarrow \mathbb{Q}$ dadas por

$$f(x) = 2x - 4 \qquad \text{y} \qquad g(x) = \frac{2x^2 - 8}{x + 2}$$

(9) Sean $A = \{1, 2, 3, a\}$, $B = \{2, 3, b\}$; y sean $f : \mathscr{P}(A) \longrightarrow \mathscr{P}(B)$ y $g : \mathscr{P}(A) \longrightarrow \mathscr{P}(B)$ dadas por

$$f(X) = B - X \qquad \text{y} \qquad g(X) = B - (B \cap X),$$

para todo $X \subseteq A$.

(10) Sea $f : \mathbb{N} \longrightarrow \mathbb{Q}$ y $g : \mathbb{N} \longrightarrow \mathbb{Q}$ dadas por

$$f(x) = \begin{cases} \frac{2x^2-3x+1}{x-1} & \text{si } x > 3 \\ \\ 2x(x-1) & \text{si } 0 \leq x \leq 2 \end{cases} \quad \text{y} \quad g(x) = \begin{cases} 2x-1 & \text{si } x > 3 \\ \\ x^2(x-1) & \text{si } 0 \leq x \leq 2 \end{cases}.$$

(11) Sea $f : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ y $g : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ dadas por

$$f(x,y) = \begin{cases} x & \text{si } y \leq x \\ y & \text{si } x < y \end{cases} \qquad \text{y} \qquad g(x,y) = \frac{x+y+|y-x|}{2}.$$

(12) Sean $f : \mathbb{R} \longrightarrow \mathbb{Z}$ y $g : \mathbb{R} \longrightarrow \mathbb{Z}$ dadas por

$$f(x) = \begin{cases} x & \text{si } x \in \mathbb{Z} \\ \lfloor x \rfloor + 1 & \text{si } x \in \mathbb{R} - \mathbb{Z} \end{cases} \qquad \text{y} \qquad g(x) = \lceil x \rceil.$$

1.4.14. Sea X un conjunto. Dado un subconjunto $A \subseteq X$ definimos la función $\chi_A : X \longrightarrow \{0,1\}$ como

$$\chi_A(x) = \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{si } x \in X - A\,. \end{cases}$$

χ_A se llama **función característica** del subconjunto $A \subseteq X$. Demuestre que:

(1) $A \subseteq B$ si y sólo si $\chi_A \leq \chi_B$.
(2) $\chi_{A\cap B} = \chi_A \cdot \chi_B = \text{mín}\{\chi_A, \chi_B\}$.
(3) $\chi_{A\cup B} = \chi_A + \chi_B - \chi_A \cdot \chi_B = \text{máx}\{\chi_A, \chi_B\} = 1 - (1-\chi_A)(1-\chi_B)$.
(4) $\chi_{A^c} = 1 - \chi_A$.
(5) $\chi_{A \bigtriangleup B} = |\, \chi_A - \chi_B \,|$.[16]

1.4.15. [17] Sea $f : X \longrightarrow Y$ una función. Entonces

(1) $f \circ 1_X = f$,
(2) $1_Y \circ f = f$.

1.4.16. Sean $f : \mathbb{N} \to \mathbb{Z}$ definida por $f(x) = -x$ y $g : \mathbb{Z} \to \mathbb{N}$ definida por $g(x) = \begin{cases} x & si\ x \geq 0 \\ -x & si\ x < 0 \end{cases}$. Encuentre $g \circ f$ y muestre que $g \circ f = 1_{\mathbb{N}}$.

1.4.17. Definimos $f : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ como $f(x,y) = x + y - 3xy$ para todo $x, y \in \mathbb{Z}$. Demuestre que

$$f(f(x,y),z) = f(x, f(y,z))$$

[16] Véase la definición de $A \bigtriangleup B$ en la página 87.
[17] Parte de la proposición 1.4.24 pág. 47.

para todo $x, y, z \in \mathbb{Z}$.

Composición de funciones

1.4.18.

(1) Sea

$$g = \{(1, c), (2, a), (3, c), (4, d), (5, e)\}$$

una función de $X = \{1, 2, 3, 4, 5\}$ en $Y = \{a, b, c, d, e\}$ y

$$f = \{(a, x), (b, x), (c, z), (d, w)\}$$

una función de Y en $Z = \{w, x, y, z\}$, escriba $f \circ g$ como un conjunto de pares ordenados.

(2) Sea

$$h = \{(a, b), (b, a), (c, b), (d, a)\}$$

una función de $W = \{a, b, c, d\}$ en W. Escriba $h \circ h$ y $h \circ h \circ h$ como conjuntos de pares ordenados.

(3) Sean $F : \mathbb{N} \longrightarrow \mathbb{Z}$ y $G : \mathbb{Z} \longrightarrow \mathbb{N}$ dadas por

$$F(x) = -x + 5 \qquad \text{y} \qquad G(x) = x^2 + 1.$$

Encuentre $F \circ G$ y $G \circ F$.

(4) Sean $H : \mathbb{Z} \longrightarrow \mathbb{Q}$ y $L : \mathbb{Q} \longrightarrow \mathbb{Q}$ dadas por

$$H(x) = \frac{x^2 + 1}{2} \qquad \text{y} \qquad L(x) = \frac{2}{x^2 + 1}.$$

Encuentre $L \circ H$ y $L \circ L$.

(5) Sean $P : \mathbb{Z} \longrightarrow \mathbb{Z}$ y $Q : \mathbb{Z} \longrightarrow \mathbb{Z}$ dadas por

$$P(x) = \begin{cases} 2x - 1 & \text{si } x \geq 0 \\ x^2 - 1 & \text{si } x < 0 \end{cases} \qquad \text{y} \qquad Q(x) = \begin{cases} x^2 & \text{si } x \geq 0 \\ -x & \text{si } x < 0. \end{cases}$$

Encuentre $P \circ Q$ y $Q \circ P$.

1.4.19. Considere la función $f : \mathbb{R} \longrightarrow \mathbb{R}$ dada por

$$f(x) = (1 + (1 - x^3))^{\frac{1}{3}}.$$

Exprese a f como la composición de cuatro funciones distintas a la función $1_{\mathbb{R}}$.

1.4.20. Sean $f, g, h : \mathbb{Z} \longrightarrow \mathbb{Z}$ definidas por $f(x) = x - 1$, $g(x) = 3x$,

$$h(x) = \begin{cases} 1 & \text{si } x > 0 \\ x^2 & \text{si } x \leq 0. \end{cases}$$

Determine

(1) $f \circ g$, $g \circ f$, $g \circ h$, $h \circ g$, $f \circ (g \circ h)$, $(f \circ g) \circ h$.
(2) $f \circ f$, $f \circ f \circ f$, $g \circ g$, $g \circ g \circ g$, $h \circ h$, $h \circ h \circ h$.

1.4.21. Sean $X = \mathbb{R} - \{0, 1\}$. Definimos $f_i : X \longrightarrow X$ para $1 \leq i \leq 6$ por:

$$f_1(x) = x; \quad f_2(x) = 1 - x; \quad f_3(x) = \tfrac{x-1}{x};$$
$$f_4(x) = \tfrac{1}{x}; \quad f_5(x) = \tfrac{1}{1-x}; \quad f_6(x) = \tfrac{x}{x-1}.$$

Demuestre que $f_i \circ f_j \in \{f_k \mid 1 \leq i \leq 6\}$ para todo i, j.

1.4.22. Sea $X = \{1, 2, 3, 4\}$, y sea $f : X \longrightarrow X$ la función dada por: $f(1) = 2$, $f(2) = 3$, $f(3) = 4$ y $f(4) = 1$. Demuestre que existe una única función $g : X \longrightarrow X$ tal que $g(1) = 3$ y $f \circ g = g \circ f$. ¿Es cierto qué existe una única función $h : X \longrightarrow X$ con $h(1) = 1$ y $f \circ h = h \circ f$?.

1.4.23. Sean $X = \{a, b, c, d\}$ y $Y = \{1, 2, 3, 4, 5\}$.

(1) Dé dos funciones $f : X \longrightarrow Y$ y $g : Y \longrightarrow X$ tales que $f \circ g = g \circ f$.
(2) Dé una función $h : Y \longrightarrow Y$ tal que $h \neq 1_Y$ y $h \circ h = 1_Y$.

1.4.24. Sea X un conjunto no vacío.

(1) Sea $x_0 \in X$ y sea $f : X \longrightarrow X$ la función contante igual x_0. Demuestre que $f \circ g = f$ para toda función $g : X \longrightarrow X$.
(2) Recíprocamente, si $f : X \longrightarrow X$ es una función tal que $f \circ g = f$ para toda función $g : X \longrightarrow X$, demuestre que existe $x_0 \in X$ tal que $f(x) = x_0$ para todo $x \in X$.

1.4.25. Sea X un conjunto y $A, B \subseteq X$ (fijos). Definimos $g : \mathscr{P}(X) \longrightarrow \mathscr{P}(X)$ por $g(Y) = A \cap (B \cup Y)$ para todo $Y \subseteq X$. Demuestre que $g \circ g = g$.

1.4.26.

(1) Sean $f, g : \mathbb{R} \longrightarrow \mathbb{R}$ donde $g(x) = 1 - x + x^2$ y $f(x) = ax + b$. Si $(g \circ f)(x) = 9x^2 - 9x + 3$, determine a, b.

(2) Sean $f, g : \mathbb{R} \longrightarrow \mathbb{R}$ donde $f(x) = ax + b$ y $g(x) = cx + d$ para cualquier $x \in \mathbb{R}$, con a, b, c, d constantes reales. ¿Qué relación(es) deben satisfacer a, b, c, d si $(f \circ g)(x) = (g \circ f)(x)$ para todo $x \in \mathbb{R}$?

1.4.27. Sea X un conjunto y $F : \mathcal{P}(X) \to \mathcal{P}(X)$ dada por $F(A) = X - A$. Demuestre que $F \circ F = I_{\mathcal{P}(X)}$.

Imagen directa e imagen inversa

1.4.28. Sean $X = \{a, b, c, d\}$ y $Y = \{1, 2, 3, 4, 5\}$.

(1) Dé una función $f : X \longrightarrow Y$ tal que $f[\{a, b, c\}] = \{2, 5\}$.

(2) Dé una función $g : X \longrightarrow Y$ tal que $g^{-1}[\{1, 2, 5\}] = \{a, d\}$.

(3) Dé dos funciones $f_1, f_2 : X \longrightarrow Y$ tales que $f_1[\{a, b, c\}] = f_2[\{c, d\}]$.

(4) Dé dos funciones $g_1, g_2 : X \longrightarrow Y$ tales que $g_1^{-1}[\{1, 4, 5\}] = g_2^{-1}(3)$.

1. 4.29. Sea $X = \{1, 2, 3, \ldots, 10\}$. Dé una función $f : X \longrightarrow X$ que cumpla (simultáneamente) que:

$$f^{-1}[\{1, 2, 3\}] = \varnothing,\ f^{-1}[\{4, 5\}] = \{1, 3, 7\} \text{ y } f^{-1}[\{8, 10\}] = \{8, 10\}.$$

1.4.30.

(1) Sea $f = \{(1, c), (2, a), (3, c), (4, d), (5, e)\}$ una función de $X = \{1, 2, 3, 4, 5\}$ a $Y = \{a, b, c, d, e\}$. Determine: $f[\{1, 3, 5\}]$ y $f^{-1}[\{a, b, d\}]$.

(2) Sea $g : \mathbb{Z} \longrightarrow \mathbb{Q}$, dada por $g(x) = \frac{x^2}{3} - x$. Encuentre $g[\{-1, 2, 3\}]$ y $g^{-1}[\{b, d\}]$.

(3) Sea $h : \mathbb{R} \longrightarrow \mathbb{R}$, dada por $h(x) = |x^2 + 3x + 1|$. Encuentre $h[\{-1, 1, 2\}]$ y $h^{-1}(1)$.

(4) Sea $F : \mathbb{R} - \{-2\} \longrightarrow \mathbb{R}$, dada por

$$F(x) = \left| \frac{x}{x + 2} \right|.$$

Encuentre $F^{-1}[\{-1, 4, 7\}]$ y $F^{-1}[\{-1, 4, 7\}]$.

(5) Sea $G : \mathbb{R} \longrightarrow \mathbb{R}$ definida por

$$G(x) = \begin{cases} 3x - 5 & \text{si } x > 0 \\ -3x + 1 & \text{si } x \leq 0. \end{cases}$$

Determine $G[\{-2, -\frac{5}{3}, 0, 1\}]$ y $G^{-1}[\{-6, -1, 2, 3\}]$.

(6) Sea $H : \mathbb{R} \longrightarrow \mathbb{R}$ definida por

$$H(x) = \begin{cases} x+7 & \text{si } x \leq 0 \\ -2x+5 & \text{si } 0 < x < 3 \\ x-1 & \text{si } 3 \leq x. \end{cases}$$

Sean $A = \{x \mid -5 \leq x \leq -1\}$, $B = \{x \mid -5 \leq x \leq 5\}$ y $C = \{x \mid -2 \leq x \leq 4\}$. Encuentre $H^{-1}[A]$, $H^{-1}[B]$ y $H^{-1}[C]$.

1.4.31. Sea $f : X \longrightarrow Y$ una función, y sean $A \subseteq X$ y $B \subseteq Y$. Demuestre que:

(1) $f[A] = \varnothing \iff A = \varnothing$;
(2) $f^{-1}[B] = \varnothing \iff B \cap f[X] = \varnothing$;
(3) $f[f^{-1}[f[A]]] = f[A]$; $f^{-1}[f[f^{-1}[B]]] = f^{-1}[B]$.

1.4.32. [18] Sea $f : X \longrightarrow Y$ una función, $A_1, A_2 \subseteq X$ y $B_1, B_2 \subseteq Y$. Entonces

(1) $f[A_1 \cup A_2] = f[A_1] \cup f[A_2]$.
(2) $B_1 \subseteq B_2$ implica $f^{-1}[B_1] \subseteq f^{-1}[B_2]$.
(3) $f^{-1}[B_1 \cap B_2] = f^{-1}[B_1] \cap f^{-1}[B_2]$.
(4) $f^{-1}[f[A_1]] \supseteq A_1$.

1.4.33. Sea $X = X_1 \cup X_2$, $f : X_1 \to Y$ y $g : X_2 \to Y$ funciones. Demuestre que la relación dada por

$$h(x) = \begin{cases} g(x) \ si \ x \in X_1 \\ f(x) \ si \ x \in X_2 \end{cases}$$

es función si y sólo si $g(x) = f(x)$ para toda $x \in X_1 \cap X_2$.

1.4.34. [19] Sea $f : X \longrightarrow Y$ una función, $A_1, A_2 \subseteq X$ y $B_1, B_2 \subseteq Y$. Entonces

(1) $f[A_1 \cup A_2] = f[A_1] \cup f[A_2]$,
(2) $B_1 \subseteq B_2$ implica $f^{-1}[B_1] \subseteq f^{-1}[B_2]$,
(3) $f^{-1}[B_1 \cap B_2] = f^{-1}[B_1] \cap f^{-1}[B_2]$,
(4) $f[f^{-1}[B_1]] \subseteq B_1$.

1.4.35. Dé un contraejemplo para mostrar la falsedad del siguiente enunciado: si $f : X \longrightarrow Y$ es una función, entonces para cualesquiera $A_1, A_2 \subseteq X$, $f[A_1] \subseteq f[A_2]$ implica que $A_1 \subseteq A_2$.

---

[18] Parte del teorema 1.4.31 pág. 49.

[19] Parte del Teorema 1.4.31 pág. 49.

1.4.36. Proponer conjuntos X e Y, subconjuntos $A_1, A_2 \subseteq X$ y una función $f : X \longrightarrow Y$ tales que

(1) $f[A_1 \cap A_2] = f[A_1] \cap f[A_2]$;
(2) $f[A_1 - A_2] = f[A_1] - f[A_2]$;
(3) $f[X - A_1] \subseteq Y - f[A_1]$;
(4) $f^{-1}[f[A_1]] = A_1$;
(5) $Y - f[A_1] \subseteq f[X - A_1]$;
(6) $f[X - A_1] \cap (Y - f[A_1]) = \varnothing$.

1.4.37. Demuestre que para cualquier función $f : X \longrightarrow Y$, $A \subseteq X$ y $B \subseteq Y$:

(1) $f[A] \cap B = f[A \cap f^{-1}[B]]$;
(2) $f^{-1}[B] = f^{-1}[B \cap f[X]]$;
(3) $f[A] \cap B = \varnothing \iff A \cap f^{-1}[B] = \varnothing$;
(4) $f[A] \subseteq B \implies A \subseteq f^{-1}[B]$.

1.4.38. Sea $f : X \longrightarrow Y$. Demostrar la equivalencia de las siguientes proposiciones cualesquiera que sean $A \subseteq X$ y $B \subseteq Y$.

(1) $f^{-1}[f[A]] = A$.
(2) $f[A \cap B] = f[A] \cap f[B]$.
(3) $A \cap B = \varnothing \implies f[A] \cap f[B] = \varnothing$.
(4) $B \subseteq A \implies f[A - B] = f[A] - f[B]$.

§§ Ejercicios sección 1.5.

1.5.1. Sean $X = \{a, b, c, d\}$, $Y = \{1, 2, 3, 4, 5\}$ y $Z = \{6, 7, 8\}$. Para cada una de las siguientes funciones haga un diagrama de ella y determine si es inyectiva y si es suprayectiva.

(1) $f : X \longrightarrow Y$ dada por: $f(a) = 4$, $f(b) = 5$, $f(c) = 3$ y $f(d) = 2$.

(2) $g : Y \longrightarrow Z$ dada por: $g(1) = 8$, $g(2) = 7$, $g(3) = 8$, $g(4) = 7$ y $g(5) = 6$.

(3) $h : Y \longrightarrow X$ dada por: $h(1) = a$, $h(2) = c$, $h(3) = b$, $h(4) = a$ y $h(5) = c$.

(4) $i : X \longrightarrow X$ dada por: $i(a) = c$, $i(b) = a$, $i(c) = b$ y $i(d) = a$.

1.5.2. Sean $X = \{a, b, c, d\}$ y $Y = \{1, 2, 3, 4, 5\}$.

(1) Dé una función inyectiva f de X a Y tal que $f(a) = 5$ y $f(d) \neq 1$.
(2) Dé una función inyectiva g de X a Y tal que $g[\{b, c\}] = \{2, 4\}$ y $g(a) \neq 5$.
(3) Dé una función inyectiva h de X a Y tal que $h^{-1}[\{1, 2\}] = \{a\}$ y $h(b) = 2$.

Haga un diagrama de cada una de las funciones.

1. 5.3. Sean $X = \{a, b, c, d\}$ y $Y = \{1, 2, 3, 4, 5\}$. Considerando la función $f : X \longrightarrow Y$ dada por: $f(a) = 1$, $f(b) = 5$, $f(c) = 4$ y $f(d) = 2$. Exhiba tres inversas izquierdas de f.

1.5.4. Sean $X = \{a, b, c, d, e\}$ y $Y = \{1, 2, 3\}$.

(1) Dé una función suprayectiva f de X a Y tal que $f(c) = f(d)$ y $f(b) \neq f(e)$.
(2) Dé una función suprayectiva g de X a Y tal que $g[\{b, c\}] \cap g[\{a, d\}] \neq \emptyset$.
(3) Dé una función suprayectiva h de X a Y tal que $h^{-1}[\{1, 3\}] = \{a, c, e\}$.

Haga un diagrama de cada una de las funciones.

1.5.5. Sean $X = \{a, b, c, d, e\}$ y $Y = \{1, 2, 3\}$. Considerando la función $f : X \longrightarrow Y$ dada por: $f(a) = 1$, $f(b) = 2$, $f(c) = 3$, $f(d) = 2$ y $f(e) = 3$. Exhiba tres inversos derechos de f.

1.5.6.

(1) Dé una función $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ que sea inyectiva pero no suprayectiva.
(2) Dé una función $g : \mathbb{N} \longrightarrow \mathbb{N}$ que sea suprayectiva pero no inyectiva.
(3) Dé una función $h : \mathbb{Z} \longrightarrow \mathbb{Z}$ que no sea suprayectiva ni inyectiva.

1.5.7. Determine cuál de las siguientes funciones son inyectivas o suprayectivas.

(1) $f : \mathbb{N} \longrightarrow \mathbb{N}$, $f(x) = 7x$;
(2) $f : \mathbb{R} \longrightarrow \mathbb{R}$, $f(x) = 7x$;
(3) $f : \mathbb{N} \longrightarrow \mathbb{Q}$, $f(x) = \frac{x-1}{2}$;
(4) $f : \mathbb{N} \longrightarrow \mathbb{N}$, $f(x) = x^2 + 1$;
(5) $f : \mathbb{Z} \longrightarrow \mathbb{N}$, $f(x) = x^2 - 1$;
(6) $f : \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$, $f(x) = (x - 1, 1)$;
(7) $A = \{1, 2, 3\}$ y $B = \{1, 2\}$, $f : \mathscr{P}(A) \longrightarrow \mathscr{P}(B)$, $f(X) = X \cap B$;
(8) $f : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$, $f(x, y) = x + y + 1$;
(9) $f : \mathbb{Z} \times \mathbb{N} \longrightarrow \mathbb{Z}$, $f(x, y) = x^2 + y$;
(10) $f : \mathbb{Z} \times \mathbb{N} \longrightarrow \mathbb{N}$, $f(x, y) = x^2 + y$;
(11) $f : \mathbb{Z} \longrightarrow \mathbb{Q}$, $f(x) = \frac{1}{x^2+1}$;
(12) $f : \mathbb{N} \longrightarrow \mathbb{Q}$, $f(x) = \frac{1}{x^2+1}$;
(13) $f : \mathbb{N} \longrightarrow \mathbb{Z}$, $f(n) = \begin{cases} -\frac{n}{2} & \text{si } n \text{ es par} \\ \frac{n+1}{2} & \text{si } n \text{ es impar;} \end{cases}$

(14) $f : \mathbb{N} \longrightarrow \mathbb{N}$, $f(n) = \begin{cases} \frac{n}{2} & \text{si } n \text{ es par} \\ n & \text{si } n \text{ es impar;} \end{cases}$

(15) $f : \mathbb{N} \longrightarrow \mathbb{N}$, $f(n) = \begin{cases} n+1 & \text{si } n \text{ es par} \\ n-1 & \text{si } n \text{ es impar;} \end{cases}$

(16) $f : \mathbb{N} \longrightarrow \mathbb{N}$, $f(n) = \begin{cases} \frac{n}{2} & \text{si } n \text{ es par} \\ 0 & \text{si } n \text{ es impar;} \end{cases}$

(17) $f : \mathbb{R} \longrightarrow \mathbb{Z}$, $f(x) = \lfloor x \rfloor$;

(18) $f : \mathbb{R} \longrightarrow \mathbb{R}$, $f(x) = |x|$;

(19) $f : \mathbb{R} \longrightarrow \mathbb{R}$, $f(x) = x^2|x|$;

(20) $f : \mathbb{R} \longrightarrow \mathbb{R}$, $f(x) = x^3|x|$;

(21) $f : \mathbb{R} \longrightarrow \mathbb{R}$, $f(x) = ||x-1|-1|$;

(22) $f : X \longrightarrow Y$, donde $X = \{x \in \mathbb{R} \mid x \leq 0\}$ y $Y = \{x \in \mathbb{R} \mid x \geq 0\}$, $f(x) = ||x-1|-1|$;

(23) $f : \mathbb{R} - \{1\} \longrightarrow \mathbb{R}$, $f(x) = \frac{x}{x-1}$;

(24) $f : C \longrightarrow \mathbb{R}$, donde $C = \{x \in \mathbb{R} \mid -2 \leq x\}$, $f(x) = \frac{x}{x-1}$;

(25) $f : \mathbb{R} \longrightarrow D$, donde $D = \{x \in \mathbb{R} \mid -1 < x < 1\}$, $f(x) = \frac{x}{1+|x|}$;

(26) $f : \mathbb{R} \longrightarrow \mathbb{R}$, $f(x) = x^3$;

(27) $f : \mathbb{R} \longrightarrow \mathbb{R}$, $f(x) = \begin{cases} 4x+1 & \text{si } x \geq 0 \\ x & \text{si } x < 0; \end{cases}$

(28) $f : \mathbb{R} \longrightarrow \mathbb{R}$, $f(x) = \begin{cases} 1-x & \text{si } x \geq 0 \\ x^2 & \text{si } x < 0; \end{cases}$

(29) $f : \mathbb{R} \longrightarrow \mathbb{R}$, $f(x) = \begin{cases} 3x & \text{si } x \geq 0 \\ x+3 & \text{si } x < 0; \end{cases}$

(30) $f : \mathbb{R} \longrightarrow \mathbb{R}$, $f(x) = \begin{cases} x & \text{si } x \geq 0 \\ x-1 & \text{si } x < 0. \end{cases}$

1.5.8. Sea $f : X \longrightarrow Y$ una función y $X' \subseteq X$

(1) Demuestre que si f es inyectiva, entonces $f|_{X'}$ también lo es.
(2) Demuestre que si $f|_{X'}$ es sobre, entonces f también lo es.

1.5.9. Sean $f : \mathbb{R} \longrightarrow \mathbb{R}$ y $g : \mathbb{R} \longrightarrow \mathbb{R}$ funciones definidas por

$$f(x) = \begin{cases} 4x+1 & \text{si } x \geq 0 \\ x & \text{si } x < 0 \end{cases}, \quad g(x) = \begin{cases} 3x & \text{si } x \geq 0 \\ x+3 & \text{si } x < 0 \end{cases}.$$

Demuestre que $g \circ f$ es biyectiva y dé una fórmula para $(g \circ f)^{-1}$. Demuestre también que $f \circ g$ es inyectiva pero no suprayectiva.

1.5.10. Sean $f : \mathbb{R} \longrightarrow \mathbb{R}$ y $g : \mathbb{R} \longrightarrow \mathbb{R}$ funciones definidas por

$$f(x) = \begin{cases} 1 - x & \text{si } x \geq 0 \\ x^2 & \text{si } x < 0\,, \end{cases} \quad g(x) = \begin{cases} x & \text{si } x \geq 0 \\ x - 1 & \text{si } x < 0\,. \end{cases}$$

Encuentre una fórmula para $f \circ g$. Pruebe que $f \circ g$ es biyectiva y encuentre su inversa. Encuentre también una fórmula para $g \circ f$ y demuestre que $g \circ f$ es inyectiva pero no suprayectiva.

1.5.11. Para las siguientes funciones muestre que son biyectivas y encuentre su inversa.

(1) $\mathbb{N}^* = \mathbb{N} - \{0\}$, $i : \mathbb{N} \longrightarrow \mathbb{N}^*$, $i(x) = x + 1$;

(2) $j : \mathbb{Q} \longrightarrow \mathbb{Q}$, $j(x) = 3x + 5$;

(3) $f : \mathbb{R} \longrightarrow \mathbb{R}$, $f(x) = x|x|$;

(4) $g : \mathbb{R} \longrightarrow \mathbb{R}$, $g(x) = \begin{cases} -x^2 & \text{si } x \geq 0 \\ 1 - x^3 & \text{si } x < 0 \end{cases}$;

(5) $h : \mathbb{R} \longrightarrow \mathbb{R}$, $h(x) = \begin{cases} x^4 & \text{si } x \geq 0 \\ x(2 - x) & \text{si } x < 0 \end{cases}$;

(6) $F : \mathbb{R} \longrightarrow \mathbb{R}$, $F(x) = \begin{cases} \frac{x+1}{x+2} & \text{si } x \neq -2 \\ 1 & \text{si } x = 2 \end{cases}$;

(7) $G : \mathbb{R} \longrightarrow \mathbb{R}$, $G(x) = \begin{cases} 1 - x & \text{si } x \geq 0 \\ (1 - x)^2 & \text{si } x < 0 \end{cases}$;

(8) $\mathbb{N}^* = \mathbb{N} - \{0\}$, $H : \mathbb{N}^* \longrightarrow \mathbb{Z}$, $H(x) = (-1)^n \lfloor \frac{n}{2} \rfloor$;

(9) $\{a_1, \ldots, a_n\} \subseteq \mathbb{R}$, $S : \mathbb{R} \longrightarrow \mathbb{R}$, $S(x) = \begin{cases} x & \text{si } x \notin \{a_1, \ldots, a_n\} \\ a_{i+1} & \text{si } x = a_i,\ 1 \leq i \leq n-1 \\ a_1 & \text{si } x = a_n \end{cases}$.

1.5.12. Sea $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$, y sea $f : \mathbb{R}^+ \longrightarrow \mathbb{R}^+$ dada por $f(x) = \frac{1}{1+x^2}$. Muestre que f es inyectiva y encuentre dos funciones distintas $g, h : \mathbb{R}^+ \longrightarrow \mathbb{R}^+$ tales que $g \circ f = h \circ f = 1_{\mathbb{R}^+}$.

1.5.13. Sean $a, b, c, d \in \mathbb{R}$ con $c \neq 0$. Para $x \neq -\frac{d}{c}$ establece la identidad

$$\frac{ax + b}{cx + d} = \frac{a}{c} - \frac{ad - bc}{c^2} \cdot \frac{1}{x + \frac{d}{c}}.$$

Sea $X = \mathbb{R} - \{-\frac{d}{c}\}$ y $f : X \longrightarrow \mathbb{R}$ dada por $f(x) = \frac{ax+b}{cx+d}$. Muestre que f es una función constante o inyectiva. Encuentre en cada caso $Im(f)$.

1.5.14. Dé un ejemplo de conjuntos no vacíos A, B, C y funciones inyectivas

$$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} A$$

tales que ninguna de ellas es una biyección.

1.5.15. Sea $f : \mathbb{N} \longrightarrow \mathbb{N}$ dada por $f(n) = n^2$.

(1) Exhiba dos inversas izquierdas de f.
(2) Demuestre que f no tiene inversa derecha.

1.5.16. Sean $h : A' \to A$ y $g : B \to B'$ funciones biyectiva y $f : A \to B$ una función. Demuestre que:

(1) Si f no es inyectiva, entonces $h \circ f$ y $f \circ g$ tampoco lo son.
(2) Si f no es suprayectiva, entonces $h \circ f$ y $f \circ g$ tampoco lo son.

1.5.17. Sea $f : A \to B$ una función. Demuestre que:

(1) Si f es inyectiva y g es un inverso izquierdo de f, entonces g es suprayectiva. En esta situación, g es inyectiva si y sólo si f es suprayectiva.
(2) Si f es suprayectiva y h es un inverso derecho de f, entonces h es inyectiva. En esta situación, h es suprayectiva si y sólo si f es inyectiva.

1.5.18. Sean $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ y $g : \mathbb{Z} \longrightarrow \mathbb{Z}$ dadas por $f(n) = 2n$ y $g(n) = \lfloor \frac{n}{2} \rfloor$. Demuestre que $g \circ f = 1_{\mathbb{Z}}$ pero $f \circ g \neq 1_{\mathbb{Z}}$.

1.5.19.

(1) Sea $\alpha : \mathbb{N} \longrightarrow \mathbb{N}$ dada por $\alpha(n) = n + 1$. Demuestre que no existe una función $g : \mathbb{N} \longrightarrow \mathbb{N}$ tal que $\alpha \circ g = 1_{\mathbb{N}}$ pero existe una infinidad de funciones $k : \mathbb{N} \longrightarrow \mathbb{N}$ tales que $k \circ \alpha = 1_{\mathbb{N}}$.
(2) Sea $\beta : \mathbb{N} \longrightarrow \mathbb{N}$ dada por

$$\beta(n) = \begin{cases} \frac{n}{2} & \text{si } n \text{ es par} \\ \frac{n-1}{2} & \text{si } n \text{ es impar} \end{cases}.$$

Pruebe que no existe una función $f : \mathbb{N} \longrightarrow \mathbb{N}$ con $f \circ \beta = 1_{\mathbb{N}}$ pero existe una infinidad de funciones $k : \mathbb{N} \longrightarrow \mathbb{N}$ tales que $\beta \circ k = 1_{\mathbb{N}}$.

1.5.20. Sea $f : \mathbb{R} \longrightarrow \mathbb{R}$ una función dada por $f(x) = ax + b$, donde $a, b \in \mathbb{R}$. ¿Para qué valores de a, b es f biyectiva? ¿Para qué valores de a, b es f biyectiva con $f \circ f = 1_{\mathbb{R}}$?.

1.5.21. Sean $f : X \longrightarrow Y$, $g : Y \longrightarrow Z$ y $h : Z \longrightarrow W$ funciones. Muestre que si $g \circ f$ y $h \circ g$ son biyectivas, entonces f, g y h también lo son.

1. 5.22. Sean $X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} X$ funciones son tales que $h \circ g \circ f$ y $f \circ h \circ g$ son suprayectivas, mientras que $g \circ f \circ h$ es inyectiva. Demuestre f, g y h son biyecciones.

1.5.23. Sean $X \xrightarrow{f} Y \xrightarrow{g} Z$ funciones. Demuestre que:

(1) Si $f \circ g$ y f biyectivas, entonces g también lo es.
(2) Si $f \circ g$ y g biyectivas, entonces f también lo es.

1.5.24. Sean $X \xrightarrow{f} Y \xrightarrow{g} Z$ funciones. Demuestre que son equivalentes:

(1) Existe una función $h : Z \longrightarrow X$ tal que $f \circ h \circ g = 1_Y$.
(2) f es suprayectiva y g es inyectiva.

Deduce que para cualquier función $\alpha : X \longrightarrow Z$ existe una función $\beta : Z \longrightarrow X$ tal que $\alpha \circ \beta \circ \alpha = \alpha$. (Sugerencia: Toma $Y = Im(\alpha)$).

1.5.25. Sea $f : X \longrightarrow Y$ una función con $X \neq \emptyset$. Demuestre que son equivalentes:

(1) f es inyectiva.
(2) Para todo $A \subseteq X$, $f^{-1}[f[A]] = A$.
(3) Para cualesquiera $A_1, A_2 \subseteq X$, $f[A_2 - A_1] = f[A_2] - f[A_1]$.
(4) Para cualesquiera $A_1, A_2 \subseteq X$, $f[A_2 \cap A_1] = f[A_2] \cap f[A_1]$.

1.5.26. Sea $f : X \longrightarrow Y$ una función. Demuestre que son equivalentes:

(1) f es suprayectiva.
(2) Para todo $\emptyset \neq B \subseteq Y$, $f^{-1}[A] \neq \emptyset$.
(3) Para todo $B \subseteq Y$, $f[f^{-1}[B]] = B$.
(4) Para todo $A \subseteq X$, $f[X - A] \supseteq Y - f[A]$.

1.5.27. Sea $f : X \longrightarrow Y$ una función. Demuestre que f es biyectiva si y sólo si $f[X - A] = Y - f[A]$ para todo $A \subseteq X$.

1.5.28.

(1) Dé un ejemplo de funciones $X \xrightarrow{f} Y \xrightarrow{g} Z$ tales que g es suprayectiva y $g \circ f$ no lo es.

(2) Dé un ejemplo de funciones $X \xrightarrow{f} Y \xrightarrow{g} Z$ tales que f es inyectiva, g es suprayectiva y $g \circ f$ no es inyectiva ni suprayectiva.

(3) Dé un ejemplo de funciones $X \xrightarrow{f} Y \xrightarrow{g} Z$ tales que f no es suprayectiva, g no es inyectiva y $g \circ f$ es biyectiva.

1.5.29. Sean f y g funciones. ¿Es posible que:

(1) $f \circ g$ sea invertible, sin que f y g no sean ambas invertibles;
(2) $f \circ g$ no sea invertible, aunque f y g sean invertibles?

1.5.30. Considere la función g definida en la página 56 (la cual se ilustra en la figura 19). Muestre que la definición de $g(4)$ es irrelevante para que $g \circ f = 1_X$.

1.5.31. Sean A, B, C y D conjuntos y $f : A \to B$, $g : B \to C$ y $h : C \to D$ funciones tales que f y h son biyectivas.

(1) Demuestre que si g es inyectiva y no suprayectiva, entonces $h \circ g \circ f$ es una función inyectiva pero no suprayectiva.
(2) Demuestre que si g es suprayectiva y no inyectiva, entonces $h \circ g \circ f$ es una función suprayectiva pero no inyectiva.

1.5.32. Sea $f : X \longrightarrow Y$ función. Demuestre que

(1) Si f es inyectiva, entonces cualquier inverso izquierdo de f es suprayectivo.
(2) Si f es suprayectiva, entonces cualquier inverso derecho de f es inyectivo.
(3) Si f tiene un inverso derecho y un inverso izquierdo, entonces f es biyectiva.
(4) Si f tiene un único inverso derecho (izquierdo), entonces f es biyectiva.

§§ Ejercicios sección 1.6.

1.6.1. Sea $X = \{1, 2, 3, 4, 5, 6\}$. Considere las siguientes relaciones en X.

(1) $R_1 = \{(1, 1), (3, 3), (1, 2), (2, 2), (6, 6), (2, 1)\}$
(2) $R_2 = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (4, 4), (4, 5), (5, 4), (5, 5), (6, 6)\}$
(3) $R_3 = \{(6, 6), (1, 4), (4, 1), (1, 1), (4, 4), (5, 5), (5, 6), (6, 5), (2, 2), (3, 3), (2, 3), (3, 2)\}$
(4) $R_4 = \{(1, 1), (2, 2), (3, 3), (3, 1), (4, 4), (5, 5), (6, 6)\}$

Determine cuales son de equivalencia y en caso de que si lo sea encuentre la partición en X inducida por ésta.

1. 6.2. Determínese si la relación dada es una relación de equivalencia y si es así descríbase la partición inducida.

a) $n \sim m$ en $\mathbb{Z}$ si $nm \geq 0$.
b) $a \sim b$ en $\mathbb{Z}$ si $a + b$ es par.
c) $a \sim b$ en $\mathbb{Z}$ si $a + b$ es impar.
d) $a \sim b$ en $\mathbb{Z}$ si $a^2 + a = b^2 + b$.
e) $x \sim y$ en $\mathbb{R}$ si $|x| = |y|$.
f) $x \sim y$ en $\mathbb{R}$ si $x^2 + y^2 = 4$.
g) $n \sim m$ en $\mathbb{N}$ si $n \neq m$.
h) $(x, y) \sim (x', y')$ en $\mathbb{R}^2$ si $y = y'$.
i) $x \sim y$ en $\mathbb{R}$ si $|x - y| \leq 3$.
j) M es el conjunto de todos los meses de este año; $a \sim b$ en M si a y b comienzan el mismo día de la semana.

1.6.3. El siguiente es un famoso argumento falso. Encuéntrese el error. “El criterio de reflexividad es redundante en las condiciones para una relación de equivalencia, ya que de $x \sim y$ y $y \sim x$ (simetría) deducimos $x \sim x$ por transitividad”.

1.6.4. Una relación R sobre un conjunto X cumple con las siguientes propiedades:

(1) $(x, x) \in R$, para todo $x \in X$;
(2) Si $(x, y) \in R$ y $(y, z) \in R$ entonces $(z, x) \in R$.

Demuestre que R es una relación de equivalencia. ¿Es cierto que toda relación de equivalencia en X satisface (1) y (2)?.

1.6.5. Sea R una relación de equivalencia en el conjunto $X = \{1, 2, 3, 4, 5, 6, 7\}$ tal que $[1]_R = \{1, 6, 7\}$, $[2]_R = \{2\}$ y $[3]_R = \{3, 4\}$.

(1) Encuentre: $[4]_R$, $[5]_R$, $[6]_R$, $[7]_R$.
(2) ¿Quién es R y X/R?

1. 6.6. Considere la relación $R = \{(a, b), (a, c), (a, a), (b, d), (c, c)\}$ definida en el conjunto $X = \{a, b, c, d\}$. Encuentra el mínimo número de elementos de $X \times X$ tal que al añadirle estos elementos a R es

(1) reflexiva;
(2) simétrica;
(3) una relación de equivalencia.

Misma pregunta para $S = \{(a,b),(a,c),(a,a),(c,c)\}$.

1.6.7.

(1) Construye una relación binaria que es simétrica y transitiva, pero no reflexiva.
(2) Demuestre que, si R es una relación en X que es transitiva, simétrica y $Dom(R) \cup Im(R) = X$, entonces R es de equivalencia en X.

1.6.8. Demuestre que si la relación R en X es de equivalencia, entonces R^{-1} también lo es.

1.6.9. Sea $X = \{1,2,3,4,5\}$.

(1) Construye una relación en X que sea reflexiva, pero no transitiva ni simétrica.
(2) Construye una relación en X que sea simétrica, pero no transitiva ni reflexiva.
(3) Construye una relación en X que sea transitiva, pero no reflexiva ni simétrica.
(4) Construye una relación en X que sea reflexiva y simétrica, pero no transitiva.
(5) Construye una relación en X que sea reflexiva y antisimétrica, pero no transitiva.
(6) Construye una relación en X que sea reflexiva y transitiva, pero no simétrica.
(7) Construye una relación en X que sea reflexiva y transitiva, pero no simétrica.
(8) Construye una relación en X que sea de equivalencia.

1.6.10. Sea $X = \{a,b,c,d,e,f\}$.

(1) Dé una relación de equivalencia R_1 en X tal que $b \in [c]_{R_1}$.
(2) Dé una relación de equivalencia R_2 en X tal que $a, b \in [c]_{R_2}$.
(3) Dé una relación de equivalencia R_3 en X tal que $b \in [c]_{R_3}$ y $e \in [f]_{R_3}$.
(4) Dé una relación de equivalencia R_4 en X tal que $b \in [c]_{R_4}$, $e \in [f]_{R_4}$ y $[c]_{R_4} \neq [f]_{R_4}$.
(5) Dé una relación de equivalencia en X que tenga exactamente dos clases de equivalencia.
(6) Dé una relación de equivalencia en X con al menos una clase de equivalencia con tres o más elementos.
(7) Dé una relación de equivalencia en X con una clase de equivalencia que tenga exactamente cuatro elementos.
(8) Dé una relación de equivalencia en X con una única clase de equivalencia que tenga exactamente tres elementos.

1.6.11. Demuestre que la relación $\sim$ en $\mathbb{Z}$ definida por

$$x \sim y \iff (x = y) \vee (x + y = 3),$$

es de equivalencia.

1.6.12. Sea A un conjunto y B un subconjunto fijo de A. Defina la relación R sobre $\mathscr{P}(A)$ como $X \sim Y$, para $X, Y \subseteq A$ si $B \cup X = B \cup Y$.

(1) Verifique que $\sim$ es una relación de equivalencia en $\mathscr{P}(A)$.¿Cuál es la relación $\sim$ si $B = \emptyset$? ¿$B = A$?.
(2) Si $A = \{1, 2, 3\}$ y $B = \{1, 2\}$, encuentre la partición de $\mathscr{P}(A)$ inducida por $\sim$.
(3) Si $A = \{1, 2, 3, 4, 5\}$ y $B = \{1, 2, 3\}$, encuentre la clase de equivalencia $[\{1, 3, 5\}]_{\sim}$.
(4) Para $A = \{1, 2, 3, 4, 5\}$ y $B = \{1, 2, 3\}$, ¿Cuántas clases de equivalencia hay en la partición inducida por $\sim$?.

1.6.13. Sea $A = \{1, 2, 3, 4, 5\} \times \{1, 2, 3, 4, 5\}$ y considere la relación R en A definida por

$$(x_1, y_1) \underset{R}{\sim} (x_2, y_2) \iff x_1 + y_1 = x_2 + y_2.$$

(1) Demuestre que R es una relación de equivalencia en A.
(2) Determine las clases de equivalencia y la partición inducida por R.

1.6.14. Sea $A = \{1, 2, 3, 4, 5, 6, 7, \}$ y considere la relación R en A definida por $x \underset{R}{\sim} y$ si $x - y$ es múltiplo de 3.[20]

(1) Demuestre que R es una relación de equivalencia en A.
(2) Determine las clases de equivalencia y la partición inducida por R.

1.6.15. Considere la relación R en $\mathbb{Z}^+$ definida por: $x \underset{R}{\sim} y$ si y sólo si $x = 2^n y$ para algún $n \in \mathbb{Z}$.

(1) Demuestre que R es una relación de equivalencia en $\mathbb{Z}^+$.
(2) ¿Cuántas clases de equivalencia distintas encontramos entre [1], [2], [3] y [4]?
(3) ¿Cuántas clases de equivalencia distintas encontramos entre [6], [7], [21], [24], [28], [35], [42] y [48]?

1.6.16. Suponga $Y \subset X$ y considere la relación R en $\mathscr{P}(X)$ definida por

$$A \underset{R}{\sim} B \iff A \bigtriangleup B \subseteq Y,$$

para todo $A, B \subseteq X$.

(1) Demuestre que R es una relación de equivalencia en $\mathscr{P}(X)$.

[20] Un múltiplo de 3 es un entero x tal que $x = 3y$ para algún $y \in \mathbb{Z}$.

(2) Demuestre que para todo $A \in \mathscr{P}(X)$ existe un único $B \in [A]_R$ tal que $B \cap Y = \varnothing$.

1.6.17. Sea $f : X \longrightarrow Y$ una función. Defina la siguiente relación en X como sigue

$$a \sim b \iff f(a) = f(b),$$

para $a, b \in X$. Demuestre que $\sim$ es una relación de equivalencia en X.

1.6.18. Sean R y S relaciones de equivalencia en X tales que $X/R = X/S$. Demuestre que $R = S$.

1.6.19. Sean R y S relaciones de equivalencia en X.

(1) Demuestre que $R \cap S$ es una relación de equivalencia en X.
(2) Demuestre que para todo $x \in X$, $[x]_{R\cap S} = [x]_R \cap [x]_S$.

1.6.20. Sea R una relación de equivalencia en X y $Y \subseteq X$. Sea $S = R \cap (Y \times Y)$.

(1) Demuestre que S es una relación de equivalencia en Y.
(2) Demuestre que para todo $y \in Y$, $[y]_S = [y]_R \cap Y$.

1.6.21. Sean R y S relaciones de equivalencia en X tales que $X/R = X/S$. Demuestre que $R = S$.

1.6.22. Sean X y Y conjuntos ajenos. Sea R una relación de equivalencia en X y S una relación de equivalencia en Y.

(1) Demuestre que $R \cup S$ es una relación de equivalencia en $X \cup Y$.
(2) Demuestre que para todo $x \in X$, $[x]_{R\cup S} = [x]_R$, y para todo $y \in Y$, $[y]_{R\cup S} = [y]_S$.
(3) Demuestre que $(X \cup Y)/(R \cup S) = (X/R) \cup (Y/S)$

1.6.23. Sea R una relación de equivalencia en X y S una relación de equivalencia en Y. Definimos la relación T en $X \times Y$ por

$$(x, y) \underset{T}{\sim} (x', y') \iff (x \underset{R}{\sim} x') \wedge (y \underset{S}{\sim} y'),$$

para todo $(x, y), (x', y') \in X \times Y$

(1) Demuestre que T es una relación de equivalencia en $X \times Y$.
(2) Demuestre que si $x \in X$ y $y \in Y$, entonces $[(x, y)]_T = [x]_R \times [y]_S$.

1.6.24. Sea $R \subseteq X \times X$. Demuestre que R es de equivalencia en X si y sólo si $(R \circ R^{-1}) \cup \Delta_X = R$.

1.6.25. Muestre que la unión $R_1 \cup R_2$ de dos relaciones de equivalencia R_1 y R_2 en X es de equivalencia si y sólo si $R_1 \cup R_2 = R_1 \circ R_2$.

1.6.26. Sean R y S dos relaciones de equivalencia en un conjunto X. Pruebe que las afirmaciones siguientes son equivalentes:

(1) $R \cup S$ es una relación de equivalencia.
(2) $S \circ R \subseteq R \cup S$ y $R \circ S \subseteq R \cup S$.

1.6.27. Demuestre que la composición $R_1 \circ R_2$ de dos relaciones de equivalencia R_1 y R_2 en X es de equivalencia si y sólo si $R_1 \circ R_2 = R_2 \circ R_1$.

1.6.28. Pruebe que una relación R en X es de equivalencia si y sólo si $\Delta_X \subseteq R$, $R = R^{-1}$ y $R = R \circ R$.

Particiones

1.6.29. Determine si cada una de las siguientes colecciones de conjuntos es partición para el conjunto dado A. Si la colección no es una partición, indique por qué.

(1) $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$; $P = \{\{4, 5, 6\},\ \{1, 8\},\ \{2, 3, 7\}\}$.
(2) $A = \{a, b, c, d, e, f, g, h\}$; $P = \{\{d, e\},\ \{a, c, d\},\ \{f, h\},\ \{b, g\}\}$.
(3) $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$; $P = \{\{1, 3, 4, 7\},\ \{2, 6\},\ \{5, 8\}\}$.
(4) $A = \{a, b, c, d\}$; $P = \{\{a, b\},\ \{c, d\},\ \varnothing\}$.
(5) $A = \{1, 2, 3, 4\}$; $P = \{\{1, 2, 3, 4\}\}$.
(6) $A = \mathbb{Q}$; $P = \{\{n \in \mathbb{Q} \mid n^2 < 2\}, \{n \in \mathbb{Q} \mid n^2 > 2\}\}$.

1.6.30. Sea $X = \{1, 2, 3, 4, 5, 6, 7, 8\}$.

(1) Dé una partición $\{X_1, X_2, X_3\}$ de X de modo que: $3, 4 \in X_2$, $5, 6 \in X_3$ y X_1 tiene exactamente tres elementos.
(2) Dé una partición $\{X_1, X_2, X_3\}$ de X de modo que: $1, 2 \in X_1$, $3, 4 \in X_2$ y $5, 6 \in X_3$.
(3) Dé una partición $\{X_1, X_2, X_3, X_4\}$ de X de modo que: $1, 2, 3, 4 \in X_1$ y $5 \in X_3$.

1.6.31. Sea $X = \{1, 2, 3\}$.

(*a*) Determine todas las particiones de X.
(*b*) Para cada una de las particiones del inciso (*a*) encuentre la relación de equivalencia inducida por ésta, listando todos sus elementos.

1.6.32. Sea $X = \{1, 2, 3, 4\}$. Para cada una de las siguientes particiones de X determine la relación de equivalencia inducida por ésta, listando todos sus elementos.

(1) $\{\{1,2\},\{3,4\}\}$
(2) $\{\{1\},\{2\},\{3,4\}\}$
(3) $\{\{1\},\{2\},\{3\},\{4\}\}$
(4) $\{\{1,2,3\},\{4\}\}$
(5) $\{\{1,2,3,4\}\}$
(6) $\{\{1\},\{2,4\},\{3\}\}$

1.6.33. Sea $X = X_1 \cup X_2 \cup X_3$, donde $X_1 = \{1,2\}$, $X_2 = \{2,3,4\}$ y $X_3 = \{5\}$. Considere la relación R en X definida por: $x \underset{R}{\sim} y$ si x y y están en el mismo subconjunto X_i, para algún $1 \leq i \leq 3$. ¿Es ésta una relación de equivalencia?

1.6.34. Sea R una relación de equivalencia en X, S y S' dos conjuntos de representantes para esta relación. Demostrar que las particiones asociadas a R considerando cada uno de los conjunto S y S' son iguales.

1.6.35. Sea $f : X \longrightarrow Y$ una función suprayectiva. Sea

$$P = \{f^{-1}[\{y\}] \mid y \in Y\}.$$

Demuestre que P es una partición de X y escriba la relación de equivalencia asociada a P.

1.6.36. Sean X y Y conjuntos ajenos. Si P es una partición de X y Q una partición de Y, entonces $P \cup Q$ es una partición de $X \cup Y$.

1.6.37. Sea X un conjunto no vacío y $\{X_i\}_{i\in I}$ una partición de X. ¿Es $\{\mathscr{P}(X_i)\}_{i\in I}$ una partición de $\mathscr{P}(X)$?

1.6.38.

(1) Para todo $x \in \mathbb{R}$, sea $A_x = \{x, -x\}$. Demuestre que $\{A_x \mid x \in \mathbb{R}\}$ es una partición de $\mathbb{R}$.
(2) Para todo $n \in \mathbb{N}$, sea $B_n = \{x \in \mathbb{R} \mid n \leq x < n+1\}$. Demuestre que $\{B_n \mid n \in \mathbb{N}\}$ es una partición de $\mathbb{R}$.
(3) Para todo $r \in \mathbb{R}$, sea $C_r = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid x + y = r\}$. Pruebe que $\{C_r \mid r \in \mathbb{R}\}$ es una partición de $\mathbb{R} \times \mathbb{R}$.
(4) Para todo $r \in \mathbb{Q}$ con $0 \leq r < 1$, sea $A_r = \{x \in \mathbb{Q} \mid x - \lfloor x \rfloor = r\}$. Pruebe que $\{A_r \mid 0 \leq r < 1\}$ es una partición de $\mathbb{Q}$.

1.6.39. Sean X un conjunto, R una relación de equivalencia en X y P_R el conjunto de las clases de equivalencia. Considere la función

$$f : X \to P_R, \text{ dada por } f(x) = [x].$$

Demuestre que f es biyectiva si y sólo si $R = \Delta_X$.

1.6.40. Se define una relación R en $\mathbb{R}$ como: $a \sim b \underset{def.}{\Leftrightarrow} a - b \in \mathbb{Z}$. Demuestre que R es de equivalencia y encuentra la partición asociada.

1.6.41. En el conjunto $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ defina la relación $R \subseteq \mathbb{R}^2 \times \mathbb{R}^2$ como:

$$(a, b) \sim (c, d) \iff a - c \in \mathbb{Z} \wedge b - d \in \mathbb{Z}.$$

Demuestre que R es una relación de equivalencia. Determínese el conjunto cociente.

1.6.42.

(1) Si A es el conjunto de rectas $\mathfrak{L}$ en el plano, muestre que la relación $\mathfrak{L}_1 \| \mathfrak{L}_2$ ($\mathfrak{L}_1$ es paralela a $\mathfrak{L}_2$) es una relación de equivalencia.
(2) Considere el círculo unitario $S^1 \subseteq \mathbb{R}^2$ definido por

$$S^1 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$$

y defina la relación siguiente en S^1: dos puntos $P, Q \in S^1$ están relacionados, denotado $P \sim Q$, si y sólo si P y Q son iguales o están en los extremos opuestos de una diagonal de S^1, entiéndase por diagonal cualquier segmento que pasa por el centro de S^1 y cuyos extremos son puntos de S^1. Demuestre que $\sim$ es una relación de equivalencia en S^1. Determínese el conjunto cociente.

1.6.43. Considere la siguiente relación en $\mathbb{Z}$: $a \sim b \underset{def.}{\Leftrightarrow} ab > 0$ o $a = b = 0$. Demuestre que es de equivalencia y encuentre la partición asociada.

1.6.44. (1) ¿Es cierto que si R es una relación de equivalencia en un conjunto A infinito, entonces el conjunto cociente A/R ha de ser necesariamente un conjunto infinito?
(2) ¿Es cierto que si R es una relación de equivalencia definida en un conjunto A infinito, entonces cada clase de equivalencia ha de ser también un conjunto infinito?

(3) Si R es una relación de equivalencia definida en un conjunto finito A de modo que R y A tienen el mismo número de elementos, ¿qué se puede afirmar sobre la relación R?

§§ Ejercicios sección 1.7.

1.7.1. Determine cuáles de las siguientes relaciones en $X = \{1, 2, 3, 4\}$ son órdenes parciales en X.

(1) $R_1 = \{(2, 1), (1, 3), (4, 4), (2, 3)\}$.
(2) $R_2 = \{(1, 2), (1, 3), (2, 3), (1, 4), (3, 4), (2, 4)\}$.
(3) $R_3 = \{(1, 3), (4, 2), (2, 1), (4, 1), (2, 3), (4, 3)\}$.
(4) $R_4 = \{(1, 4), (2, 1), (1, 3), (2, 3), (2, 4)\}$.
(5) $R_5 = \{(3, 2), (2, 1), (3, 1)\}$.

En los casos en que sí es un orden parcial:

(a) Encuentre los elementos maximales, minimales, máximo y mínimo, si existen del conjunto X en cada caso.
(b) ¿Cuáles son órdenes totales?

1.7.2. Sea $X = \{a, b, c, d, e\}$. Definimos el siguiente orden en X: $a < b$, $a < c$, $b < c$, $d < c$ y $d < e$.

(1) Verifique que $<$ es un orden parcial en X. ¿Es éste un orden total?
(2) Encuentre los elementos maximales, minimales, máximo y mínimo, si existen del conjunto X.
(3) Encuentre las cotas superiores e inferiores del conjunto $Y = \{b, d\}$ en X. ¿Existen ínf Y y sup Y?.
(4) Obtener algún subconjunto de X con más de dos elementos que esté totalmente ordenado.

1.7.3. Sea $X = \{a, b, c\}$. Determine todos los órdenes parciales $<$ sobre X tales que

(1) $a < b$.
(2) b es un elemento minimal.
(3) c es un elemento máximo.

1.7.4. Sea $X = \{1, 2, 3, 4\}$.

(1) Determine todos los órdenes parciales sobre X tales que 1 y 2 son comparables pero 3 y 4 no lo son.
(2) ¿Cuántos órdenes totales hay en el conjunto $X = \{1, 2, 3, 4\}$? ¿Cuáles son?.

1.7.5. Un empleado de un centro de cómputos, tiene que ejecutar 10 programas $P_0, P_1, \ldots, P_9$ que, debido a las prioridades, están restringidos a las siguientes condiciones:
$P_9 > P_7$, $P_9 > P_2$, $P_7 > P_6$, $P_6 > P_4$, $P_2 > P_8$, $P_2 > P_5$, $P_5 > P_3$, $P_5 > P_0$, $P_8 > P_3$, $P_8 > P_4$, $P_3 > P_1$, $P_4 > P_1$, $P_0 > P_1$,
donde, por ejemplo, $P_i > P_j$ significa que el programa P_i debe realizarse antes que el programa P_j. Determine un orden para estos programas de modo que se satisfagan las restricciones.

1.7.6. Sea $X = \{2, 3, 4, 6, 9, 12, 18, 36\}$. Definimos en X el siguiente orden

$$a \leq b \iff \text{existe } k \in \mathbb{N} \text{ tal que b=ak.}$$

(1) Demuestre $\leq$ es un orden parcial en X.
(2) Encontrar los elementos maximales, minimales, máximo y mínimo, (si los hay) de X
(3) Encontrar las cotas inferiores, cotas superiores, supremo e ínfimo, si existen, para el subconjunto $Y = \{2, 4, 6, 12\}$ de X.

1.7.7. Determine si las siguientes relaciones $\leq$ en $\mathbb{Z}$ son órdenes parciales y si sí determine el orden parcial $<$ inducido por éste.

(1) $a \leq b$ si y sólo si $a = 2b$.
(2) $a \leq b$ si y sólo si $a - b$ es un entero par no negativo.
(3) $a \leq b$ si y sólo si $a^2 = b^2$.
(4) $a \leq b$ si y sólo si $a = b^k$ para algún $k \in \mathbb{N} - \{0\}$. Observe que k depende de a y b.

1.7.8. Sea X un conjunto. Demuestre que:

(1) $(\mathscr{P}(X), \subsetneq)$ es un orden parcial;
(2) $(\mathscr{P}(X), \subsetneq)$ es orden total si y sólo si X tiene a lo más un elemento.

1.7.9. Complete al demostración del lema 1.7.6

1.7.10. Sea $A = \{1, 2, 3, 4\}$. Considere el conjunto parcialmente ordenado $(\mathscr{P}(A), \subseteq)$. Para cada uno de los siguientes subconjuntos X (de $\mathscr{P}(A)$), determine el ínfimo y el supremo de X.

(1) $X = \{\{1\}, \{2\}\}$
(2) $X = \{\{1\}, \{2\}, \{3\}, \{1, 2\}\}$
(3) $X = \{\varnothing, \{1\}, \{2\}, \{1, 2\}\}$

(4) $X = \{\{1\}, \{1,2\}, \{1,3\}, \{1,2,3\}\}$
(5) $X = \{\{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}\}$
(6) $X = \{\{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$

1.7.11. Sea $A = \{1,2,3,4,5,6,7\}$. Considere el conjunto parcialmente ordenado $(\mathscr{P}(A), \subseteq)$. Para $X = \{\{1\}, \{2\}, \{2,3\}\} \subseteq \mathscr{P}(A)$, determine lo siguiente:

(1) El número de cotas superiores de X que contienen
(a) 3 elementos de A, (b) 4 elementos de A, (c) 5 elementos de A.
(2) El número de cotas superiores para X.
(3) El supremo de X.
(4) El número de cotas inferiores de X.
(5) El ínfimo de X.

1.7.12. Sean A, B y C subconjuntos del conjunto E. Ordene por inclusión ($\subseteq$) a los siguientes conjuntos

(1) $E_1 = B \cap C$
(2) $E_2 = \varnothing$
(3) $E_3 = A \cup B \cup C$
(4) $E_4 = C \cap (A \cup B)$
(5) $E_5 = B \cup C$
(6) $E_6 = A \cap B \cap C$
(7) $E_7 = C \cup (A \cap B)$

1.7.13. Demuestre que el conjunto A dado en el ejemplo 1.7.17 no está acotado superiormente.

1.7.14.

(1) Dé un ejemplo de un conjunto parcialmente ordenado que tenga tres elementos minimales y dos elementos maximales.
(2) Dé un ejemplo de un conjunto parcialmente ordenado que tiene elemento máximo y mínimo, pero no es un orden total.
(3) Dé un ejemplo de un conjunto totalmente ordenado que no tiene máximo ni mínimo.
(4) Dé un ejemplo de un conjunto parcialmente ordenado que es total pero no es un buen orden.
(5) Dé un ejemplo de un conjunto parcialmente ordenado con un único elemento minimal y sin un elemento mínimo.

1.7.15. Dé ejemplos de un conjunto parcialmente ordenado $(X, <)$ y un subconjunto Y de X tal que

(1) Y no tiene elemento máximo en X;
(2) Y no tiene elemento mínimo en X;
(3) Y tiene supremo en X, pero no tiene máximo;
(4) Y no tiene supremo en X.

1.7.16. Sea $(X, <)$ un conjunto parcialmente ordenado y $Y \subseteq X$.

(1) Demuestre que el supremo (ínfimo) de Y, si existe, es único.
(2) ¿En qué caso X tiene supremo? ¿en qué caso lo tiene $\emptyset$?. ¿En qué caso X tiene ínfimo?, ¿en qué caso lo tiene $\emptyset$?. ¿Qué elementos de X son, si existen, $\sup X$, $\inf X$, $\sup \emptyset$, $\inf \emptyset$?.
(3) Si $(X, <)$ tiene la propiedad de que todo subconjunto no vacío con una cota superior tiene supremo, pruebe que X tiene la propiedad de que cualquier subconjunto de X no vacío con una cota inferior tiene ínfimo.

1.7.17. Sea $(X, \leq)$ un conjunto parcialmente ordenado, y sean $A \subseteq B \subseteq X$. Suponiendo que existen $\inf B$, $\inf A$, $\sup A$ y $\sup B$, demuestre que

$$\inf B \leq \inf A \leq \sup A \leq \sup B.$$

1.7.18. Sea $(X, \leq)$ un conjunto parcialmente ordenado, y sean A y B subconjuntos no vacíos de X. Escribimos $A \leq B$ en el caso en que todo elemento de A es menor o igual que todo elemento de B, es decir, $x \leq y$ para todo $x \in A$ y $y \in B$. Si existen $\inf B$, $\sup A$, demuestre que si $A \leq B$ entonces $\sup A \leq \inf B$.

1.7.19. Sea $\varphi : A \times A \longrightarrow A$ tal que, para todo $x, y, z \in A$,

$$\begin{aligned} \varphi(x, y) &= \varphi(y, x) \\ \varphi(x, \varphi(y, z)) &= \varphi(\varphi(x, y), z) \\ \varphi(x, x) &= x \end{aligned}$$

Definimos $x \leq y \iff \varphi(x, y) = x$. Pruebe que

(1) $\leq$ es un orden parcial en A;
(2) $\varphi(x, y)$ es el ínfimo del subconjunto $\{x, y\}$ de A.

1.7.20.

(1) Sea $(X, <)$ un conjunto parcialmente ordenado. Definimos

$$x <^* y \iff y < x.$$

Demuestre que $(X, <^*)$ es un conjunto parcialmente ordenado. A dicho orden se le llama orden **inverso** o **dual** del orden $<$ en X. ¿Qué se puede decir acerca de $<^*$ cuando $<$ es un orden total?.

(2) Demuestre que para $Y \subseteq X$ se cumple

(a) y es el elemento mínimo de Y respecto a $<^*$ si y sólo si y es el elemento máximo de Y respecto a $<$.

(b) Similarmente para minimal y maximal, y supremo e ínfimo.

1.7.21. Sean $(X, <_1)$ y $(Y, <_2)$ dos conjuntos parcialmente ordenados. Demuestre que $<_3$ es un orden parcial en $X \times Y$, donde $<_3$ se define como $(x_1, y_1) <_3 (x_2, y_2)$ si y sólo si $x_1 <_1 x_2$ y $y_1 <_2 y_2$. El conjunto ordenado $(X \times Y, <_3)$ se llama **producto (cartesiano)** de los conjuntos ordenados $(X, <_1)$ y $(Y, <_2)$.

1.7.22. Sean $(A, \leq_A)$ y $(B, \leq_B)$ dos conjuntos parcialmente ordenados. En $A \times B$ se define la relación $\leq$ dada por

$$(a_1, b_1) \leq (a_2, b_2) \iff (a_1 <_A a_2) \vee (a_1 = a_2 \wedge b_1 \leq_B b_2).$$

(1) Demuestre que $\leq$ es un orden parcial sobre $A \times B$, llamado **orden lexicográfico**.

(2) ¿Qué se puede decir acerca de $(A \times B, \leq)$ si $(A, \leq_A)$ y $(B, \leq_B)$ son conjuntos totalmente ordenados?

(3) ¿Qué se puede decir acerca de $(A \times B, \leq)$ si $(A, \leq_A)$ y $(B, \leq_B)$ son conjuntos bien ordenados?

(4) Sea $A = \mathbb{N} \times \mathbb{N}$ con el orden lexicográfico definido a partir del orden usual en $\mathbb{N}$. Indicar cuáles de las siguientes afirmaciones son verdaderas y cuáles falsas, justificando su respuesta:

(I) $(2, 15) \leq (3, 2)$

(II) $(16, 1) \leq (15, 112)$

(III) $(4, 12) \leq (4, 20)$

(IV) $(3, 12) \leq (3, 10)$

1.7.23.

(1) Sea $(A, <)$ un conjunto ordenado, y sea $b \notin A$. Definimos la relación $<'$ en $B = A \cup \{b\}$ como sigue

$$x <' y \iff (x, y \in A \wedge x < y) \vee (y = b \wedge x \in A).$$

Demuestre que $<'$ es un orden sobre B tal que $<' \cap (A \times A) = <$.

(2) Sean $(A_1, <_1)$, $(A_2, <_2)$ dos conjuntos ordenados tales que $A_1 \cap A_2 = \emptyset$. Definimos la relación $<_3$ en $B = A_1 \cup A_2$ como sigue

$$x <_3 y \iff (x, y \in A_1 \ \wedge \ x <_1 y) \ \vee \ (x, y \in A_2 \ \wedge \ x <_2 y) \ \vee \ (x \in A_1 \ \wedge \ y \in A_2).$$

Demuestre que $<_3$ es un orden sobre B tal que $<_3 \cap (A_1 \times A_1) = <_1$, $<_3 \cap (A_2 \times A_2) = <_2$. (Intuitivamente $<_3$ pone a todo elemento de A_2 después de todo elemento de A_1 y coincide con los órdenes originales en A_1 y A_2; esta es la razón de que el orden $<_3$ se llama **orden de yuxtaposición**). ¿Qué se puede decir acerca de $(B, <_3)$ si $(A_1, <_1)$ y $(A_2, <_2)$ son conjuntos totalmente ordenados?. ¿Qué se puede decir acerca de $(B, <_3)$ si $(A_1, <_1)$ y $(A_2, <_2)$ son conjuntos bien ordenados?.

1.7.24. Consideremos $f : A \longrightarrow B$ un **isomorfismo** de los conjuntos parcialmente ordenados $(A, <_A)$ y $(B, <_B)$, es decir, una función biyectiva de A en B verificando que para todo $a_1, a_2 \in A$

$$a_1 <_A a_2 \iff f(a_1) <_B f(a_2).$$

Demuestre que:

(1) a es maximal (minimal) de A si y sólo si $f(a)$ es maximal (minimal) de B.
(2) a es el máximo (mínimo) de A si y sólo si $f(a)$ es el máximo (mínimo) de B.
(3) Si $C \subseteq A$, entonces a es cota superior (inferior) de C si y sólo si $f(a)$ es cota superior (inferior) de $f[C]$.
(4) Si $C \subseteq A$, entonces a es el supremo (ínfimo) de C si y sólo si $f(a)$ es supremo (ínfimo) de $f[C]$.

1.7.25. Sea $(Y, <)$ un conjunto parcialmente ordenado y $f : X \longrightarrow Y$ una función biyectiva. Se define en X el siguiente orden

$$x_1 <' x_2 \iff f(x_1) < f(x_2),$$

para todo $x_1, x_2 \in X$. Demuestre que $(X, <')$ es un conjunto parcialmente ordenado.

1.7.26. Sean $(A, \leq_A)$ y $(B, \leq_B)$ dos conjuntos parcialmente ordenados. Una función $f : A \longrightarrow B$ es **creciente** si para todo $x \leq_A y$ implica $f(x) \leq_B f(y)$. Una función $f : A \longrightarrow B$ es **estrictamente creciente** si para todo $x <_A y$ implica $f(x) <_B f(y)$.

(1) Sea $f : A \longrightarrow B$ una función inyectiva y creciente. Demuestre que f es estrictamente creciente. Demostrar que si $(A, \leq_A)$ es totalmente ordenado se verifica el recíproco.

(2) Sea $f : A \longrightarrow B$ una función estrictamente creciente. Probar que si b es un elemento maximal de B, entonces cada elemento de $f^{-1}(b)$ es maximal de A.

1.7.27. Dado un conjunto X describe todas las relaciones que son órdenes parciales (reflexivos) y relaciones de equivalencia al mismo tiempo.

1.7.28. Sean R y S órdenes parciales arbitrarios sobre un conjunto X. Decide cuál de las siguientes relaciones son necesariamente órdenes parciales en X:

(1) $R \cap S$;
(2) $R \cup S$;
(3) $R - S$;
(4) $R \circ S$.

1.7.29. Sean R_1 y R_2 dos órdenes totales en el conjunto X. ¿Cuándo $R_1 \circ R_2$ es también un orden total?

1.7.30. Demuestre que si R es un orden parcial (orden lineal, buen orden) sobre X y $Y \subseteq X$, entonces $R \cap (Y \times Y)$ es un orden parcial (orden lineal, buen orden) sobre Y.

1.7.31. Sea R una relación en X. Demuestre que una condición necesaria y suficiente para que R sea un orden parcial (reflexivo) sobre X es que:

(1) $R \circ R = R$.
(2) $R \cap R^{-1} = \Delta_X$.

1.7.32. Sea R una relación binaria en X. Demuestre que una condición necesaria y suficiente para que R sea un orden total (reflexivo) sobre X es que:

(1) $R \circ R = R$.
(2) $R \circ R^{-1} = X \times X$.
(3) $R \cap R^{-1} = \Delta_X$.

1.7.33. Considere la siguientes relaciones sobre el conjunto $\mathbb{N}$ de los números naturales. ($\leq$ denota el orden usual en $\mathbb{N}$)

(1) $m \preceq n \iff \begin{cases} m, n \text{ son pares y } m \leq n\text{; o} \\ m, n \text{ son impares y } m \leq n\text{; o} \\ m \text{ es impar y } n \text{ es par} \end{cases}$

(2) $m \sqsubseteq n \iff \begin{cases} m, n \text{ son pares y } m \leq n\text{; o} \\ m, n \text{ son impares y } m \leq n \end{cases}$

(3) $m \trianglelefteq n \iff \begin{cases} m, n \text{ son pares y } m \geq n; \text{ o} \\ m, n \text{ son impares y } m \leq n; \text{ o} \\ m \text{ es par y } n \text{ es impar} \end{cases}$

Demuestre que cada relación es un orden parcial sobre $\mathbb{N}$. ¿Cuál de estos órdenes es un orden total?. ¿Qué órdenes tienen elemento máximo?, si lo tiene, ¿quién es?. ¿Qué órdenes tienen elemento mínimo?, si lo tiene, ¿quién es?.

1.7.34. Un conjunto parcialmente ordenado $(X, \leq)$ es una **retícula** si para cada $a, b \in X$ el conjunto $\{a, b\}$ tiene supremo e ínfimo. Si A es un conjunto, demuestre que $(\mathscr{P}(A), \subseteq)$ es una retícula.

1.7.35. Haga un diagrama del conjunto parcialmente ordenado $(\mathcal{P}(E), \subseteq)$ para el conjunto E que se indica:

(1) $E = \varnothing$;
(2) $E = \{\varnothing\}$;
(3) $E = \{\{\varnothing\}\}$;
(4) $E = \{\varnothing, \{\varnothing\}\}$;
(5) $E = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$.

1.7.36. Si $(X, \leq)$ es una retícula, pruebe que para todo $a, b, c, d \in X$ se verifica:

(1) $a \leq c$ y $b \leq c \iff \sup\{a, b\} \leq c$.
(2) $c \leq a$ y $c \leq b \iff c \leq \text{ínf}\{a, b\}$.
(3) $a \leq b$ y $c \leq d \implies \sup\{a, c\} \leq \sup\{b, d\}$ e $\text{ínf}\{a, c\} \leq \text{ínf}\{b, d\}$.
(4) $a \leq b \implies \sup\{a, c\} \leq \sup\{b, c\}$ e $\text{ínf}\{a, c\} \leq \text{ínf}\{b, c\}$.
(5) $a \leq b \iff \sup\{a, b\} = b$.
(6) $a \leq b \iff \text{ínf}\{a, b\} = a$.
(7) $\sup\{a, b\} = b \iff \text{ínf}\{a, b\} = a$.

1.7.37. Sea $(X, \leq)$ un conjunto parcialmente ordenado. Demuestre o refute las siguientes proposiciones.

(1) Si $(X, \leq)$ es una retícula, entonces es un orden total.
(2) Si $(X, \leq)$ es un orden total, entonces es una retícula.

§§ Ejercicios sección 1.8.

1.8.1. [21] Sea $\{A_i\}_{i \in I}$ es una familia de conjuntos. Entonces

[21] Parte del teorema 1.8.6 pág. 77.

(1) $A_j \subseteq \bigcup_{i\in I} A_i$ para toda $j \in I$.
(2) Si $I \neq \emptyset$, entonces $\bigcap_{i\in I} A_i \subseteq A_j$ para toda $j \in I$.

1.8.2. [22] Sean $\{A_i\}_{i\in I}$ una familia no vacía de conjuntos y X un conjunto. Demuestre que

(1) $X \cap \left(\bigcup_{i\in I} A_i\right) = \bigcup_{i\in I}(X \cap A_i)$.
(2) $X - \left(\bigcup_{i\in I} A_i\right) = \bigcap_{i\in I}(X - A_i)$.

1.8.3. Para cada $n \in \mathbb{N}$, sea $A_n = \{1, 2, \ldots, n\}$. Determine

$(a) \bigcup_{n=0}^{7} A_n$, $(b) \bigcap_{n=0}^{11} A_n$, $(c) \bigcup_{n=0}^{m} A_n$, $(d) \bigcap_{n=0}^{m} A_n$.

1.8.4. Para cada $n \in \mathbb{N}$, sea $B_n = \{n + 1, n + 2, n + 3, \ldots\}$. Determine

$(a) \bigcup_{n=0}^{8} B_n$, $(b) \bigcap_{n=3}^{12} B_n$, $(c) \bigcup_{n\in\mathbb{N}} B_n$, $(d) \bigcap_{n=0}^{m} B_n$.

1. 8.5. Determine si los siguientes enunciados son verdaderos o falsos. Si son verdaderos, probar el resultado, y si son falsos, dar un contraejemplo.

(1) Si $x \in \bigcup_{i\in I} A_i$, entonces $x \in A_i$ para todo $i \in I$;
(2) Si $x \in A_i$ para todo $i \in I$, entonces $x \in \bigcup_{i\in I} A_i$;
(3) Si $x \in \bigcap_{i\in I} A_i$, entonces existe algún $i \in I$ tal que $x \in A_i$;
(4) Si $x \in A_i$ para algún $i \in I$, entonces $x \in \bigcap_{i\in I} A_i$;
(5) Si $\bigcap_{i\in I} A_i = \emptyset$, entonces $A_i = \emptyset$ para todo $i \in I$;
(6) Si $\bigcup_{i\in I} A_i = \emptyset$, entonces $A_i = \emptyset$ para todo $i \in I$.

1.8.6. Demuestre que:

(1) Si $A_i \subseteq B$ para todo $i \in I$, entonces $\bigcup_{i\in I} A_i \subseteq B$;
(2) Si $B \subseteq A_i$ para todo $i \in I$, entonces $B \subseteq \bigcap_{i\in I} A_i$;
(3) Si $A_i \subseteq B_i$ para todo $i \in I$, entonces $\bigcup_{i\in I} A_i \subseteq \bigcup_{i\in I} B_i$ y $\bigcap_{i\in I} A_i \subseteq \bigcap_{i\in I} B_i$.

[22] Parte del Teorema 1.2.8 pág. 78.

1.8.7. Sea $\{A_i\}_{i\in I}$ una familia de subconjuntos de X. Demuestre que con respecto al orden $\subseteq$ definido en $\mathscr{P}(X)$:

(1) $\bigcup\limits_{i\in I} A_i$ es el menor conjunto que contiene a todos los conjuntos A_i;
(2) $\bigcap\limits_{i\in I} A_i$ es el mayor conjunto que está contenido en todos los conjuntos A_i.

1.8.8. Considere dos familias de conjuntos $\{A_i\}_{i\in I}$ y $\{B_j\}_{j\in J}$. Pruebe que:

(1) $\left(\bigcup\limits_{i\in I} A_i\right) \cap \left(\bigcup\limits_{j\in J} B_j\right) = \bigcup\limits_{(i,j)\in I\times J} \left(A_i \cap B_j\right)$;
(2) $\left(\bigcap\limits_{i\in I} A_i\right) \cup \left(\bigcap\limits_{j\in J} B_j\right) = \bigcup\limits_{(i,j)\in I\times J} \left(A_i \cup B_j\right)$;
(3) $\left(\bigcup\limits_{i\in I} A_i\right) \times \left(\bigcup\limits_{j\in J} B_j\right) = \bigcup\limits_{(i,j)\in I\times J} \left(A_i \times B_j\right)$;
(4) $\left(\bigcap\limits_{i\in I} A_i\right) \times \left(\bigcap\limits_{j\in J} B_j\right) = \bigcup\limits_{(i,j)\in I\times J} \left(A_i \times B_j\right)$;
(5) $\bigcap\limits_{i\in I} \mathscr{P}(A_i) = \mathscr{P}\left(\bigcap\limits_{i\in I} A_i\right)$;
(6) $\bigcup\limits_{i\in I} \mathscr{P}(A_i) \subseteq \mathscr{P}\left(\bigcup\limits_{i\in I} A_i\right)$.

1.8.9. Demuestre que:

(1) $\bigcup\limits_{i\in I}\left(\bigcup\limits_{j\in J} A_{ij}\right) = \bigcup\limits_{j\in J}\left(\bigcup\limits_{i\in I} A_{ij}\right)$;
(2) $\bigcap\limits_{i\in I}\left(\bigcap\limits_{j\in J} A_{ij}\right) = \bigcap\limits_{j\in J}\left(\bigcap\limits_{i\in I} A_{ij}\right)$;
(3) $\bigcup\limits_{j\in J}\left(\bigcap\limits_{i\in I} A_{ij}\right) \subseteq \bigcap\limits_{i\in I}\left(\bigcup\limits_{j\in J} A_{ij}\right)$
(4) Dé un ejemplo para mostrar que en el inciso (3), $\subseteq$ no se puede cambiar por $=$.

1.8.10. Sea $f : X \longrightarrow Y$ una función y sean $\{A_i\}_{i\in I}$ y $\{B_j\}_{j\in J}$ familias de subconjuntos de X y Y respectivamente. Pruebe que:

(1) $f\left[\bigcup\limits_{i\in I} A_i\right] = \bigcup\limits_{i\in I} f[A_i]$;

(2) $f^{-1}\left[\bigcup_{j\in J} B_j\right] = \bigcup_{j\in J} f^{-1}\left[B_j\right]$;

(3) $f\left[\bigcap_{i\in I} A_i\right] \subseteq \bigcap_{i\in I} f\left[A_i\right]$;

(4) $f^{-1}\left[\bigcap_{j\in J} B_j\right] = \bigcap_{j\in J} f^{-1}\left[B_j\right]$.

1.8.11. Sea $f : X \longrightarrow Y$ una función y $\{A_i\}_{i\in I}$ una familia de subconjuntos de X. Si f es una función inyectiva demuestre que $f\left[\bigcap_{i\in I} A_i\right] = \bigcap_{i\in I} f\left[A_i\right]$.

1. 8.12. Sea $\{A_n\}_{n\in\mathbb{N}}$ una familia de subconjuntos de X. Pongamos $E_0 = \varnothing$ y $F_0 = A_0$. Para $n \geq 1$, sea

$$E_n = \bigcup_{i=1}^{n} A_i, \qquad F_n = A_n - E_{n-1}.$$

Muestre que

(1) Si $n \neq m$, entonces $F_n \cap F_m = \varnothing$;
(2) $\bigcup_{n\in\mathbb{N}} E_n = \bigcup_{n\in\mathbb{N}} F_n = \bigcup_{n\in\mathbb{N}} A_n$.

1. 8.13. Sea X un conjunto, y sea $\{R_i\}_{i\in I}$ una familia de ordenes parciales en X. Pruebe que $\bigcap_{i\in I} R_i$ es un orden parcial en X.

1.8.14. Sea $\{X_i\}_{i\in I}$ una familia de conjuntos no vacíos, y sean A_i y B_i subconjuntos no vacíos de X_i, para cada $i \in I$. Demuestre que:

(1) $\left(\bigtimes_{i\in I} A_i\right) \cap \left(\bigtimes_{i\in I} B_i\right) = \bigtimes_{i\in I} (A_i \cap B_i)$;
(2) $\left(\bigtimes_{i\in I} A_i\right) \cup \left(\bigtimes_{i\in I} B_i\right) \subseteq \bigtimes_{i\in I} (A_i \cup B_i)$;

1. 8.15. Sea $I \neq \varnothing$ un conjunto de índices. Considere dos familias de conjuntos $\{A_i\}_{i\in I}$ y $\{B_i\}_{i\in I}$. Muestre lo siguiente:

(1) Si $A_i \subseteq B_i$ para cada $i \in I$, entonces $\bigtimes_{i\in I} A_i \subseteq \bigtimes_{i\in I} B_i$.
(2) El recíproco del inciso anterior se cumple si $\bigtimes_{i\in I} A_i \neq \varnothing$.

1.8.16. Sea $\{A_i\}_{i\in I}$ una familia de conjuntos no vacíos. Para cada $j \in I$, se define la **proyección en la j-ésima coordenada** como la función $p_j : \bigtimes_{i\in I} A_i \longrightarrow A_j$ dada por $p_j((a_i)_{i\in I}) = a_j$. Pruebe que p_j es suprayectiva.

1.8.17. Sea $\{A_i\}_{i\in I}$ una familia de conjuntos no vacíos, y para cada $i \in I$ sea B_i un subconjunto de A_i. Demuestre que en $\bigtimes_{i\in I} A_i$ se cumple lo siguiente:

(1) $\bigtimes_{i\in I} B_i = \bigcap_{i\in I} p_i^{-1}[B_i]$;

(2) $\left(\bigtimes_{i\in I} A_i\right) - p_j^{-1}[B_j] = p_i^{-1}[A_j - B_j]$;

(3) $\left(\bigtimes_{i\in I} A_i\right) - \left(\bigtimes_{i\in I} B_i\right) = \bigcup_{i\in I} p_i^{-1}[A_i - B_i]$.

1.8.18. Pruebe que si $\{A_i\}_{i\in I}$ una familia de conjuntos no vacía, entonces para cualquier conjunto X y cualquier familia $\{f_i\}_{i\in I}$ de funciones $f_i : X \longrightarrow A_i$, existe una única función

$$f_i : X \longrightarrow \bigtimes_{i\in I} A_i$$

tal que para cada $i \in I$, $f_i = p_i \circ f$. Las funciones f_i se llaman funciones coordenadas de f, y a veces f se denota por $\{f_i\}_{i\in I}$ o bien por $\bigtimes_{i\in I} f_i$.

1.8.19. Sea $\{I_j\}_{j\in J}$ una partición del conjunto I. Determine una función inyectiva entre los conjuntos

$$\bigtimes_{i\in I} A_i \quad \text{y} \quad \bigtimes_{j\in J}\left(\bigtimes_{i\in I_j} A_i\right).$$

"¿Es en rigor verdadera una imagen en cuanto mera cosa visible y tangible?
Friedrich Ludwig Gottlob Frege
1848 - 1925

Capítulo **2**

Los números naturales

§ 2.1. Números naturales, suma, producto y orden

Los números naturales es el sistema numérico más primitivo que conocemos. En la antigüedad se les usaba aun sin tener un concepto claro de lo que un número natural es, simplemente se le dio un nombre con su respectiva notación (según la region) y se usaban básicamente para "contar" objetos. Por ejemplo, 1, llamado uno, denota el número de objetos que tiene un conjunto con un único elemento; 2, llamado dos, denota el número de objetos que tiene un conjunto que consta de una pareja de objetos distintos, etc. De esta manera cuando se hablaba de un número determinado de objetos se entendía a "cuántos" objetos se referían.

En este capítulo simplemente presentaremos los números naturales, aceptaremos que se conocen la suma y el producto junto con sus propiedades y definiremos el orden. Introduciremos un axioma que satisfacen los números naturales, llamado *Principio de Inducción Completa* y demostraremos que es equivalente al llamado *Axioma del Buen Orden* que dice que el orden definido en los números naturales es un buen orden (véase definición 1.7.18). Algunos resultados que introducimos aquí no podremos demostrarlos con lo que tenemos hasta el momento, así que los aceptaremos.

El lector interesado en una construcción formal de los números naturales pueden remitirse al capítulo 5. Es ahí donde se justifican los resultados que aquí se presentan.

Denotaremos con $\mathbb{N}$ al conjunto de los números naturales:

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}^1$$

La *suma* $+$ y el *producto* $\cdot$ de números naturales tienen las siguientes propiedades.

Propiedades de la Suma. Para cualesquiera $m, n, r \in \mathbb{N}$

(S_1) $(m + n) + r = m + (n + r)$	(propiedad asociativa)
(S_2) $m + n = n + m$	(propiedad conmutativa)
(S_3) $m + 0 = 0 + m = m$	(existencia de neutro aditivo: 0)
(S_4) Si $m + n = m + r$, entonces $n = r$	(ley de cancelación por la izquierda)
$(S_{4'})$Si $m + n = r + n$, entonces $m = r$	(ley de cancelación por la derecha)

Propiedad del Producto. Para cualesquiera $m, n, r \in \mathbb{N}$

(P_1) $(m \cdot n) \cdot r = m \cdot (n \cdot r)$	(propiedad asociativa)
(P_2) $m \cdot n = n \cdot m$	(propiedad conmutativa)
(P_3) $m \cdot 1 = 1 \cdot m = m$	(existencia de neutro multiplicativo: 1)
(P_4) Si $m \cdot n = m \cdot r$ y $m \neq 0$, entonces $n = r$	(ley de cancelación por la izquierda)
$(P_{4'})$Si $m \cdot n = r \cdot n$ y $n \neq 0$, entonces $m = r$	(ley de cancelación por la derecha)

Distributividad del Producto sobre la suma. Para cualesquiera $m, n, r \in \mathbb{N}$

(D) $\quad m \cdot (n + r) = m \cdot n + m \cdot r.$

Las propiedades (S_4) y $(S_{4'})$ son equivalentes y lo mismo sucede con (P_4) y $(P_{4'})$. Cada una de ellas se deduce de la otra usando la conmutatividad.

Proposición 2.1.1. *El neutro aditivo y el neutro multiplicativo son únicos, es decir,* 0 *y* 1 *son los únicos números naturales que satisfacen respectivamente* $m + 0 = m = 0 + m$ *y* $m \cdot 1 = m = 1 \cdot m$ *para todo* $m \in \mathbb{N}$.

Demostración. Supongamos que 0 y $0'$ son neutros aditivos. Entonces,

(1) $0' = 0' + 0$, por ser 0 neutro aditivo y,
(2) $0 = 0' + 0$, por ser $0'$ neutro aditivo.

Por lo tanto $0' = 0' + 0 = 0$. De manera análoga se demuestra que 1 es el único neutro multiplicativo. ∎

Usando las propiedades dadas de la suma y el producto se tiene

Proposición 2.1.2.

(1) $m \cdot 0 = 0$ *para toda* $m \in \mathbb{N}$.
(2) Si $m, n \in \mathbb{N}$ *y* $m \cdot n = 0$, *entonces* $m = 0$ *ó* $n = 0$.

[1] Algunos autores consideran a los número naturales a partir de 1, $\mathbb{N} = \{1, 2, 3, \ldots\}$.

Demostración.

(1) Aplicando las propiedades de la suma y el producto se tiene

$$m \cdot 0 + 0 \underset{S_3}{=} m \cdot 0 \underset{S_3}{=} m \cdot (0 + 0) \underset{D}{=} m \cdot 0 + m \cdot 0,$$

y por la ley de cancelación por la izquierda para la suma, $m \cdot 0 = 0$.

(2) Supongamos que $m \cdot n = 0$ y que $m \neq 0$. Demostraremos que $n = 0$.

$m \cdot n = 0 = m \cdot 0$. Como $m \neq 0$, entonces cancelando m a ambos lados de la igualdad obtenemos $n = 0$. ∎

Otra manera de enunciar la propiedad (2) de esta última proposición es:

$$\text{si } m \neq 0 \text{ y } n \neq 0, \text{ entonces } m \cdot n \neq 0.$$

Introduciremos ahora el orden en $\mathbb{N}$.

Definición 2.1.3. *Sean $m, n \in \mathbb{N}$. Diremos que* $\boldsymbol{m < n}$ *si existe $r \in \mathbb{N}$, $r \neq 0$ tal que $m + r = n$.*

Como hemos visto (página 71), podríamos haber definido el orden usando $\leq$ y en este caso sería. (ejercicio 2.1.1)

$$m \leq n \text{ si y sólo si existe } r \in \mathbb{N} \text{ tal que } m + r = n. \ [2]$$

Para demostrar que $<$ es un orden parcial aceptaremos la siguiente [3]

Proposición 2.1.4. *Sean $m, n \in \mathbb{N}$ tales que $m + n = 0$. Entonces $m = n = 0$.*

La última proposición se puede expresar de manera equivalente: $m \neq 0$ o $n \neq 0$ implica $m + n \neq 0$.

Proposición 2.1.5. *$<$ es un orden parcial en $\mathbb{N}$.*

Demostración.

(1) $m \not< m$. No puede ser que $m < m$ ya que si así lo fuera, entonces existiría $r \in \mathbb{N}$, $r \neq 0$ tal que $m + r = m = m + 0$ y por la ley de cancelación se tendría $r = 0$ lo cual contradice que $r \neq 0$.

(2) Si $n < m$ y $m < r$, entonces $n < r$. Como $n < m$ y $m < r$, por definición, existen $t, s \in \mathbb{N}$, $t \neq 0$, $s \neq 0$ tales que $n + t = m$ y $m + s = r$. Entonces

$$n + (t + s) = (n + t) + s = m + s = r.$$

[2] Aquí no se pide que $r \neq 0$.

[3] En el teorema 5.1.12 inciso (5) se demuestra un resultado equivalente a la proposición.

Como $t \neq 0$ y $s \neq 0$, por la proposición 2.1.4, $t + s \neq 0$ y así $n < r$. ∎

Veremos ahora algunas propiedades del orden.

Teorema 2.1.6. *Sean $m, n, r, s \in \mathbb{N}$.*

(1) Si $m < n$, entonces $m + r < n + r$.
(2) Si $m < n$ y $r < s$, entonces $m + r < n + s$.
(3) Si $m < n$ y $r \neq 0$, entonces $m \cdot r < n \cdot r$.
(4) Si $m < n$ y $r < s$, entonces $m \cdot r < n \cdot s$.

Demostración.

(1) Si $m < n$, entonces existe $t \in \mathbb{N}$, $t \neq 0$ tal que $m + t = n$. Sumando r a ambos lados de la igualdad, tenemos que $(m + t) + r = n + r$, que por las propiedades de la suma es $(m + r) + t = n + r$. Como $t \neq 0$, entonces $m + r < n + r$.

(2) Si $m < n$ y $r < s$, entonces existen $q, t \in \mathbb{N} - \{0\}$ tales que $m + q = n$ y $r + t = s$. Sumando ambas igualdades obtenemos que

$$(m + r) + (q + t) = n + s,$$

y como $q + t \neq 0$ por la proposición 2.1.4, entonces $m + r < n + s$.

(3) Supongamos $m < n$ y $r \neq 0$. Entonces existe $t \in \mathbb{N}$, $t \neq 0$ tal que $m + t = n$ y multiplicando la igualdad por r se tiene que, $m \cdot r + t \cdot r = (m + t) \cdot r = n \cdot r$. Ahora $t \neq 0$ y $r \neq 0$, así que por (2) de la proposición 2.1.2, $t \cdot r \neq 0$ y así $m \cdot r < n \cdot r$.

(4) Si $m < n$ y $r < s$, entonces existen $q, t \in \mathbb{N}$, $q \neq 0$ y $t \neq 0$ tales que $m + q = n$ y $r + t = s$. Multiplicando ambas igualdades llegamos a que $m \cdot r + (m \cdot t + q \cdot r + q \cdot t) = n \cdot s$. Por la proposición 2.1.2, $q \cdot t \neq 0$ ya que $q \neq 0$ y $t \neq 0$ y ahora por la proposición 2.1.4, $(m \cdot t + q \cdot r) + q \cdot t \neq 0$. Luego $m \cdot r < n \cdot s$. ∎

Si cambiamos $<$ por $\leq$ las propiedades son prácticamente las mismas salvo en el inciso (3) en el que no se necesita pedir $r \neq 0$ (véase ejercicio 2.1.2).

Proposición 2.1.7. *$0 < n$ para toda $n \in \mathbb{N}$, $n \neq 0$ y $n < n + k$ para todo $n \in \mathbb{N}$ y toda $k \in \mathbb{N}$, $k \neq 0$.*

Demostración. Como $n \neq 0$ y $0 + n = n$, entonces por la definición de orden, $0 < n$. De la misma manera, ya que $k \neq 0$ y $n + k = n + k$, entonces $n < n + k$. ∎

Nota 2.1.8. Sean $m, n \in \mathbb{N}$ tales que $m \leq n$. Entonces existe $r \in \mathbb{N}$ tal que $m + r = n$. Debido a la ley de cancelación para la suma, r es único (ejercicio 2.1.4),

así que no puede haber confusión si denotamos a r como $\boldsymbol{n-m}$. Por ejemplo $n-m=0$ en el caso en que $m=n$.

Definición 2.1.9. *Sean $m,n\in\mathbb{N}$ tales que $m\leq n$. Al único número natural r que satisface $m+r=n$ lo llamaremos* **la diferencia** de *n y m y lo denotaremos por $\boldsymbol{n-m}$.*

Debe quedar claro que la diferencia $n-m$ sólo está definida en $\mathbb{N}$ cuando $m\leq n$. Además por la definición de $n-m$ se tiene que $n-m\leq n$, ya que $m+(n-m)=n$. He aquí algunas de las propiedades de la diferencia.

Proposición 2.1.10. *Sean $m,n,r,s\in\mathbb{N}$ tales que $m\leq n$ y $s\leq r$. Entonces*

(1) $n-n=0$ *y* $n-0=n$ *para toda* $n\in\mathbb{N}$.
(2) $(s+m)+(n-m)=s+n$.
(3) $(n+r)-(m+s)=(n-m)+(r-s)$.
(4) Si $r\leq n-m$, *entonces* $(n-m)-r=n-(m+r)$.
(5) Si $r\leq m$, *entonces* $n-(m-r)=(n-m)+r$.
(6) $n\cdot(r-s)=n\cdot r-n\cdot s$.
(7) $(n-m)\cdot(r-s)=(n\cdot r+m\cdot s)-(n\cdot s+m\cdot r)$.

Demostración. Para demostrar las igualdades usaremos la unicidad de $n-m$ (nota 2.1.8), es decir, si $m+t=n$, entonces $t=n-m$.

(1) $n\leq n$ implica, por definición, que $n+(n-n)=n=n+0$, y de aquí obtenemos que $n-n=0$.

Igualmente $0\leq n$ implica $0+(n-0)=n=0+n$. Entonces $n-0=n$.

(2) $m\leq n$ implica que $m+(n-m)=n$. Entonces

$$(s+m)+(n-m)=s+[m+(n-m)]=s+n. \quad (\textit{asociatividad})$$

(3) $m\leq n$ y $s\leq r$ implican $m+s\leq n+r$.

$$\begin{aligned}(m+s)+[(n+r)-(m+s)] &= n+r && \text{definición de } (n+r)-(m+s)\\ &= (s+n)+(r-s) && \text{por inciso (2)}\\ &= [(s+m)+(n-m)]+(r-s) && \text{por inciso (2)}\\ &= (m+s)+[(n-m)+(r-s)] && \text{por asociatividad}\end{aligned}$$

Cancelando $m+s$ obtenemos

$$(n+r)-(m+s)=(n-m)+(r-s).$$

(4) Si $r \leq n-m$, entonces sumando m en ambos lados de la desigualdad, tenemos, usando el teorema 2.1.6, que

$$m + r \leq m + (n - m) = n.$$

Así que está definido $n - (m + r)$. Entonces

$$\begin{aligned}(m + r) + [n - (m + r)] &= n && \text{por definición de } n - (m + r)\\ &= m + (n - m) && \text{por definición de } n - m\\ &= (m + r) + [(n - m) - r] && \text{por inciso (2)}\end{aligned}$$

Cancelando $m + r$ obtenemos

$$n - (m + r) = (n - m) - r.$$

(5) Si $r \leq m$, entonces $r \leq n$ y además $m - r \leq m \leq n$, por lo que están definidos $n - r$ y $n - (m - r)$. Entonces

$$\begin{aligned}(m - r) + [n - (m - r)] &= n && \text{por definición de } n - (m - r)\\ &= r + (n - r) && \text{por definición de } n - r\\ &= [(n - r) + (m - m)] + r && \text{ya que } m - m = 0 \text{ inciso (1)}\\ &= [(m + n) - (r + m)] + r && \text{por inciso (3)}\\ &= [(m - r) + (n - m)] + r && \text{por inciso (3)}\\ &= (m - r) + [(n - m) + r] && \text{por asociatividad}\end{aligned}$$

Cancelando $m - r$ a ambos lados tenemos entonces que

$$n - (m - r) = (n - m) + r.$$

(6) $s + (r - s) = r$ por definición de $r - s$ y $n \cdot [s + (r - s)] = n \cdot r$

$$\begin{aligned}n \cdot s + n \cdot (r - s) &= n[s + (r - s)] && \text{por distributividad}\\ &= n \cdot r && \text{por definición de } r - s\\ &= n \cdot s + (n \cdot r - n \cdot s) && \text{por definición de } n \cdot r - n \cdot s\end{aligned}$$

Cancelando $n \cdot s$, tenemos que $n \cdot (r - s) = n \cdot r - n \cdot s$.

(7) Demostraremos que $(n - m) \cdot (r - s) + (n \cdot s + m \cdot r) = n \cdot r + m \cdot s$ que es equivalente a $(n - m) \cdot (r - s) = (n \cdot r + m \cdot s) - (n \cdot s + m \cdot r)$

$$\begin{aligned}(n - m) \cdot (r - s) &= (n - m) \cdot r - (n - m) \cdot s && \text{por inciso (6)}\\ &= (n \cdot r - m \cdot r) - (n \cdot s - m \cdot s) && \text{por inciso (6)}\\ &= [(n \cdot r - m \cdot r) - n \cdot s] + m \cdot s && \text{por inciso (5)}\\ &= [n \cdot r - (m \cdot r + n \cdot s)] + m \cdot s && \text{por inciso (4)}\\ &= [n \cdot r - (m \cdot r + n \cdot s)] + (m \cdot s - 0) && \text{por inciso (1)}\\ &= (n \cdot r + m \cdot s) - [(m \cdot r + n \cdot s) + 0] && \text{por inciso (3)}\\ &= (n \cdot r + m \cdot s) - (m \cdot r + n \cdot s) && \text{propiedad del 0}\blacksquare\end{aligned}$$

Aceptaremos que el orden que hemos definido en $\mathbb{N}$ es un buen orden, esto es,

Teorema 2.1.11 *(Axioma del buen orden). Si $A \subseteq \mathbb{N}$ y $A \neq \emptyset$, entonces A tiene mínimo.*

Teniendo en cuenta el Axioma del Buen Orden podemos definir una función

$$s : \mathbb{N} \longrightarrow \mathbb{N}$$

llamada la **función sucesor**, como sigue:

$$s(n) = mín\{m \in \mathbb{N} \mid n < m\}$$

Para todo número natural n, a $s(n)$ lo llamamos el **sucesor** de n.

Nota 2.1.12. Sabemos, por la proposición 2.1.7, que $n < n + k$ para todo $k \in \mathbb{N}$ tal que $k \neq 0$ y por lo tanto $\{m \in \mathbb{N} \mid n < m\} \neq \emptyset$.

Para un número natural n, $s(n)$ satisface $n < x \leq s(n) \Rightarrow x = s(n)$.

Proposición 2.1.13. *$s(n) = n + 1$ para todo $n \in \mathbb{N}$.*

Demostración. Primero demostraremos que $s(0) = 1$. Sea $s(0) = n_0$. Entonces, como $0 < 1$, debe ser $0 < n_0 \leq 1$. Si fuera $n_0 < 1$, entonces se tendría que $0 < n_0^2 < n_0$, lo que contradice que n_0 es el mínimo tal que $0 < n_0$. Luego $n_0 = 1$. Ahora, para cualquier $n \in \mathbb{N}$, $n < s(n) \leq n + 1$. Sea $s(n) = n + k$, donde $k \neq 0$, por la definición de orden. Entonces como $s(n)$ es el mínimo número natural tal que $n < s(n)$, entonces $n + k \leq n + 1$ y por lo tanto $0 < k \leq 1$ (véase ejercicio 2.1.7 (1)), lo que es posible sólo si $k = 1$ ya que $s(0) = 1$ es el mínimo número natural tal que $0 < s(0)$. Luego $s(n) = n + 1$. ∎

Corolario 2.1.14. *Sean $n, m \in \mathbb{N}$. Si $n < m$, entonces $n + 1 \leq m$.*

Corolario 2.1.15. *Sean $n, x \in \mathbb{N}$. si $n \leq x \leq n + 1$, entonces $x = n$ o $x = n + 1$.*

Recordemos que si $1 \leq n$, entonces $n-1$ es el número natural tal que $(n-1)+1 = n$, y por lo tanto se tendrá, por la proposición 2.1.13, que $s(n - 1) = n$ así que llamamos a $n - 1$ el **antecesor** de n con lo cual se tiene que todo número natural salvo 0 es sucesor de algún número, es decir, $Im(s) = \mathbb{N} - \{0\}$.
Los números naturales, escritos en forma ascendente mediante el orden, son

$$0 < s(0) = 0 + 1 = 1 < s(1) = 1 + 1 = 2 < s(2) = 2 + 1 = 3 < \cdots < s(n) = n + 1 < \cdots,$$

es decir

$$0 < 1 < 2 < 3 < \cdots < n < n+1 < \cdots .$$

§ 2.2. Principio de inducción completa

Sea $P(x)$ un predicado y supongamos que cada vez que damos un número natural n, $P(n)$ resulta verdadera. Aun cuando estos números naturales pueden ser "muchos", no podríamos afirmar que $P(n)$ es verdadera para todo $n \in \mathbb{N}$. En algunas ocasiones podremos encontrar una demostración de que efectivamente $P(n)$ es verdadera para todo $n \in \mathbb{N}$, pero en otras esto no es nada fácil, por ejemplo $1 + n + n^2 + \cdots + n^k = \frac{n^{k+1}-1}{n-1}$. Existe un principio, inherente a los números naturales, que además de ser bastante intuitivo nos permite, en muchos casos, demostrar propiedades relativas a los números naturales. La idea de este principio es la siguiente:

Supongamos que a partir del hecho de que $P(n)$ es verdadera ($n \in \mathbb{N}$) podemos demostrar que $P(n+1)$ es verdadera. Entonces tendríamos que:

si $P(0)$ verdadera, entonces $P(1)$ verdadera,

como $P(1)$ es verdadera, entonces $P(2)$ es verdadera,

como $P(2)$ es verdadera, entonces $P(3)$ es verdadera, etc.

Intuitivamente podríamos concluir que $P(n)$ es verdadera para todo $n \in \mathbb{N}$ ya que teniendo en cuenta que el orden en $\mathbb{N}$ es total, a los números naturales los podemos presentar en forma ascendente (respecto al orden) $0 < 1 < 2 < 3 < \cdots$, donde dado un número natural éste aparece en algún lugar de esta sucesión. A este principio se le conoce como Principio de Inducción Completa y como veremos, es consecuencia (en realidad es equivalente) del axioma de buen orden para los numeros naturales. Formalmente este principio dice:

Principio de Inducción Completa.- *Sea $A \subseteq \mathbb{N}$ tal que*

(1) $0 \in A$

(2) $n \in A$ *implica* $n + 1 \in A$.

Entonces $A = \mathbb{N}$.

Sea $P(n)$ una proposición. Si queremos demostrar que $P(n)$ es verdadera para todo $n \in \mathbb{N}$, es decir, que

$$A = \{n \in \mathbb{N} \mid P(n) \text{ es verdadera}\} = \mathbb{N}.$$

es suficiente mostrar que A satisface las dos hipótesis del principio de inducción completa.

Teorema 2.2.1. *El axioma del buen orden es equivalente al principio de inducción completa.*

Demostración.

⇒) El axioma del buen orden implica el principio de inducción completa.
Sea $A \subseteq \mathbb{N}$ tal que
(1) $0 \in A$
(2) $n \in A$ implica $n + 1 \in \mathbb{N}$.
Debemos demostrar que $A = \mathbb{N}$ y para esto supongamos que no es así, es decir, $A \subsetneq \mathbb{N}$.

Sea $B = \mathbb{N} - A$. Entonces $\varnothing \neq B \subseteq \mathbb{N}$ y por lo tanto B tiene elemento mínimo n_0. Como $0 \in A$ y $A \cap B = \varnothing$, debe ser $n_0 \neq 0$; luego n_0 tienen antecesor $n_0 - 1$ y puesto que $A \cup B = \mathbb{N}$ y $n_0 - 1 \notin B$, entonces $n_0 - 1 \in A$. Pero por hipótesis, $n_0 - 1 \in A$ implica $(n_0 - 1) + 1 = n_0 \in A$, lo cual es un absurdo ya que $n_0 \notin A$. Por lo tanto debe ser $A = \mathbb{N}$.

⇐) El principio de inducción completa implica el axioma del buen orden.
Sea $\varnothing \neq A \subseteq \mathbb{N}$ y supongamos que A no tiene mínimo. Entonces $0 \notin A$ porque en caso contrario 0 sería el mínimo de A. Sea entonces

$$B = \{n \in \mathbb{N} \mid n < a \text{ para toda } a \in A\}.$$

(1) $0 \in B$ puesto que $0 < a$ para todo $a \in A$.
(2) Sea $n \in B$. Queremos demostrar que $n + 1 \in B$. Para esto supongamos que no es así, es decir, que $(n + 1) \notin B$. Esto significa que existe $a_0 \in A$ tal que $a_0 \leq n + 1$. Por otro lado, como $n < a$ para todo $a \in A$ por el corolario 2.1.14, $n + 1 \leq a$ para todo $a \in A$, en particular $n + 1 \leq a_0$. Luego debe ser $a_0 = n + 1 \in A$ y por lo tanto a_0 sería el mínimo de A, lo que contradice la hipótesis de que A no tiene mínimo. Luego $n + 1 \in B$.
Por último como B satisface las dos hipótesis del principio de inducción, entonces $B = \mathbb{N}$ lo que es un absurdo pues $\varnothing \neq A = A \cap \mathbb{N} = A \cap B = \varnothing$. Con esto concluimos que A debe tener mínimo. ∎

Ejemplo 2.2.2. Para cada número natural n, sea

$$s_n = 0 + 1 + 2 + \cdots + n$$

Afirmamos que $s_n = \frac{n(n+1)}{2}$ para todo $n \in \mathbb{N}$. Podemos demostrar que esta igualdad es cierta de la siguiente manera:

$$s_n = 0 + 1 + \cdots (n-1) + n$$
$$s_n = n + (n-1) + \cdots + 1 + 0$$

Sumando estas dos igualdades tenemos entonces que

$$\begin{aligned} 2s_n &= (n+0) + (1 + (n-1)) + \cdots + ((n-1)+1) + (n+0) \\ &= \underbrace{n + n + \cdots + n + n}_{n+1-veces} \\ &= n(n+1) \end{aligned}$$

Por lo tanto $s_n = \frac{n(n+1)}{2}$.
Sin embargo también podríamos demostrarlo usando el principio de inducción:
Sea $A = \{n \in \mathbb{N} \mid s_n = 0 + 1 + 2 + \cdots + n = \frac{n(n+1)}{2}\}$.

(1) $0 \in A$, puesto que $s_0 = 0 = \frac{0(0+1)}{2}$.
(2) Supongamos que $n \in A$, es decir, $s_n = 0+1+2+\cdots+n = \frac{n(n+1)}{2}$. Entonces

$$\begin{aligned} s_{n+1} &= 0 + 1 + 2 + \cdots + n + (n+1) \\ &= s_n + (n+1) = \tfrac{n(n+1)}{2} + (n+1) \\ &= \tfrac{n(n+1)+2(n+1)}{2} \\ &= \tfrac{(n+1)(n+2)}{2} \\ &= \tfrac{(n+1)((n+1)+1)}{2} \end{aligned}$$

Esto es $n + 1 \in A$. Como se satisfacen las dos hipótesis del principio de inducción concluimos que $A = \mathbb{N}$.

Podrá suceder que una proposición $P(n)$ no sea verdadera para algunos números naturales que son menores que cierto número k, pero que sí lo es para todo número natural j tal que $j \geq k$. Se puede usar también el principio de inducción considerando el conjunto

$$A = \{n \in \mathbb{N} \mid P(n+k) \text{ es verdadera}\}$$

en cuyo caso esto se reduce a demostrar que

(1) $P(k)$ es verdadera y
(2) Si $P(n)$ es verdadera y $n \geq k$, entonces $P(n+1)$ es verdadera.

Ejemplo 2.2.3. Sea $P(n) : 2n + 1 < 2^n$. $P(n)$ no es verdadera para $n = 0, 1, 2$, sin embargo lo es para toda $n \in \mathbb{N}$ tal que $n \geq 3$.

(1) $P(3)$ es verdadera porque $7 = 2 \cdot 3 + 1 < 2^3 = 8$

(2) Supongamos que $n \geq 3$ y $P(n)$ es verdadera, es decir $2n+1 < 2^n$. Como $n \geq 3$ y $2 < 2^n$ (véase ejercicio 2.2.2), sumando estas dos desigualdades obtenemos

$$2(n + 1) + 1 = (2n + 1) + 2 < 2^n + 2^n = 2^{n+1}.$$

Por lo tanto $P(n)$ es verdadera para todo $n \in \mathbb{N}$, $n \geq 3$.

Ejemplo 2.2.4. Sea $n \geq 1$ y supongamos que queremos encontrar una fórmula para la suma de los primeros n números impares, esto es, para cada $n \geq 1$ queremos encontrar s_n donde

$$s_n = 1 + 3 + \cdots + (2n - 1)$$

Veamos si podemos descubrir esta fórmula dando algunos de valores a n.

$s_1 = 1$; $s_2 = 1 + 3 = 4$; $s_3 = 1 + 3 + 5 = 9$; $s_4 = 1 + 3 + 5 + 7 = 16$; $s_5 = 1 + 3 + 5 + 7 + 9 = 25$.

Entonces

$$s_1 = 1^2; \quad s_2 = 2^2 \quad s_3 = 3^2; \quad s_4 = 4^2; \quad s_5 = 5^2,$$

por lo que podríamos proponer que $s_n = n^2$ para todo número natural $n \geq 1$.
Para mostrar la validez de la afirmación para todo natural podemos usar el principio de inducción

(1) $s_1 = 1 = 1^2$.

(2) Supongamos que para $n \geq 1$, $s_n = 1 + 3 + \cdots + (2n - 1) = n^2$. Entonces

$$\begin{aligned} s_{n+1} &= 1 + 3 + \cdots + (2n - 1) + (2(n + 1) - 1) \\ &= s_n + (2(n + 1) - 1) \\ &= n^2 + (2(n + 1) - 1) \\ &= n^2 + 2n + 1 \\ &= (n + 1)^2. \end{aligned}$$

Otra equivalencia del principio de inducción completa se conoce como el principio de inducción modificado y también es de gran utilidad como veremos más adelante

Principio de Inducción Modificado. *Sea $A \subseteq \mathbb{N}$ tal que*

(a) $0 \in A$

(b) *$k \in A$ para todo $k = 0, 1, \ldots, n$ implica $n + 1 \in A$.*

Entonces $A = \mathbb{N}$.

Teorema 2.2.5. *El principio de inducción completa es equivalente al principio de inducción modificado.*

Demostración.

$\Rightarrow$) El principio de inducción completa implica el principio de inducción modificado.

Sea $A \subseteq N$ tal que

(a) $0 \in A$

(b) Si $k \in A$ para todo $k = 0, 1, \ldots, n$, entonces $n + 1 \in A$.

Para demostrar que $A = \mathbb{N}$ veremos que A satisface las hipótesis del principio de inducción completa.

(1) $0 \in A$.

(2) Supongamos que $n \in A$ y supongamos que $B = \{k \in \mathbb{N} \mid k < n \, y \, k \notin A\} \neq \emptyset$. Sea k_0 el mínimo de B, recuérdese que el principio de inducción completa es equivalente al axioma del buen orden. Entonces $k_0 \notin A$ y $k_0 \neq 0$ ya que $0 \in A$ y $0, 1, \cdots, k_0 - 1$ pertenecen a A, luego por hipótesis, $k_0 \in A$ lo que es una contradicción y por lo tanto deber ser $B = \emptyset$. Así que $0, 1, \ldots, n \in A$. Pero por hipótesis esto implica que $n + 1 \in A$

Entonces $A = \mathbb{N}$.

$\Leftarrow$) El principio de inducción modificado implica el principio de inducción completa. Sea $A \subseteq \mathbb{N}$ tal que

(1) $0 \in A$

(2) Si $n \in A$, entonces $n + 1 \in A$.

Para ver que $A = \mathbb{N}$ demostraremos que A satisface las hipótesis del principio de inducción modificado.

(a) $0 \in A$

(b) Sea $k \in A$ para todo $k = 0, 1, \ldots, n$. En particular $n \in A$, así que por hipótesis $n + 1 \in A$.

Por lo tanto $A = \mathbb{N}$. ∎

Existe un teorema (teorema 5.1.6 capítulo 5, sistemas de Peano) que nos permite definir conceptos relativos a los números naturales, llamándose a este tipo de definiciones por recursión, donde la idea de este teorema está muy ligada a la del principio de inducción completa. Mostramos dos ejemplos:

Ejemplo 2.2.6. Dado $a \in \mathbb{N}$, se define $n \cdot a$ para todo $n \in \mathbb{N}$ como sigue

(1) Para $n = 0$, definimos $0 \cdot a = 0$

(2) Si $n \cdot a$ está definido, definimos $(n+1) \cdot a = n \cdot a + a$.

El teorema de recursión nos permite afirmar que $n \cdot a$ queda definido para todo $n \in \mathbb{N}$. Veamos cómo es para los primeros números naturales

$$0 \cdot a = 0;\ 1 \cdot a = 0 \cdot a + a = a;\ 2 \cdot a = 1 \cdot a + a;\ 3 \cdot a = 2 \cdot a + a = a + a + a; \ldots;\ n \cdot a = \underbrace{a + a + \cdots + a}_{n-veces}.$$

Entonces a^n es multiplicar a por sí misma n veces $a^n = \underbrace{a \cdot a \cdot \cdots \cdot a}_{n-veces}$.

Ejemplo 2.2.7. Dado $a \in \mathbb{N}$, se define a^n para todo $n \in \mathbb{N}$ como sigue

(1) Para $n = 0$, definimos $a^0 = 1$

(2) Si a^n está definido, definimos $a^{n+1} = a^n \cdot a$.

El teorema de recursión nos permite afirmar que a^n queda definido para todo $n \in \mathbb{N}$. Veamos cómo es para los primeros números naturales

$$a^0 = 1;\ a^1 = a^0 \cdot a = a;\ a^2 = a^1 \cdot a = a \cdot a;\ a^3 = (a \cdot a) \cdot a = a \cdot a \cdot a;\ a^4 = a^3 \cdot a = (a \cdot a \cdot a) \cdot a.$$

Entonces a^n es multiplicar a por sí misma n veces $a^n = \underbrace{a \cdot a \cdot \cdots \cdot a}_{n-veces}$.

Ejemplo 2.2.8. Definimos el factorial de n, $n!$.

(1) Para $n = 0$, definimos $0! = 1$

(2) Suponiendo que se tiene definido $n!$, definimos $(n+1)! = n! \cdot (n+1)$

Entonces

$$0! = 1;\ 1! = 0! \cdot 1 = 1 \cdot 1 = 1;\ 2! = 1! \cdot 2 = 1 \cdot 2 = 2;\ 3! = 2! \cdot 3 = 1 \cdot 2 \cdot 3;\ 4! = 3! \cdot 4 = 1 \cdot 2 \cdot 3 \cdot 4.$$

Así que para cada $n \in \mathbb{N}$, $n! = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot n$, esto es, $n!$ es el producto de todos los números naturales distintos de cero y menores o iguales a n.

§§ Ejercicios sección 2.1.

2.1.1. Defina para $m, n \in \mathbb{N}$, $m \leq n$ si y sólo si existe $r \in \mathbb{N}$ tal que $m + r = n$. Demuestre que $\leq$ es un orden parcial en $\mathbb{N}$.

2.1.2. [4] Sean $m, n, r \in \mathbb{N}$. Demuestre para $m \leq n$ y $r \in \mathbb{N}$, entonces $m \cdot r \leq n \cdot r$.

[4] Véase página 132.

2.1.3. Si considera $\leq$ en lugar de $<$ ene l teorema 2.1.6, muestre que siguen siendo válidas los enunciados en cada uno de los incisos y que en el inciso (3) la propiedad es válida aun cuando $r = 0$, esto es, no se necesita pedir $r \neq 0$.

2.1.4. Sean $m, n \in \mathbb{N}$ tales que $n \leq m$. Demuestre que existe un único $r \in \mathbb{N}$ tal que $n + r = m$.

2.1.5. Sean $m, n, r \in \mathbb{N}$ con $r \neq 0$. Demuestre que si $m \cdot r = n$, entonces $m \leq n$.

2.1.6. Demuestre que la función sucesor (Ver página 135) $s : \mathbb{N} \longrightarrow \mathbb{N}$ es una función inyectiva.

2.1.7. Sean $m, n, r, s \in \mathbb{N}$. Demuestre que:

(1) Si $m + r < n + r$, entonces $m < n$.
(2) Si $m \cdot r < n \cdot r$, entonces $m < n$.
(3) Si $m \cdot r < n \cdot s$ y $n \leq m$, entonces $r < s$.

2.1.8. Sean $m, n, r, s \in \mathbb{N}$. Utilizando las propiedades de la suma y del producto de números naturales demuestre que: (mencione en cada caso las propiedades que se utilizan)

(1) $(m + n) + r = (m + r) + n$.
(2) $(m + (n + r)) + s = m + (n + (r + s))$.
(3) $(m + n) + (r + s) = (r + m) + (n + s)$.
(4) $(mn)\, r = (rn)\, m$.
(5) $(n + r)\, m = mr + nm$.
(6) $(m + n)\,(r + s) = (mr + nr) + (ms + ns)$.

2.1.9. Defina para $m, n \in \mathbb{N}$, $m \leq n$ si y sólo si existe $r \in \mathbb{N}$ tal que $m + r = n$. Demuestre que $\leq$ es un orden parcial en $\mathbb{N}$, es decir, $\leq$ es una relación reflexiva, antisimétrica y transitiva.

2.1.10. Sean $m, n, r \in \mathbb{N}$. Demuestre que

(1) Si $m \leq n$ y $n < r$, entonces $m < r$.
(2) Si $m < n$ y $n \leq r$, entonces $m < r$.

2.1.11. Sean $m, n, r, s \in \mathbb{N}$. Demuestre que:

(1) Si $m + r < n + r$, entonces $m < n$.
(2) Si $m \cdot r < n \cdot r$, entonces $m < n$.
(3) Si $m \cdot r < n \cdot s$ y $n \leq m$, entonces $r < s$.

2.1.12. Sean $m, n, r, s \in \mathbb{N}$. Demuestre que $m = n + r$ y $n = m + s$, entonces $r = 0$ y $s = 0$.

2.1.13. Sean $m, n, r, s \in \mathbb{N}$ tales que $m + n = r + s$. Pruebe que $m < r$ si y sólo si $s < n$.

2.1.14. Sean $m, n, r, s \in \mathbb{N}$ tales que $n < m$ y $s < r$. Demuestre que $nr + ms < ns + mr$.

2.1.15. Encuentre $m, n, r \in \mathbb{N}$ tales que $m - (n - r) \in \mathbb{N}$ pero $(m - n) - r \notin \mathbb{N}$.

2.1.16. Sean $m, n, r \in \mathbb{N}$ tales que $r \leq m$ y $r \leq n$. Si $m - r = n - r$, demuestre que $m = n$.

2.1.17. Sean $m, n \in \mathbb{N}$ tales que $m \leq n$. Demuestre que $(n-m)\cdot(n+m) = n^2 - m^2$.

§ § Ejercicios sección 2.2.

Denotemos por $\mathbb{N}^+$ al conjunto $\mathbb{N} - \{0\}$.

2.2.1. Usando inducción demuestre que:

(1) $0^2 + 1^2 + 2^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1)$, para todo $n \in \mathbb{N}$.
(2) $1^2 - 2^2 + 3^2 - \cdots + (-1)^{n+1}n^2 = \frac{(-1)^{n+1}n(n+1)}{2}$, para todo $n \in \mathbb{N}^+$.
(3) $0^3 + 1^3 + 2^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$, para todo $n \in \mathbb{N}$.
(4) $1 + 3 + 5 + 7 + \cdots + (2n-1) = n^2$, para todo $n \in \mathbb{N}^+$.
(5) $1^3 + 3^3 + 5^3 + \cdots + (2n-1)^3 = n^2(2n^2 - 1)$, para todo $n \in \mathbb{N}^+$.
(6) $5 + 10 + 15 + \cdots + 5n = \frac{5n(n+1)}{2}$, para todo $n \in \mathbb{N}^+$.
(7) $1 \cdot 3 + 2 \cdot 3^2 + 3 \cdot 3^3 + \cdots + n \cdot 3^n = \frac{(2n-1)\cdot 3^{n+1}+3}{4}$, para todo $n \in \mathbb{N}^+$.
(8) $1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + \cdots + n(n+2) = \frac{n(n+1)(2n+7)}{6}$, para todo $n \in \mathbb{N}^+$.
(9) $\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$, para todo $n \in \mathbb{N}^+$.
(10) $\frac{1}{1\cdot 3} + \frac{1}{3\cdot 5} + \frac{1}{5\cdot 7} + \cdots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}$, para todo $n \in \mathbb{N}^+$.
(11) $\frac{1}{2\cdot 5} + \frac{1}{5\cdot 8} + \frac{1}{8\cdot 11} + \cdots + \frac{1}{(3n-1)(3n+2)} = \frac{n}{6n+4}$, para todo $n \in \mathbb{N}^+$.
(12) $\frac{1}{1\cdot 2\cdot 3} + \frac{1}{2\cdot 3\cdot 4} + \frac{1}{3\cdot 4\cdot 5} + \cdots + \frac{1}{n(n+1)(n+2)} = \frac{n(n+3)}{4(n+1)(n+2)}$, para todo $n \in \mathbb{N}^+$.
(13) $\frac{1}{2\cdot 4} + \frac{1\cdot 3}{2\cdot 4\cdot 6} + \frac{1\cdot 3\cdot 5}{2\cdot 4\cdot 6\cdot 8} + \cdots + \frac{1\cdot 3\cdot 5\cdots(2n-1)}{2\cdot 4\cdot 6\cdots(2n+2)} = \frac{1}{2} - \frac{1\cdot 3\cdot 5\cdots(2n+1)}{2\cdot 4\cdot 6\cdots(2n+2)}$, para todo $n \in \mathbb{N}^+$.
(14) $\sum_{i=1}^{n} i(2^i) = 2 + (n-1)2^{n+1}$.
(15) $\sum_{i=1}^{n} 2(3^{i-1}) = 3^n - 1$.
(16) $\sum_{i=1}^{n} (i)(i!) = (n+1)! - 1$.

2.2.2. Demuestre que $2 < 2^n$ para todo $n \in \mathbb{N}$, $n \geq 2$.

2.2.3. Sea $P(x)$ una propiedad, y sea $k \in \mathbb{N}$ un número natural fijo. Suponga que
(1) $P(k)$ es válida; y que
(2) $\forall n \geq k\,(P(n) \implies P(n+1))$.
Demuestre que $P(n)$ es válida para todo $n \geq k$.

2.2.4. Usando inducción pruebe que:
(1) Para todo $n \in \mathbb{N}$, $1 + 2^n \leq 3^n$.
(2) Si $n \in \mathbb{N}$ y $n > 10$, entonces $n - 2 < \frac{n^2-n}{12}$.
(3) Si $n \in \mathbb{N}$ y $n > 3$, entonces $2^n < n!$.
(4) Si $n \in \mathbb{N}$ y $n > 4$, entonces $n^2 < 2^n$.
(5) Si $n \in \mathbb{N}$ y $n > 9$, entonces $n^3 < 2^n$.
(6) Para todo $n \in \mathbb{N}^+$, $(2n)! < 2^{2n}(n!)^2$.
(7) Para todo $n \in \mathbb{N}^+$, $\frac{1}{2n} \leq \frac{1\cdot 3\cdot 5\cdots(2n-1)}{2\cdot 4\cdot 6\cdots(2n)}$.
(8) Para todo $n \in \mathbb{N}^+$, $\frac{1\cdot 3\cdot 5\cdots(2n-1)}{2\cdot 4\cdot 6\cdots(2n)} \leq \frac{1}{\sqrt{1+n}}$.
(9) Para todo $n \in \mathbb{N}^+$, $\frac{1}{2^1} + \frac{2}{2^2} + \frac{3}{2^3} + \cdots + \frac{n}{2^n} < 2$.

2.2.5. Demuestre que si $n \in \mathbb{N}$, con $n \geq 2$, entonces

$$\left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{3^2}\right)\cdots\left(1 - \frac{1}{n^2}\right) = \frac{(n+1)}{2n}.$$

2.2.6. Para $n \in \mathbb{N}^+$, sea $S(n)$ la proposición abierta

$$\sum_{i=1}^{n} i = \frac{(n + \frac{1}{2})^2}{2}$$

Demuestre que la verdad de $S(k)$ implica la verdad de $S(k+1)$ para cualquier $k \in \mathbb{N}^+$. ¿Para qué valores de n es verdadera $S(n)$?

2.2.7. Encuéntrese todos los valores de $n \in \mathbb{N}^+$ para los cuales $\sum_{i=1}^{2n} i = \sum_{i=1}^{n} i^2$.

2.2.8. Para $n \in \mathbb{N}^+$, se define el n-ésimo número armónico como $H_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$.
(1) Para todo $n \in \mathbb{N}$, demuestre que $1 + \frac{n}{2} \leq H_{2^n}$.
(2) Demuestre que para todo $n \in \mathbb{N}^+$,

$$\sum_{j=1}^{n} jH_j = \left(\frac{n(n+1)}{2}\right) H_{n+1} - \left(\frac{n(n+1)}{4}\right).$$

(3) Demuestre que para todo $n \in \mathbb{N}^+$, $\sum_{i=0}^{n} \frac{1}{2i+1} = H_{2n+1} - \frac{1}{2}H_n$.

2.2.9. Sean $a_1, a_2, \ldots, a_{2^n}$ números positivos. Demuestre que

$$(a_1 a_2 \cdots a_{2^n})^{\frac{1}{2^n}} \leq \frac{a_1 + a_2 + \cdots + a_{2^n}}{2^n}$$

para $n = 1, 2, \ldots$

2.2.10. Consideremos las cuatro ecuaciones siguientes:

$$\begin{aligned}
(1) \qquad 1 &= 1 \\
(2) \qquad 2 + 3 + 4 &= 1 + 8 \\
(3) \qquad 5 + 6 + 7 + 8 + 9 &= 8 + 27 \\
(4) \qquad 10 + 11 + 12 + 13 + 14 + 15 + 16 &= 27 + 64
\end{aligned}$$

Conjeture la fórmula general sugerida por estas cuatro ecuaciones y demuéstrela.

2.2.11. Consideremos las seis ecuaciones siguientes:

(1) $1^2 + 0^2 = 1^2$;
(2) $3^2 + 4^2 = 5^2$;
(3) $5^2 + 12^2 = 13^2$;
(4) $7^2 + 24^2 = 25^2$;
(5) $9^2 + 40^2 = 41^2$;
(6) $11^2 + 60^2 = 61^2$

Conjeture la fórmula general sugerida por estas seis ecuaciones y demuéstrela.

2.2.12. Si $n \in \mathbb{N}^+$, demuestre que si $sen\theta \neq 0$, entonces

(1) $(\cos\theta)(\cos 2\theta)(\cos 4\theta)(\cos 8\theta)\cdots[\cos(2^{n-1}\theta)] = \frac{sen(2^n\theta)}{2^n sen\theta}$;
(2) $\cos\theta + \cos 3\theta + \cos 5\theta + \cdots + \cos(2n-1)\theta = \frac{sen2n\theta}{2sen\theta}$.

2.2.13. Sea x un número real, $x \geq -1$. Pruebe que $(1 + x)^n \geq 1 + nx$, para todo $n \in \mathbb{N}$.

2.2.14. Demuestre por inducción que para toda $n \geq 1$,

$$a^n - b^n = (a - b) \cdot \left(\sum_{i=0}^{n-1} a^{n-1-i} b^i \right).$$

2.2.15. Demuestre por inducción que para toda $n \in \mathbb{N}$,

$$a^{2n+1} + b^{2n+1} = (a+b) \cdot \left(\sum_{i=0}^{n-1} (-1)^i a^{2n-i} b^i \right).$$

2.2.16. Demostrar por inducción que las siguientes proposiciones son ciertas.

(1) $n^2 + n$ es par, para $n = 1, 2, 3, \ldots$
(2) $n^3 - n$ es múltiplo de 6, para $n = 1, 2, 3, \ldots$
(3) $n(n+1)(n+2)(n+3)$ es múltiplo de 24, para $n = 1, 2, 3, \ldots$
(4) 7^n es impar, para $n = 1, 2, 3, \ldots$
(5) $11^n - 1$ es múltiplo de 5, para $n = 1, 2, 3, \ldots$
(6) $3^n + 7^n - 2$ es múltiplo de 8, para $n = 1, 2, 3, \ldots$

2.2.17. Sean a, r dos números cualesquiera (no necesariamente naturales). Si $r \neq 1$, demuestre que para toda $n \in \mathbb{N}$, $a + ar + ar^2 + \cdots + ar^n = \frac{a(r^{n+1})-1}{r-1}$.

2.2.18. **La moneda falsa.** Suponga que se tienen 3^n monedas y se sabe que una de ellas es falsa y pesa menos que las otras. Suponga también que se tiene una balanza con dos platos sin graduación ni pesas para la báscula, de tal manera que la única forma de pesar las monedas es poner algunas en un plato y otras monedas en el otro plato y comparar si los platos quedan o no balanceados. Con este procedimiento usted tiene que encontrar la moneda falsa. Usando inducción demuestre que n pesadas bastan para encontrar la moneda falsa. Explique.

2.2.19. ¿Qué está mal en la siguiente "demostración"de que

$$\frac{1}{2} + \frac{2}{3} + \cdots + \frac{n}{n+1} \neq \frac{n^2}{n+1}$$

para toda $n \geq 2$?
Suponga, a manera de contradicción, que

$$\frac{1}{2} + \frac{2}{3} + \cdots + \frac{n}{n+1} = \frac{n^2}{n+1}. \tag{5}$$

Entonces también

$$\frac{1}{2} + \frac{2}{3} + \cdots + \frac{n}{n+1} + \frac{n+1}{n+2} = \frac{(n+1)^2}{n+2}.$$

Se podría probar la afirmación (5) por inducción. En particular, el paso inductivo daría

$$\left(\frac{1}{2}+\frac{2}{3}+\cdots+\frac{n}{n+1}\right)+\frac{n+1}{n+2}=\frac{n^2}{n+1}+\frac{n+1}{n+2}.$$

Por lo tanto

$$\frac{n^2}{n+1}+\frac{n+1}{n+2}=\frac{(n+1)^2}{n+2}$$

Al multiplicar cada lado de esta ecuación por $(n+1)(n+2)$ se tiene

$$n^2(n+2)+(n+1)^2=(n+1)^3$$

2.2.20. Suponga que se tiene un conjunto finito de canicas cualquiera y se quiere probar que no importa cuál sea este conjunto, todas las canicas son de un solo color. La demostración de esta afirmación es por inducción sobre el número n de canicas del conjunto dado:

(1) Si $n = 1$, no hay nada que probar.
(2) Supongamos que el resultado es válido para conjuntos con menos de n canicas y supongamos que tenemos un conjunto con n canicas y queremos probar que éstas son del mismo color. Enumeremos estas n canicas como: $c_1, c_2, \ldots, c_n$. Si quitamos la canica c_n queda el conjunto $c_1, c_2, \ldots, c_{n-1}$ con $n-1 < n$ canicas y así, por hipótesis de inducción, todas las canicas $c_1, c_2, \ldots, c_{n-1}$ son del mismo color. De manera similar, si quitamos la canica c_1, el conjunto $\{c_2, \ldots, c_n\}$ tiene $n-1 < n$ canicas y por hipótesis de inducción todas éstas son del mismo color. Notamos ahora que los conjuntos $\{c_1, c_2, \ldots, c_{n-1}\}$ y $\{c_2, \ldots, c_n\}$ tienen la canica c_2 en común y por lo tanto todas las canicas $c_1, c_2, \ldots, c_n$ son del mismo color, como se quería demostrar. ¿Qué está mal con el argumento anterior? (es decir, encontrar en qué momento el procedimiento que se sigue en la supuesta demostración es incompleto o incorrecto).

2.2.21. La siguiente afirmación es obviamente falsa: "El conjunto $\mathbb{N}$ de los números naturales es finito". Determinar cuál es el error en la "demostración"por inducción que presentamos a continuación (es decir, encontrar en qué momento el procedimiento que se sigue en la supuesta demostración es incompleto o incorrecto): "Para cada natural n sea $A_n = \{n\}$. Sabemos que la unión de todos los conjuntos A_n nos da el conjunto $\mathbb{N}$, y que la unión de dos conjuntos finitos es finito. Entonces $A_1 \cup A_2$ es finito. Supongamos que $A_1 \cup A_2 \cup \cdots \cup A_{n-1}$ es finito para cierta $n \geq 3$. Entonces, como $A_1 \cup A_2 \cup \cdots \cup A_n = (A_1 \cup A_2 \cup \cdots \cup A_{n-1}) \cup A_n$, que es la unión de

dos conjuntos finitos (usando la hipótesis de inducción), también es finito. Queda entonces probado que $\mathbb{N}$ es finito."

2.2.22. Encuéntrese la falla en este razonamiento.
Demostraremos por inducción que dos números enteros positivos cualesquiera, son iguales. Usemos inducción en el máximo de los dos números. Sea $P(n)$ la afirmación de que dos enteros positivos con valor máximo n son iguales.
Como los dos únicos enteros enteros positivos cuyo valor máximo es uno son 1 y 1, vemos que $P(1)$ es cierto.
Supóngase que $P(k)$ es cierto y sean r y s números positivos con valor máximo $k+1$. Entonces, el valor máximo de $r-1$ y $s-1$ es k, de modo que $r-1=s-1$ por la hipótesis de inducción. Por lo tanto, $r=s$. Así, $P(k+1)$ es cierto, de modo que $P(n)$ s cierto para todas las $n \in \mathbb{N}^+$.

2.2.23 Las torres de Hanoi. En un templo budista en Asia, los monjes tienen un juego que consiste en 3 torres (algo así como 3 postes) y 64 discos de tamaño diferente, ordenados de arriba hacia abajo con el mayor disco abajo y el menor arriba, de tal forma que encima de cualquier disco dado no hay disco mayor que el disco dado. Los discos se hallan acomodados en, digamos, la torre A y el problema es trasladar todos los discos a la torre C (usando a la torre B como intermediaria) de acuerdo con las reglas siguientes:

(1) Sólo se puede mover un disco a la vez;
(2) Nunca se puede poner un disco de tamaño mayor sobre un disco de tamaño menor.

Por supuesto que, si no existiera la torre B, el problema no tendría solución. Para hacer el problema más interesante, podemos pensar que se tienen n discos y queremos hallar el menor número de movidas para llevar los discos de A a C.
Para resolver el problema, llamamos $T(n)$ al número mínimo de movidas necesarias para llevar los n discos de A a C.

(a) Demuestre que para todo $n \in \mathbb{N}^+$, $T(n+1) = 2T(n)+1$.
(b) Pruebe por inducción que $T(n) = 2^n - 1$ para todo $n \in \mathbb{N}^+$.

2.2.24. Si $a \in \mathbb{N}$ definimos las potencias a^n para cada $n \in \mathbb{N}$ como sigue:

Para $n = 0$, definimos $a^0 = 1$,
Si a^n ya está definido, se define $a^{n+1} = a^n \cdot a$.

(1) Sean $a, b \in \mathbb{N}$ elementos fijos en los números naturales. Demuestre que para todo $n, m \in \mathbb{N}$ se tiene que

(a) $(ab)^n = a^n b^n$.
(b) $a^n a^m = a^{m+n}$.
(c) $(a^n)^m = a^{nm}$.

(2) Demuestre con un ejemplo que no es cierto en general que: $n^{m^k} = (n^m)^k$ y $n^m = m^n$.

2.2.25 Principio de inducción finita. Sea $P(x)$ una propiedad, y sea $k \in \mathbb{N}$ un número natural fijo. Suponga que

(1) $P(0)$ es válida; y que
(2) $\forall n < k\,(P(n) \implies P(n+1))$.

Demuestre que $P(n)$ es válida para todo $n \leq k$.

2.2.26 Doble inducción. Sea $P(x, y)$ una propiedad. Suponga que:

(1) $P(0, 0)$ es válida;
(2) $P(m, 0)$ implica $P(m + 1, 0)$; y
(3) $P(m, n)$ implica $P(m, n + 1)$.

Demuestre que $P(m, n)$ es válida para todo $m, n \in \mathbb{N}$.

Principio de Inducción Modificado

2.2.27. En realidad, nunca hemos podido encontrar una falla en (*a*). Pruebe su suerte en (*a*) y después responda (*b*).

(*a*) Un asesino recibe la sentencia de ser ejecutado; pide al juez que no se le diga el día de la ejecución. El juez dice: "Lo sentencio a ser ejecutado a las 10 a.m. de algún día del próximo enero, pero le prometo que no se dará cuenta de que será ejecutado ese día, sino hasta que vayan por usted a las 8 a.m." El criminal va a su celda y procede a demostrar que no puede ser ejecutado en enero, de la siguiente manera:

Sea $P(n)$ la afirmación de que no puedo ser ejecutado el día $(31 - n)$ de enero. Quiero probar $P(n)$ para $0 \leq n \leq 30$. Ahora bien, no puedo ser ejecutado el 31 de enero, pues es el último día de mes y como seré ejecutado ese mes, sabría que ése es el día, antes de las 8 a.m., lo cual contradice que la sentencia del juez. Así, $P(0)$ es cierto. Supóngase $P(m)$ es cierto para $0 \leq m \leq k$ donde $k \leq 29$. Esto es, supóngase que que no puedo ser ejecutado de enero $(31 - k)$ a enero 31. Entonces, enero $(31 - k - 1)$ debe ser el último día posible para la ejecución y lo sabría antes de las 8 a.m., lo cual contradice la sentencia del juez. Así, no puedo ser ejecutado en enero $(31 - (k + 1))$, de modo que $P(k)$ es cierto. Por tanto, no puedo

ser ejecutado en enero.
(Por supuesto, el criminal fue ejecutado el 17 de enero.)
(b) Una profesora imparte una clase cinco días a la semana, de lunes a viernes. Le comunica a sus alumnos que hará un examen más, algún día de la última semana de clases, pero que los alumnos no sabrán si el examen será ese día, sino hasta llegar al aula. ¿Cuál es el último día de la semana en que puede hacer el examen, para satisfacer estas condiciones?.

2.2.28. Pruebe que todo natural mayor que 7 se puede expresar como suma de 3's y 5's de la forma $3x + 5y$ donde $x, y \in \mathbb{N}$.

2.2.29.
(1) Sea $n \in \mathbb{N}$, con $n \neq 0, 1, 3$. Demuestre que n puede expresarse como una suma de doses, cincos o ambos.
(2) Para cualquier $n \in \mathbb{N}$, pruebe que si $n \geq 24$, entonces n puede expresarse como una suma cincos y/o sietes.

2.2.30. Demuestre que un importe postal de 6 centavos o más se logra sólo usando timbres de 2 y 7 centavos.

2. 2.31. Demuestre que un importe postal de 24 centavos o más se logra sólo usando timbres de 5 y 7 centavos.

2.2.32. Considere la siguiente sucesión de números enteros definida como sigue:

$a_1 = 3$; $a_2 = 5$;
$a_n = 3a_{n-1} - 2a_{n-2}$ para $n \geq 3$.

(1) Encuentre a_3, a_4, a_5 y a_6.
(2) Razonando por inducción, demuestra que $a_n = 2^n + 1$, para todo $n \geq 1$. ¿Qué tipo de inducción utilizas?

2.2.33. Considere la siguiente sucesión de números enteros definida como sigue:

$a_0 = 1$, $a_1 = 2$, $a_2 = 3$, y
$a_n = a_{n-1} + a_{n-2} + a_{n-3}$ para $n \geq 3$.

(1) Encuentre a_3, a_4 y a_5.
(2) Razonando por inducción, demuestra que $a_n \leq 3^n$, para todo $n \in \mathbb{N}$.

2.2.34. Considere la siguiente sucesión de números enteros definida como sigue:

$a_1 = 1$, $a_2 = 2$, y
$a_n = a_{n-1} + a_{n-2}$ para $n \geq 3$.

(1) Encuentre a_3, a_4, a_5, a_6 y a_7.
(2) Demuestra que $a_n < \left(\frac{7}{4}\right)^n$, para todo $n \geq 1$.

2.2.35. Para $n \geq 1$, sea p_n el número (aproximado) de bacterias que hay en un cultivo, al final de n horas (después de iniciado un experimento). Si

$p_1 = 1000$, $p_2 = 2000$, y
$p_n = p_{n-1} + p_{n-2}$ para $n \geq 3$,

demuestra que

$$p_n = \left(\frac{1000}{\sqrt{5}}\right)\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right].$$

2.2.36. Consideremos la sucesión $c_1, c_2, \ldots$ definida por las ecuaciones

$$c_1 = 0 \quad y \quad c_n = c_{\lfloor \frac{n}{2} \rfloor} + n^2 \quad \text{para todo } n > 1$$

(donde $\lfloor x \rfloor$ es el entero más grande menor o igual que x, de manera informal se está redondeando hacia abajo).

(1) Calcule c_2, c_3, c_4 y c_5.
(2) Pruebe que $c_n < 4n^2$ para toda $n \geq 1$.

2.2.37. Consideremos la sucesión $c_1, c_2, \ldots$ definida por las ecuaciones

$$c_1 = 0 \quad y \quad c_n = 4c_{\lfloor \frac{n}{2} \rfloor} + n \quad \text{para todo } n > 1.$$

(1) Calcule c_2, c_3, c_4 y c_5.
(2) Pruebe que $c_n \leq 4(n-1)^2$ para toda $n \geq 1$.
(3) Pruebe que $\frac{(n+1)^2}{8} < c_n$ para toda $n \geq 2$. Sugerencia: los pasos bases son $n = 2, 3$. Además, $\lfloor \frac{n}{2} \rfloor \geq \frac{n-1}{2}$.

2.2.38. Suponga que se tienen dos pilas de cartas cada una con n cartas. Dos jugadores juegan el siguiente juego. Cada jugador, en su turno, elige una pila y quita cualquier número de cartas, pero al menos una, de la pila elegida. El jugador que quita la última carta gana el juego. Pruebe que el segundo jugador siempre puede ganar.

2.2.39. Critíquese este razonamiento.
Mostremos que todo natural tiene alguna propiedad interesante. Sea $P(n)$ la afirmación de que n tiene una propiedad interesante. Usemos el Principio de Inducción Modificado.

Claro que $P(0)$ es cierto, pues 0 es el neutro aditivo, lo cual ciertamente es una propiedad interesante del 0.
Supóngase que $P(m)$ es cierto para $0 \leq m \leq k$. Si $P(k+1)$ no fuera cierto, entonces $k+1$ sería el menor natural sin una propiedad interesante, lo cual sería, por sí mismo, una propiedad interesante de $k+1$. De modo que $P(k+1)$ debe ser cierto. Así, $P(n)$ es cierto para todas las $n \in \mathbb{N}$.

2.2.40. Los egipcios de la antigüedad expresaban una fracción como la suma de fracciones cuyos numeradores eran 1. Por ejemplo, $\frac{5}{6}$ se expresa como

$$\frac{5}{6} = \frac{1}{2} + \frac{1}{3}.$$

Decimos que la fracción $\frac{p}{q}$, donde $p, q \in \mathbb{N}^+$, está en forma egipcia si

$$\frac{p}{q} = \frac{1}{n_1} + \frac{1}{n_2} + \cdots + \frac{1}{n_k},$$

donde $n_1, n_2, \ldots, n_k$ son naturales tales que $1 \leq n_1 < n_2 < \ldots < n_k$.

(1) Demuestre que la forma egipcia de una fracción no necesariamente es única representando a $\frac{5}{6}$ de dos maneras.
(2) Demuestre que la forma egipcia de una fracción nunca es única.

2.2.41. Use inducción para demostrar que n líneas rectas en el plano lo dividen en $\frac{n^2+n+2}{2}$ regiones. Suponga que no hay dos líneas paralelas y que no hay tres líneas con un punto en común.

2.2.42. Siguiendo los pasos descritos, proporcione una prueba por inducción sobre p para demostrar que toda fracción $\frac{p}{q}$ con $0 < \frac{p}{q} < 1$ puede expresarse en forma egipcia.

(1) Verifique el paso base ($p = 1$).
(2) Suponga que $0 < \frac{p}{q} < 1$ y que todas las fracciones $0 < \frac{s}{q'} < 1$, con $1 \leq s < p$ y q' arbitrarios, se pueden expresar en forma egipcia. Seleccione el menor entero positivo n tal que $\frac{1}{n} \leq \frac{p}{q}$. Demuestre que

$$n > 1 \quad y \quad \frac{p}{q} < \frac{1}{n-1}.$$

(3) Demuestre que si $\frac{p}{q} = \frac{1}{n}$, la prueba queda completa.

(4) Suponga que $\frac{1}{n} < \frac{p}{q}$. Sea

$$p_1 = np - q \quad y \quad q_1 = nq.$$

Demuestre que

$$\frac{p_1}{q_1} = \frac{p}{q} - \frac{1}{n}, \quad 0 < \frac{p_1}{q_1} < 1, \quad y \quad p_1 < p.$$

Concluya que

$$\frac{p_1}{q_1} = \frac{1}{n_1} + \cdots + \frac{1}{n_k},$$

donde $n_1, \ldots, n_k$ son diferentes.

(5) Demuestre que $\frac{p_1}{q_1} < \frac{1}{n}$.

(6) Demuestre que

$$\frac{p}{q} = \frac{1}{n} + \frac{1}{n_1} + \cdots + \frac{1}{n_k},$$

donde $n, n_1, \ldots, n_k$ son diferentes.

∞.

John Wallis
1616 - 1703

Capítulo **3**

Conjuntos finitos

Cuando hablamos del tamaño de un conjunto, intuitivamente nos referimos a "cuántos" elementos tiene. Para ciertos conjuntos (finitos) es posible "contar" sus elementos uno a uno. Sin embargo existen otros conjuntos para los cuales, siguiendo la idea de "contarlos" uno por uno, esto no puede hacerse. A estos conjunto se les llama infinitos y lo único que podemos hacer con ellos es "compararlos" con otros para tener una idea de qué tan "grandes" son.

Precisemos un poco la idea de contar, que es algo que hacemos en nuestra vida diaria. Sea $A = \{a, b, c\}$, donde a, b y c son distintos entre sí. Al contar los elementos de A lo que hacemos es asociar 1 con a, 2 con b y 3 con c para llegar a la conclusión de que A tiene 3 elementos. Lo que en realidad hicimos fue establecer una función biyectiva f de $I_3 = \{1, 2, 3\}$ en A, donde $f(1) = a$, $f(2) = b$, $f(3) = c$. Si B es el conjunto $\{v, w, x, y, z\}$, de las últimas letras del alfabeto latino, podemos establecer una función biyectiva de $I_5 = \{1, 2, 3, 4, 5\}$ en B para concluir que B tiene 5 elementos. Si tuviésemos otros conjuntos A' y B' con 3 y 5 elementos respectivamente, sabríamos, por propiedades conocidas de las funciones, que existe una función biyectiva de A en A' y una función biyectiva de B en B'. Sin embargo, existen conjuntos para los cuales, sin importar qué número natural sea n, no existe una función biyectiva de $I_n = \{1, 2, \ldots, n\}$ en estos conjuntos y un ejemplo de tal conjunto es $\mathbb{N}$, el conjunto de los números naturales. Estableceremos la diferencia entre estos dos tipos de conjuntos llamando a unos finitos y a los otros infinitos. El concepto de cardinal de un conjunto reflejará esta idea de "tamaño" de un conjunto.

§ 3.1. Conjuntos finitos e infinitos

Definición 3.1.1. *Decimos que dos conjuntos A y B son* **equipotentes** *si existe una función biyectiva de A en B y lo denotaremos por* $\boldsymbol{A \approx B}$.

Proposición 3.1.2. *Sean A, B y C conjuntos. Entonces*

(1) $A \approx A$.

(2) Si $A \approx B$, *entonces* $B \approx A$.

(3) Si $A \approx B$ *y* $B \approx C$, *entonces* $A \approx C$.

Demostración. Estas tres propiedades son consecuencia de la propiedades ya conocidas de funciones.

(1) $1_A : A \longrightarrow A$ es biyectiva.

(2) Si $f : A \longrightarrow B$ es biyectiva, entonces existe su inversa $f^{-1} : B \longrightarrow A$ que es biyectiva.

(3) Si $f : A \longrightarrow B$ y $g : B \longrightarrow C$ son biyectivas, entonces $g \circ f : A \longrightarrow C$ es biyectiva. ∎

Debido a las propiedades que satisface $\approx$, se podría decir que $\approx$ es una relación de equivalencia, el problema aquí es que estamos definiendo la equipotencia de conjuntos arbitrarios y ya hemos visto que la colección de conjuntos no es un conjunto. Es por esto que hemos evitado decir que $\approx$ es una relación de equivalencia. Sin embargo, las propiedades se mantienen.
Aun cuando no vamos a dar una definición formal de cardinal, (es decir, no vamos a decir exactamente qué es) podemos dar las propiedades que los determinan y estas son:

(1) *Cada conjunto tiene asociado un objeto que es su cardinal.*

(2) *Los conjuntos A y B tienen el mismo cardinal si y sólo si $A \approx B$ (son equipotentes).*

Para cada $n \in \mathbb{N}$, $n > 0$, definimos el conjunto

$$I_n = \{x \in \mathbb{N} \mid 1 \leq x \leq n\} = \{1, 2, \ldots, n\}.$$

Entonces

$$I_1 = \{1\},\ I_2 = \{1, 2\},\ I_3 = \{1, 2, 3\},\ I_4 = \{1, 2, 3, 4\},\ \text{etc.}$$

Cada uno de estos conjuntos I_n ($n \geq 1$) tiene mínimo y máximo, que son 1 y n respectivamente. Veamos algunas propiedades de estos conjuntos.

Proposición 3.1.3. *Sean $n, m \in \mathbb{N} - \{0\}$. Entonces $I_n \subsetneq I_m$ si y sólo si $n < m$.*

Demostración.

$\Rightarrow$) Supongamos que $I_n \subsetneq I_m$. Como $n \in I_n$, entonces $n \in I_m$ y así $n \leq m$. Además $n \neq m$ ya que en caso contrario se tendría $I_n = I_m$ que por hipótesis no es así. Por lo tanto debe se $n < m$.

$\Leftarrow$) Supongamos $n < m$. Para cada $k \in I_n$, se tiene que $1 \leq k \leq n$ y entonces $1 \leq k \leq m$. Luego $k \in I_m$. Como $m \in I_m - I_n$, concluimos que $I_n \subsetneq I_m$. ∎

Corolario 3.1.4. *Si $n, m \in \mathbb{N}$, entonces $I_n \subseteq I_m$ o $I_m \subseteq I_n$.*

Demostración. Como el orden en $\mathbb{N}$ es total, dados $m, n \in \mathbb{N}$ tendremos 3 casos; si $n = n$, entonces $I_n = I_m$. Por otra parte, si $n < m$ la proposición 3.1.3 garantiza $I_n \subsetneq I_m$; finalmente, si $m < n$ nuevamente por la proposición 3.1.3 tendríamos $I_m \subsetneq I_n$. ∎

Proposición 3.1.5. *Sean $n, m \in \mathbb{N} - \{0\}$ $I_n \approx I_m$ si y sólo si $n = m$.*

Demostración.

$\Rightarrow$) Demostraremos por inducción sobre $n \geq 1$, que si $I_n \approx I_m$, entonces $n = m$.

(*i*) $n = 1$. Sea $f : I_1 \longrightarrow I_m$ biyectiva. Entonces $Im(f) = \{f(1)\} = I_m = \{x \in \mathbb{N} \mid 1 \leq x \leq m\}$. Luego, debe ser $I_m = \{1\}$ y esto implica que $m = 1$, ya que si fuera $m > 1$, $1 \neq m \in I_m$, con lo cual se tendría $Im(f) \subsetneq I_m$, lo que contradice la elección de f.

(*ii*) Supongamos cierta la afirmación para $n \geq 1$.
Sea $f : I_{n+1} \longrightarrow I_m$ una función biyectiva. Como $n + 1 \geq 2$, entonces I_{n+1} tiene al menos dos elementos distintos y por lo tanto $m \geq 2$, ya que si $m = 1$, entonces $I_m = \{1\}$ y f no sería inyectiva. Sea

$$f(1) = i_1, f(2) = i_2, \ldots, f(n) = i_n, f(n + 1) = i_{n+1}.$$

Ahora, por ser f suprayectiva, $I_m = \{i_1, i_2, \ldots, i_n, i_{n+1}\}$. Como $m \in I_m$, debe ser $m = i_j$ para algún $j = 1, 2, \ldots, n, n + 1$. Tenemos dos casos: $j = n + 1$ o $j \neq n + 1$.

1^{o} caso: $j = n + 1$, es decir, $f(n + 1) = i_{n+1} = m$.
En este caso, $f(n + 1) = i_{n+1} = m$. Definimos $f' : I_n \longrightarrow I_{m-1}$ como $f'(k) = f(k) = i_k$ para toda $k \in I_n$. f' está bien definida. Claramente f' es biyectiva y por hipótesis de inducción, se tiene entonces que $n = m - 1$ y así $n + 1 = m$.

2^{o} caso: $j \neq n + 1$, es decir, $i_{n+1} \neq m$. Definimos $g : I_{n+1} \longrightarrow I_{n+1}$ por

$$g(k) = \begin{cases} k & \text{si si } k \neq j \text{ y } k \neq n+1; \\ n+1 & \text{si } k = j; \\ j & \text{si } k = n+1. \end{cases}$$

Como g es biyectiva (véase ejercicio 3.1.1), entonces $f \circ g : I_{n+1} \longrightarrow I_m$ es biyectiva y $(f \circ g)(n + 1) = f(g(n + 1)) = f(j) = m$. Así por el primer caso $n + 1 = m$.

$\Leftarrow$) Es inmediato. ∎

Definiremos ahora cuándo un conjunto es finito.

Definición 3.1.6. *Un conjunto A es* **finito** *si no existe $B \subsetneq A$ tal que $A \approx B$. Un conjunto será* **infinito** *si no es finito.*

Para demostrar el siguiente resultado tendríamos que introducir la *teoría de cardinales*, la cual no está contemplada en el objetivo de este libro, por tal motivo aceptaremos sin demostración el siguiente teorema. Sin embargo el lector interesado puede consultarla en el capítulo 3, sección 3, de [**6**].

Teorema 3.1.7. *Un conjunto A es* **finito** *si y sólo si $A = \emptyset$ o existe $n \in \mathbb{N}$, $n \geq 1$ tal que $I_n \approx A$.*

En particular, I_n es finito para todo $n \in \mathbb{N}$, $n \geq 1$.

Definición 3.1.8. *La* ***cardinalidad del conjunto vacío es* 0** *y si el conjunto $A \neq \emptyset$ es finito diremos que la* ***cardinalidad*** *de A es n si $I_n \approx A$. Si A es un conjunto infinito diremos que la cardinalidad de A es infinita.*

Denotaremos por ***card*(*A*)** a la cardinalidad del conjunto A.

Por la proposición 3.1.5, $n \neq m$ si y sólo si $I_n \not\approx I_m$, así que la definición de cardinalidad de un conjunto finito está bien dada, es decir, si un conjunto $A \neq \emptyset$ es finito, existe una única $n \in \mathbb{N}$, $n \geq 1$ tal que $I_n \approx A$. En este caso si $f : I_n \longrightarrow A$ es biyectiva y $f(i) = a_i$, entonces $A = \{a_1, \ldots, a_n\}$. En muchas ocasiones describir

los elementos de A de esta manera es de gran utilidad como puede verse en la demostración de la proposición 3.1.5.

Teorema 3.1.9. *Sean A y B conjuntos finitos de cardinalidad n y m respectivamente y $f : A \longrightarrow B$ una función.*

(1) Si f es inyectiva, entonces $n \leq m$.
(2) Si f es suprayectiva, entonces $m \leq n$.

Demostración.

(1) Como $card(A) = n$ y $card(B) = m$, entonces existen funciones biyectivas $g : I_n \longrightarrow A$ y $h : I_m \longrightarrow B$. La función $h^{-1} \circ f \circ g : I_n \longrightarrow I_m$ es inyectiva. Supongamos que $m < n$. Entonces $I_m \subsetneq I_n$, así que la función $\varphi : I_n \longrightarrow I_n$ definida por $\varphi(j) = \left(h^{-1} \circ f \circ g\right)(j)$ es inyectiva pero no suprayectiva pues la imagen de φ está contenida en I_m y por lo tanto está contenida propiamente en I_n. Podemos concluir que I_n es equipotente a un subconjunto propio de él mismo, lo que es imposible debido a que I_n es finito. Entonces debe ser $n \leq m$.

(2) Sea $f : A \longrightarrow B$ suprayectiva y $g : B \longrightarrow A$ un inverso derecho de f. Entonces g es inyectiva (ejercicio 1.5.17 (2) del capítulo 1) y por el inciso (1), $m \leq n$. ∎

Teorema 3.1.10. *Sean A y B conjuntos finitos tales que $card(A) = card(B)$ y sea $f : A \longrightarrow B$ una función. Son equivalentes*

(1) f es inyectiva.
(2) f es suprayectiva.

Demostración. Sean $card(A) = card(B) = n$ y $g : I_n \longrightarrow A$ y $h : I_n \longrightarrow B$ biyectivas.

(1) Supongamos que f es inyectiva.
Si f no es suprayectiva, entonces, por el ejercicio 1.5.16 (2), $h^{-1} \circ f \circ g : I_n \longrightarrow I_n$ es inyectiva pero no suprayectiva y así I_n es equipotente a un subconjunto propio de I_n lo que es una contradicción. Por lo tanto f debe ser suprayectiva.

(2) Supongamos que f es suprayectiva. Entonces cualquier inverso derecho f' de f es inyectiva (véase ejercicio 1.5.17 (2)). Si f no fuera inyectiva, entonces f' no es suprayectiva y así $h \circ f' \circ g^{-1} : I_n \longrightarrow I_n$ es inyectiva pero no suprayectiva y esto implica, como en el caso (1), que I_n es equipotente a un subconjunto propio de I_n lo cual es una contradicción y por lo tanto f debe ser inyectiva. ∎

De acuerdo al teorema anterior, cuando dos conjuntos finitos tiene la misma cardinalidad, para demostrar que una función $f : A \longrightarrow B$ es biyectiva, es suficiente demostrar solamente que f es inyectiva o que f es suprayectiva.

Teorema 3.1.11. *Sea A un conjunto finito de cardinalidad $n \geq 1$. Para toda $a \in A$, $card(A - \{a\}) = n - 1$.*

Demostración. Como $card(A) = n$, entonces existe una función biyectiva $f : I_n \longrightarrow A$. Sea $a \in A$. Si $A - \{a\} = \emptyset$, entonces $A = \{a\}$ y $card(A) = 1$. Por lo tanto

$$card(A - \{a\}) = card(\emptyset) = 0 = 1 - 1.$$

Supongamos, entonces que $n > 1$ y sea $j \in I_n$ tal que $f(j) = a$ (f es suprayectiva.)
$1^{\underline{er}}$ caso: $j = n$. En este caso la función $f' : I_{n-1} \longrightarrow A - \{a\}$ es biyectiva, así que $card(A - \{a\}) = n - 1$.
$2^{\underline{o}}$ caso: $j \neq n$. En este caso modificaremos la función biyectiva $f : I_n \longrightarrow A$ para reducir al primer caso.
Sea $f(n) = a'$. Por hipótesis $a' \neq a$. Consideramos la siguiente función biyectiva $g : I_n \longrightarrow I_n$ definida por

$$g(k) = \begin{cases} k & \text{si } k \neq j, \text{ y } k \neq n; \\ n & \text{si } k = j; \\ j & \text{si } k = n. \end{cases}$$

Entonces $f \circ g : I_n \longrightarrow A$ es biyectiva y tiene regla de correspondencia:

$$(f \circ g)(k) = \begin{cases} f(k) & \text{si } k \neq j, \text{ y } k \neq n; \\ a' & \text{si } k = j; \\ a & \text{si } k = n. \end{cases}$$

Estamos en las condiciones del caso anterior, por lo que concluimos que $card(A - \{a\}) = n - 1$. ∎

Teorema 3.1.12. *Si A es un conjunto finito y $B \subseteq A$, entonces B es finito.*

Demostración. Por inducción sobre n=card(A)

$1^{\underline{o}}$ $n = 0$. Entonces $A = \emptyset$ y el único subconjunto de A es A mismo.

$2^{\underline{o}}$ Supongamos cierto el resultado para $n \geq 0$. Lo demostraremos para $n + 1$. Sea $card(A) = n + 1$. Si $B = A$, entonces B es finito, así que supongamos que $B \subsetneq A$ y sea $a \in A$ tal que $a \notin B$. Entonces $B \subseteq A - \{a\}$ y por el teorema 3.1.11,

$$card(A - \{a\}) = (n + 1) - 1 = n.$$

Por hipótesis de inducción, B debe ser finito. ∎

Corolario 3.1.13. *Si A es finito, entonces $A \cap B$ y $A - B$ son finitos para todo conjunto B.*

Demostración. Como $A \cap B$ y $A - B$ son subconjuntos de A que es finito, entonces deben ser finitos (teorema 3.1.12). ∎

Teorema 3.1.14. *Si A y B son conjuntos finitos, entonces $A \cup B$ es finito.*

Demostración. Si $A = \varnothing$ o $B = \varnothing$, entonces $A \cup B = B$ en el primer caso y $A \cup B = A$ en el segundo y por lo tanto en ambos $A \cup B$ es finito.
Supongamos entonces que $card(A) = n \geq 1$ y $Card(B) = m \geq 1$. Se pueden presentar dos casos, $A \cap B = \varnothing$ o $A \cap B \neq \varnothing$.

$1^{\underline{er}}$ caso: $A \cap B = \varnothing$. Sean $f : I_n \longrightarrow A$ y $g : I_m \longrightarrow B$ biyectivas. Sea $h : I_{n+m} \longrightarrow A \cup B$ definida por:

$$h(j) = \begin{cases} f(j) & \text{si } 1 \leq j \leq n; \\ g(j-n) & \text{si } n+1 \leq j \leq n+m. \end{cases}$$

h es una función biyectiva (véase ejercicio 3.1.4)y por lo tanto $A \cup B$ es finito de cardinalidad $n + m$.

$2^{\underline{o}}$ caso: $A \cap B \neq \varnothing$. Sea $A' = A - (A \cap B)$. Entonces $A' \cap B = \varnothing$ y además como $A' \subseteq A$ con A finito, por el corolario 3.1.13, A' es finito y por el caso (1), $A' \cup B$ es finito. Luego $A \cup B = A' \cup B$ es finito. ∎

Corolario 3.1.15. *Si A y B son conjuntos finitos y ajenos, entonces*

$$card(A \cup B) = card(A) + card(B).$$

Demostración. Si $A = \varnothing$ o $B = \varnothing$, entonces $A \cup B = B$ o $A \cup B = A$, respectivamente, y en tal caso el resultado es inmediato. Ahora, si $card(A) = n \geq 1$ y $card(b) = m \geq 1$, la función $h : I_{n+m} \longrightarrow A \cup B$ definida en el primer caso de la demostración del teorema 3.1.14 es biyectiva y por lo tanto $card(A \cup B) = n + m = card(A) + card(B)$. ∎

Teorema 3.1.16. *Sean A y B conjuntos finitos. Entonces*

(1) $card(C) \leq card(A)$ *para todo C subconjunto de A.*
(2) $card(A - C) = card(A) - card(C)$ *para todo subconjunto C de A.*
(3) $card(A \cup B) = card(A) + card(B) - card(A \cap B)$.

Demostración.

(1) Sea $C \subseteq A$. Entonces, por el teorema 3.1.12, C es un conjunto finito. Como la función inclusión $i : C \longrightarrow A$ dada por $i(x) = x$ para toda $x \in C$ es inyectiva, por el teorema 3.1.9 (1), $card(C) \leq card(A)$.

(2) $C \subseteq A$ y $A - C \subseteq A$ implica que C y $A - C$ son conjuntos finitos y por (1)

$$card(C) \leq card(A) \;\; y \;\; card(A - C) \leq card(A).$$

Entonces

$$card(A) = card(C \cup (A - C)) = card(C) + card(A - C).$$

siendo la última igualdad por el corolario 3.1.15. Luego

$$card(A - C) = card(A) - card(C).$$

(3) $A \cup B = A \cup (B - (A \cap B))$; donde $A \cap (B - (A \cap B)) = \varnothing$. Entonces

$$\begin{aligned} card(A \cup B) &= card(A \cup (B - (A \cap B))) \\ &= card(A) + card(B - (A \cap B)) && \text{(corolario 3.1.15)} \\ &= card(A) + card(B) - card(A \cap B) && \text{(por (2)).} \blacksquare \end{aligned}$$

Teorema 3.1.17. *Sean $A_1, \ldots, A_n$ conjuntos finitos. Entonces $A_1 \cup A_2 \cup \cdots \cup A_n$ es finito y para $n \geq 1$, si los conjuntos son ajenos dos a dos, entonces*

$$card(A_1 \cup A_2 \cup \cdots \cup A_n) = card(A_1) + \cdots + card(A_n).$$

Demostración. Por inducción sobre $n \geq 2$

1º/ Si $n = 2$, $A_1 \cup A_2$ es finito por el teorema 3.1.14 y si $A_1 \cap A_2 = \varnothing$, por el corolario 3.1.15, $card(A_1 \cup A_2) = card(A_1) + card(A_2)$.

2º/ Suponemos cierto el resultado para $n \geq 2$ y sean $A_1, \ldots, A_n, A_{n+1}$ conjuntos finitos. Por hipótesis de inducción $A_1 \cup \cdots \cup A_n$ es finito y por lo tanto por el teorema 3.1.16 $(A_1 \cup \cdots \cup A_n) \cup A_{n+1}$ es finito. Ahora, $A_i \cap A_j = \varnothing$ para cada i, j con $i \neq j$, $1 \leq i, j \leq n$, entonces por hipótesis de inducción

$$card(A_1 \cup \cdots \cup A_n) = card(A_1) + \cdots + card(A_n).$$

Como $A_{n+1} \cap A_i = \varnothing$ para todo $i = 1, \ldots, n$, entonces

$$A_{n+1} \cap (A_1 \cup \cdots \cup A_n) = (A_{n+1} \cap A_1) \cup \cdots \cup (A_{n+1} \cap A_n) = \varnothing,$$

así que

$$\begin{aligned} card(A_1 \cup \cdots \cup A_n \cup A_{n+1}) &= card(A_1 \cup \cdots \cup A_n) + card(A_{n+1}) \\ &= card(A_1) + \cdots + card(A_n) + card(A_{n+1}). \blacksquare \end{aligned}$$

Teorema 3.1.18. *Sean A y B conjuntos finitos. Entonces $A \times B$ es finito y*

$$card(A \times B) = card(A) \cdot card(B).$$

Demostración. Sean $n = card(A)$, $m = card(B)$ y $A = \{a_1, a_2, \ldots, a_n\}$. Para cada $i \in \{1, \cdots, n\}$, $\{a_i\} \times B \approx B$ (ver ejercicio 3.1.3), entonces

$$A \times B = (\{a_1\} \times B) \cup \cdots \cup (\{a_n\} \times B),$$

por el teorema 3.1.17, es finito. Por otro lado, como $(\{a_i\} \times B) \cap (\{a_j\} \times B) = \emptyset$ para cualesquiera i, j con $i \neq j$ y $1 \leq i, j \leq n$ también por el teorema 3.1.17

$$\begin{aligned} card(A \times B) &= card((\{a_1\} \times B) \cup \cdots \cup (\{a_n\} \times B)) \\ &= card(\{a_1\} \times B) + \cdots + card(\{a_n\} \times B) \\ &= \underbrace{m + \cdots + m}_{n-veces} \\ &= card(A) \cdot card(B). \blacksquare \end{aligned}$$

Teorema 3.1.19. *Si X es un conjunto finito, entonces $\mathscr{P}(X)$ (ver definición 1.2.19) es un conjunto finito de cardinalidad $2^{card(X)}$.*

La demostración de este teorema se encuentra en el capítulo 4. (teorema 4.1.19)

Teorema 3.1.20. *Si $\emptyset \neq A \subseteq \mathbb{N}$ y A es finito, entonces A tiene mínimo y máximo.*

Demostración. Como $A \neq \emptyset$, por el Axioma del Buen Orden, A tiene mínimo. La existencia del máximo lo demostraremos por inducción sobre $Card(A) = n \geq 1$.

1º/ Si $n = 1$. En este caso $A = \{a\}$, por lo que a debe ser el máximo (que coincide con el mínimo).

2º/ Supongamos que cada conjunto de cardinalidad n tiene máximo y sea $card(A) = n+1$. Tomemos cualquier elemento $a \in A$. Si a es máximo en A terminamos. Supongamos entonces que a no es máximo en A y consideremos $A' = A - \{a\}$. Por el teorema 3.1.11, $card(A') = n$ y por hipótesis de inducción A' debe tener máximo a_0. Afirmamos que a_0 es el máximo de A. Como $x \leq a_0$ para todo $x \in A'$ y $A = A' \cup \{a\}$ sólo falta ver que $a \leq a_0$. Pero por hipótesis a no es máximo en A y por lo tanto existe $a' \in A$ tal que $a < a'$. Esto último implica que $a \neq a'$ y entonces $a' \in A'$, por lo que $a' \leq a_0$ y por ser $a \leq a'$ tenemos que $a \leq a_0$. $\blacksquare$

Por último, veamos que $\mathbb{N}$ no es un conjunto finito.

Teorema 3.1.21. *El conjunto $\mathbb{N}$ de los números naturales es infinito.*

Demostración. La función $f : \mathbb{N} \longrightarrow \mathbb{N}$ dada por $f(x) = 2x$ es una función inyectiva que no es suprayectiva y por lo tanto $\mathbb{N}$ es equipotente a un subconjunto propio de él, que por definición significa que $\mathbb{N}$ es infinito. ∎

Definición 3.1.22. *Un conjunto X es* **numerable** *si $X \approx \mathbb{N}$.*

Más adelante veremos que el conjunto de los números enteros y el conjunto de los números racionales son conjuntos numerables.

§ 3.2. Ejercicios del capítulo 3.

3.1.1. Demuestre que la función g definida en la demostración de la proposición 3.1.5 página 158 es biyectiva.

3.1.2. Sea B un conjunto. Demostrar que $\{a\} \times B \approx B$.

3.1.3. Sean A y B conjuntos finitos tal que $A = \{a_1, \cdots, a_n\}$. Demuestre que para cada
$i \in \{1, \cdots, n\}$ se tiene que $\{a_i\} \times B \approx B$.

3.1.4. Demuestre que la función h definida en el teorema 3.1.14 es biyectiva

3.1.5. Demostrar que la función $g : I_n \to I_n$ definida (ii) de la demostración de la proposición 3.1.5 es biyectiva.

3.1.6. Demuestre que:

(1) $\mathbb{N} \approx \mathbb{N} - \{0, 1, 2\}$;
(2) $\mathbb{N} \approx \left\{n^2 \mid n \in \mathbb{N}\right\}$;
(3) $\{2n \mid n \in \mathbb{N}\} \approx \{2m + 1 \mid m \in \mathbb{N}\}$.

3.1.7. Sean A, B, C y D conjuntos. Muestre que:

(1) $A \times B \approx B \times A$;
(2) $(A \times B) \times C \approx A \times (B \times C)$;
(3) Para todo x, $A \approx A \times \{x\}$;
(4) Si $A \approx B$ y $C \approx D$, entonces $A \times C \approx D \times B$;
(5) Si $A \approx B$ y $C \approx D$, entonces $(A \times \{0\}) \cup (C \times \{1\}) \approx (B \times \{0\}) \cup (D \times \{1\})$;
(6) Si $A \approx B$ entonces $\mathcal{P}(A) \approx \mathcal{P}(B)$.

3.1.8. Sean A_1, A_2 y A_3 conjuntos finitos. Muestre que

$$card(A_1 \cup A_2 \cup A_3) = card(A_1) + card(A_2) + card(A_3) - card(A_1 \cap A_2) - card(A_1 \cap A_3) - card(A_2 \cap A_3) + card(A_1 \cap A_2 \cap A_3).$$

Proponga una fórmula para cuando se tienen cuatro conjuntos finitos A_1, A_2, A_3, A_4.

3.1.9. Sean A y B conjuntos finitos. Demuestre que

$$card(A \triangle B) = card(A) + card(B) - 2 \cdot card(A \cap B).$$[1]

3.1.10. Sea A un conjunto finito, y sea $\{A_i \mid i = 1, \ldots, n\}$ una familia de conjuntos tal que $A = A_1 \cup \cdots \cup A_n$. Demuestre que $\{A_i \mid i = 1, \ldots, n\}$ es una partición de A si y sólo si $Card(A) = Card(A_1) + \ldots + Card(A_n)$.

3.1.11. Sea X un conjunto finito, y sean $A, B \subseteq X$. Ordene la siguiente lista, en orden creciente de acuerdo con el tamaño:

(1) $card(A \cup B)$, $card(B)$, $card(\varnothing)$, $card(A \cap B)$ y $card(X)$.
(2) $card(A - B)$, $card(A) + card(B)$, $card(\varnothing)$, $card(A \bigtriangleup B)$, $card(A \cup B)$ y $card(X)$.
(3) $card(A - B)$, $card(\varnothing)$, $card(A)$, $card(A) + card(B)$, $card(A \cup B)$ y $card(X)$.

3.1.12. Determine si cada una de las siguientes proposiciones es falsa o verdadera. Para cada proposición falsa, dé un contraejemplo.

(1) Para cualquier conjunto X, la relación $\approx$ definida sobre los subconjuntos de X es una relación de equivalencia en $\mathscr{P}(A)$.
(2) Si A es un conjunto finito y $A \approx B$, entonces B es finito.
(3) Si A y B son conjuntos infinitos, entonces $A \cap B$ es infinito.
(4) Si B es infinito y $A \subseteq B$, entonces A es infinito.
(5) Si A y B son conjuntos numerables, entonces $A - B$ es numerable.
(6) Si A es finito y $A \subseteq B$, entonces B es finito.
(7) Si A es infinito y $A \subseteq B$, entonces B es infinito.
(8) Si $A \approx B$ y A es infinito, entonces B es infinito.
(9) Si $f : \mathbb{N} \longrightarrow B$ es una función inyectiva, entonces B es infinito.
(10) Si $f : A \longrightarrow \mathbb{N}$ es una función suprayectiva, entonces f es inyectiva.
(11) Si $f : \mathbb{N} \longrightarrow B$ es una función y B es finito, entonces f es suprayectiva.
(12) Si $n \leq m$, entonces cualquier función $f : I_n \longrightarrow I_m$ es inyectiva.

[1] Véase la definición de diferencia simétrica en la página 87.

(13) Si $m \leq n$, entonces existe una función $f : I_n \longrightarrow\!\!\!\!\!\rightarrow I_m$ suprayectiva.

(14) Si $f : I_{20} \longrightarrow\!\!\!\!\!\rightarrow I_5 \times I_4$ es una función inyectiva, entonces f es biyectiva.

3.1.13. Para cada $n \in \mathbb{N}$, sea $A_n = \{n, 2n, 3n, \ldots\}$. Pruebe que si J es un subconjunto infinito de $\mathbb{N}$, entonces $\bigcap_{i \in J} A_i = \emptyset$.

3.1.14. Sean A y B conjuntos con $A \subseteq B$. Si B es finito y $card(A) = card(B)$, demuestre que $A = B$.

3.1.15. Sea X un conjunto, y sea $\{f_n\}_{n \in \mathbb{N}}$ una familia de funciones inyectivas $f_n : I_n \longrightarrow X$. Demuestre que X es infinito.

3.1.16. Sean A y B conjuntos. Definimos el conjunto A^B como

$$A^B = \{f : B \longrightarrow A \mid f \text{ es función}\}.$$

Demuestre que:

(1) $A^{\emptyset} \approx \{\emptyset\}$.
(2) $A^{\{x\}} \approx A$.
(3) $A^{\{x,y\}} \approx A \times A$.
(4) Si A y B son finitos, entonces A^B es finito.
(5) Si A, B, A' y B' son conjuntos tales que $A \approx A'$ y $B \approx B'$, entonces $A^B \approx (A')^{B'}$.

3.1.17. Defina una relación de equivalencia en el conjunto $\mathbb{N}$ que tenga infinitas clases de equivalencia.

3.1.18. Sea A un conjunto de números naturales tal que para todo par de números naturales m, k:

$$\text{Si } m \in X \text{ y } k < m, \text{ entonces } k \in X.$$

Concluya que o bien $X = \mathbb{N}$ o bien hay $n \in \mathbb{N}$ tal que $X = I_n$.

3.1.19. Sea $(X, <)$ un conjunto parcialmente ordenado.

(1) Si $<$ es un orden total, entonces todo subconjunto finito y no vacío de X tiene máximo y mínimo.
(2) Si X es finito y $<$ es un orden total, entonces $<$ es un buen orden.

3.1.20. Si $(X, <)$ es un conjunto parcialmente ordenado y X es finito, entonces X tiene un elemento maximal y uno minimal.

3.1.21. Demuestre que todo conjunto finito X se puede bien ordenar, es decir, se puede definir un orden $<$ en X de modo que éste sea un buen orden.

3.1.22. Sean A y B conjuntos finitos. Demuestre que $card(A \triangle B) = card(A) + card(B) - 2 \cdot card(A \cap B)$.[2]

3.1.23. Justifique (utilizando lo visto en esta sección) la siguiente proposición: Si se dispone de n casillas para colocar m objetos y $m > n$, entonces en alguna casilla deberán colocarse por lo menos dos objetos.
El resultado anterior es llamado el Principio de las Casillas (o también el Principio de los Palomares).

3.1.24. (1) Demuestre que si 13 personas están en un cuarto, al menos dos de ellas cumplen años el mismo mes.
(2) Demuestre que si 8 personas están en un cuarto, al menos dos de ellas cumplen años el mismo día de la semana.
(3) Un costal está lleno de canicas de 20 colores distintos. ¿Cuál es el mínimo número de canicas que deben sacarse para poder garantizar que en la colección tomada habrá al menos 100 canicas del mismo color?

3.1.25. Demuestre que si se distribuyen m objetos en n cajas y $m > nr$ para algún $r \geq 1$, entonces al menos una caja tiene más de r objetos.

3.1.26. Sea $f : X \longrightarrow Y$ una función entre dos conjuntos finitos X y Y tal que para todo elemento $y \in Y$, $card(f^{-1}(y)) = k$ para cierto natural k. ¿Cómo se comparan $card(X)$ y $card(Y)$?

3.1.27. Sea A un conjunto de números naturales tal que para todo par de números naturales m, k:

$$\text{Si } m \in A \text{ y } k < m, \text{ entonces } k \in A.$$

Concluya que o bien $A = \mathbb{N}$ o bien hay $n \in \mathbb{N}$ tal que $A = I_n$.

3.1.28. Muestre que todo subconjunto de $\mathbb{N}$ acotado superiormente es finito.

3.1.29. Muestre que el conjunto potencia de un conjunto finito es conjunto finito.
Sugerencia: En primer lugar, observe que si $x \notin A$ y $B = A \cup \{x\}$, entonces

$$\mathcal{P}(B) = \mathcal{P}(A) \cup \{C \cup \{x\} \mid C \subseteq A\}.$$

[2] Véase la definición de diferencia simétrica en la página 87.

Luego muestre por inducción que, para todo número natural n, el conjunto potencia de un conjunto de n elementos es finito.

3.1.30. Sea $f : X \longrightarrow Y$ una función, y sean $A \subseteq X$ y $B \subseteq Y$. Muestre que si A y B son conjuntos finitos entonces $f[A]$ y $f^{-1}[B]$ también lo son. ¿Qué se puede decir en el caso en que A y B son infinitos?.

3.1.31. Sea X un conjunto, y sea $x_0 \in X$. Demuestre que si X es infinito entonces $X - \{x_0\}$ también lo es.

3.1.32. Para una relación R sobre un conjunto X definimos el símbolo R^n por recursión: $R^1 = R$, $R^{n+1} = R \circ R^n$.

(1) Prueba que si X es finito y R es una relación sobre ese conjunto, entonces existen $r, s \in \mathbb{N}$, $r < s$, tales que $R^r = R^s$.
(2) Encuentra una relación R sobre un conjunto finito tal que $R^n \neq R^{n+1}$ para cada $n \in \mathbb{N}$.
(3) Muestra que si X es infinito, la afirmación del primer inciso (de este ejercicio) no tiene por qué cumplirse (es decir, una relación R puede existir de manera que todas las relaciones R^n, $n \in \mathbb{N}$, sean distintas entre sí).

3.1.33. Sea R una relación sobre un conjunto X tal que no existe ninguna sucesión finita de elementos $x_1, x_2, \ldots, x_k$ de X que satisfagan x_1Rx_2, x_2Rx_3, x_3Rx_4, $\ldots$, $x_{k-1}Rx_k$, x_kRx_1 (decimos que R es acíclico). Suponga que X es finito. Muestre que existe un orden $\preceq$ sobre X tal que $R \subseteq \preceq$.

3.1.34. Defina una relación de equivalencia en el conjunto $\mathbb{N}$ que tenga infinitas clases de equivalencia.

3.1.35. (1) ¿Es cierto que si R es una relación de equivalencia en un conjunto A infinito, entonces el conjunto cociente A/R ha de ser necesariamente un conjunto infinito?.
(2) ¿Es cierto que si R es una relación de equivalencia definida en un conjunto A infinito, entonces cada clase de equivalencia ha de ser también un conjunto infinito?.
(3) Si R es una relación de equivalencia definida en un conjunto finito A de modo que R y A tienen el mismo número de elementos, ¿qué se puede afirmar sobre la relación R?.

3.1.36. Sea $\{A, B, C\}$ una familia de conjuntos y $E = A \cup B \cup C$. Suponga que E es un conjunto finito de n elementos de los cuales la mitad están en A. Si se sabe que $card(A \cap B) = card(A \cap C) = card(B \cap C) = \frac{n}{5}$ y que $card(A \cap B \cap C) = \frac{n}{10}$. Averigüe el número de elementos de $B \cup C$

3.1.37. En una encuesta realizada a personas que habitualmente ven la televisión se obtuvieron los siguientes datos:

(1) 64 ven programas informativos.
(2) 94 ven programas deportivos.
(3) 58 ven programas culturales.
(4) 28 ven programas informativos y culturales.
(5) 26 ven programas informativos y deportivos.
(6) 22 ven programas deportivos y culturales.
(7) 14 ven los tres tipos de programas.

(1) ¿Cuántas personas respondieron a la encuesta?
(2) ¿Cuántos de los encuestados ven informativos y no ven programas culturales?
(3) ¿Cuántos hay que no ven programas culturales?

3.1.38. En una escuela se imparten tres cursos, uno de Literatura, uno de Biología y uno de Matemáticas. De los 250 estudiantes de la escuela 180 aprobaron Matemáticas, 120 Biología y 80 de Literatura. Entre ellos, 95 aprobaron Matemáticas y Biología, 33 Matemáticas y Literatura y 10 Literatura y Biología y sólo 8 aprobaron los tres cursos.

(1) ¿Cuántos aprobaron sólo Matemáticas y Biología?
(2) ¿Cuántos aprobaron sólo Matemáticas?
(3) ¿Cuántos estudiantes no aprobaron ningún curso?
(4) ¿Cuántos aprobaron sólo un curso?
(5) ¿Cuántos aprobaron exactamente dos cursos?
(6) ¿Cuántos aprobaron Biología, pero no lo hicieron en Matemáticas?

Vale más saber alguna cosa de todo, que saberlo todo de una sola cosa.
Blaise Pascal
1623 - 1662

***Capítulo* 4**

Calculo combinatorio

En Teoría de Probabilidades, el poder contar el número de resultados de un evento es fundamental para conocer la probabilidad de que cierto resultado del evento ocurra. En el cálculo combinatorio se estudian ciertas técnicas de conteo y con la ayuda de funciones se pueden presentar de una manera clara estos conceptos de la combinatoria. Hay tres problemas típicos que se presentan aquí y combinaciones de éstos. Veamos un ejemplo de cada uno de estos tres problemas típicos:

(1) Se quiere confeccionar una bandera de 3 franjas, donde cada franja puede ser de color rojo, verde, amarillo o blanco sin importar que haya más de una franja del mismo color. ¿De cuántas maneras puede hacerse esto?

(2) Se quiere elegir un comité de 3 personas, de un total de 20, de las cuales una debe ser presidente, la otra secretario y la otra tesorero. ¿De cuántas maneras se puede elegir a dicho comite?

(3) De un grupo de 30 niños se quiere escoger a 3 para que se presenten en un festival. ¿De cuántas maneras se pueden elegir a estos 3 niños?

Para responder a estas preguntas trataremos de interpretar estos problemas con un lenguaje matemático en cada uno de los ejemplos.

(1) En este problema es importante tener en cuenta el orden ya que no es lo mismo una bandera cuyos colores en orden son rojo, rojo y amarillo que una que tenga estos mismos colores, como es rojo, amarillo, rojo. Denotemos por 1,2,3

a los lugares de cada franja en la bandera y denotemos por $\mathfrak{A}$ al conjunto de los colores que se usan para esta bandera, es decir, $\mathfrak{A} = \{R, V, A, B\}$, donde R=rojo, V=verde, A=amarillo y B=blanco. Para cada una de las tres franjas de la bandera debemos escoger un color de $\mathfrak{A}$. Cada selección de los tres colores (que se puede repetir) se pueden ver como una función de $I_3 = \{1, 2, 3\}$ en $\mathfrak{A}$; esto es, si la selección fue rojo, rojo, amarillo, ésta corresponde a la función $f : I_3 \longrightarrow \mathfrak{A}$ donde $f(1) = R$, $f(2) = R$ y $f(3) = A$. Inversamente, si damos una función $g : I_3 \longrightarrow \mathfrak{A}$, ésta determina una selección de colores para la bandera; por ejemplo, si $g : I_3 \longrightarrow \mathfrak{A}$ está dada por $g(1) = A$, $g(2) = V$ y $g(3) = B$, entonces los colores para la bandera en ese orden serán amarillo, verde y blanco. Resumiendo, cada selección podemos verla como una función $f : I_3 \longrightarrow \mathfrak{A}$, donde selecciones distintas inducen funciones distintas e inversamente cada función de I_3 en $\mathfrak{A}$ determina una selección. Así pues para saber de cuántas maneras se puede confeccionar una bandera de 3 franjas con estos colores rojo, amarillo, verde y blanco debemos contar el número de funciones que hay de I_3 a $\mathfrak{A}$.

(2) En este problema se pide contar el número de comités posibles con 3 personas de entre un grupo de 20 personas donde uno debe ser el presidente, otro secretario y el otro tesorero, pero aún cuando en algún comité aparezcan las personas A, B y C, en otro pueden también aparecer pero con cargo distinto, es decir, no es lo mismo, el comité donde A es presidente, B secretario y C tesorero, que el comité donde B es el presidente, C es secretario y A el tesorero. Para visualizar este problema, denotemos por 1 al cargo de presidente, por 2 al cargo de secretario y por 3 al cargo de tesorero. Elegir un comité es asignarle a cada uno de 1,2,3 una persona de las 20 elegibles. Esto es, elegir un comité es lo mismo que dar una función de $I_3 = \{1, 2, 3\}$ en el conjunto de 20 personas. Pero debemos tener cuidado, porque tampoco puede ser cualquier función, ya que una persona no puede ocupar dos cargos a las vez, esto es, si se eligió a las personas A, B, C ocupando los cargos de presidente (1), secretario (2) y tesorero (3) respectivamente, la función correspondiente a esta elección es $f : \{1, 2, 3\} \longrightarrow G$, donde G es el conjunto de 20 personas y $f(1) = A$, $f(2) = B$ y $f(3) = C$, y se debe tener que $f(1) \neq f(2)$, $f(1) \neq f(3)$ y $f(2) \neq f(3)$. ¿cuál es la propiedad que debe tener f? Evidentemente f debe ser inyectiva. Inversamente cada función inyectiva determina un comité. Resumiendo, elegir un comité es equivalente a dar una función inyectiva $f : \{1, 2, 3\} \longrightarrow G$, por lo que para saber cuántas elecciones posibles

se pueden hacer habrá que contar cuántas funciones inyectivas hay de I_3 en G.

(3) Queremos escoger a 3 niños de entre un grupo de 30. En este caso el orden en que se escogió estos 3 niños es irrelevante, por lo que dar una elección de 3 niños de entre 30 es lo mismo que dar un subconjunto de 3 elementos del conjunto de 30 niños. Así que para saber cuántas elecciones posibles hay debemos contar cuántos subconjuntos de 3 elementos tiene un conjunto de 30 elementos.

Veamos la diferencia que existe entre estos tres tipos de problemas. En el primero se vio que el orden es importante y que los elementos (colores) se pueden repetir en la terna a escoger. En el segundo también el orden es importante, pero a diferencia del primero, en la terna todos los elementos deben ser distintos. En el tercer problema, como lo comentamos, el orden en que se dé a los niños elegidos no importa a diferencia evidentemente de los primeros dos problemas.
Resumiendo, para dar respuesta a cada uno de los tres tipos de problemas anteriores debemos encontrar, en general,

(1) El número de funciones que hay de un conjunto con m elementos en un conjunto con n elementos.
(2) El número de funciones inyectivas de un conjunto con m elementos en un conjunto con n elementos.
(3) El número de subconjuntos con m elementos de un conjunto con n elementos.

Con la finalidad de presentar estos conceptos en el contexto del cálculo combinatorio les daremos nombres especiales a estos tres conceptos haciendo alusión a su naturaleza. Estos son, *ordenaciones con repetición*, *ordenaciones* y *combinaciones*.

§ 4.1. Ordenaciones con repetición, ordenaciones y combinaciones

Definición 4.1.1*. Las* **ordenaciones con repetición** *de n elementos tomados de m en m son las funciones de I_m en el conjunto de esos n elementos y al número total de ellas lo denotaremos* $\boldsymbol{OR_n^m}$.[1]

[1] Algunos autores denotan las ordenaciones con repetición por $\boldsymbol{OR_m^n}$.

Definición 4.1.2*. Las* **ordenaciones** *de n elementos tomados de m en m son las funciones inyectivas de $I_m = \{1, 2, \ldots, m\}$ en el conjunto de esos esos n elementos, y al número total de ellas lo denotaremos* $\boldsymbol{O_n^m}$.[2]

Definición 4.1.3*. Las* **combinaciones** *de n elementos tomados de m en m son los subconjuntos con m elementos del conjunto de n elementos y al número total de ellos lo denotaremos por* $\boldsymbol{C_n^m}$.[3]

Nota 4.1.4. En el caso en que $n < m$, evidentemente $O_n^m = 0$ y $C_n^m = 0$. Además para las ordenaciones y ordenaciones con repeticiones, consideramos $m \geq 1$. En lo que sigue para las ordenaciones sólo consideraremos $1 \leq m \leq n$ y para las combinaciones $0 \leq m \leq n$.

Nota 4.1.5. Debido a su importancia, a las ordenaciones de n elementos tomados de n en n (es decir cuando $n = m$) las llamaremos ***permutaciones*** de n elementos y por el teorema 3.1.10 no son otra cosa que las funciones biyectivas de I_n en un conjunto de n elementos y en este caso el número total de ellas lo denotaremos $\boldsymbol{P_n}$.

Antes de encontrar los valores de OR_n^m, O_n^m y C_n^m, nos será de utilidad el siguiente resultado.

Proposición 4.1.6*. Si A es un conjunto con m elementos y B un conjunto con n elementos, el número de maneras de escoger un elemento de A y un elemento de B es $m \cdot n$, teniendo en cuenta que la elección del elemento de B no depende del elemento de A seleccionado.*

Demostración. Cada selección de un elemento de A y un elemento de B determina un elemento de $A \times B$. Además si a' y b' son elementos de A y B respectivamente y son tales que $a \neq a'$ o $b \neq b'$, entonces $(a, b) \neq (a', b')$.
Por otro lado cada elemento (a, b) de $A \times B$, está determinado por un elemento de A y un elemento de B.
En base a lo anterior el número de maneras de seleccionar un elemento de A y un elemento de B es igual al número de elementos que tiene $A \times B$, que por el teorema 3.1.18 tiene $m \cdot n$ elementos. ∎

[2]Algunos autores denotan las ordenaciones por $\boldsymbol{O_m^n}$.
[3]Algunos autores denotan las combinaciones por $\boldsymbol{C_m^n}$ o también por $\boldsymbol{\binom{n}{m}}$.

Lema 4.1.7. *Sea $A = \{a_1, \ldots, a_n\}$ un conjunto con n elementos, $n \geq 1$. Entonces hay $n(n-1)$ parejas ordenadas (a_i, a_j) de elementos de A tales que $a_i \neq a_j$.*

Demostración. Sea $i \in I_n$ fija y sea $B_i = A - \{z_i\}$: Entonces el número de elementos de B_i es $n-1$. Ahora $\{(a_i, a_j) \mid a_i \neq a_j\} = \bigcup_{i=1}^{n} (a_i \times B_i)$ y como $(a_i \times B_i) \cap \left(a_j \times B_j\right)$ si $i \neq j$. Entonces, por el teorema 4.1.17,

$$card\left(\bigcup_{i=1}^{n}(a_i \times B_i)\right) = \sum_{i=1}^{n} card\,(a_i \times B_i) = \sum_{i=1}^{n}(n-1) = n(n-1).$$

Entonces hay $n(n-1)$ parejas ordenadas. ∎

Los siguientes ejemplos nos dan una idea de cuáles podrían ser los posibles valores de OR_n^m, O_n^m y C_n^m. Para esto sea A un conjunto con n elementos.

(1) Si queremos encontrar el número de funciones de I_2 en el conjunto A, debemos encontrar el número de posibilidades para la imagen de 1 y la imagen de 2. El número de maneras de escoger la imagen de 1 es n, tantos elementos como tiene A, y el número de maneras de escoger la imagen de 2 es n, ya que también puede ser cualquier elemento de A. Por lo tanto por la proposición 4.1.6, hay $OR_n^2 = n \cdot n = n^2$ maneras de escoger la imagen de 1 y de 2. Si consideramos I_3 en lugar de I_2, hay n maneras también de escoger la imagen de 3, así que en total hay $OR_n^3 = n^2 \cdot n = n^3$ funciones de I_3 en A.

(2) Encontremos ahora el número de funciones inyectivas de I_2 en el conjunto A. El número de maneras de escoger la imagen de 1 es n que es el número de elementos que tiene A. Pero aquí, a diferencia de (1), habiendo dado ya la imagen de 1, como queremos que la función sea inyectiva, la imagen de 2 puede ser cualquier elemento de A excepto el ya escogido para la imagen de 1, así que dar una función inyectiva de I_2 en A, es lo mismos que dar una pareja ordenada $(a, b) \in A \times A$ tal que $a \neq b$, donde la imagen de 1 es a y la imagen de 2 es b. De aquí tenemos que la función

$$F : B = \{f : I_2 \to A \mid f \text{ es inyectiva}\} \longrightarrow A' = \{(a, b) \in A \times A \mid a \neq b\}$$

definida por $F(f) = (f(1), f(2))$ es biyectiva.[4] Luego, por el lema 4.1.7, $O_n^2 = n \cdot (n-1) = \frac{n!}{(n-2)!}$.

Ahora si consideramos I_3 en lugar de I_2, cada función inyectiva $f : I_3 \to A$ determinará una terna (a_1, a_2, a_3) de elementos de A tal que $a_i \neq a_j$ si

[4] Ejercicio 4.1.1.

$i \neq j$ y donde $f(i) = a_i$, $i = 1, 2, 3$. Entonces, contar el número de estas funciones se reduce a contar el número de elementos que tiene el conjunto $B = \{(a_1, a_2, a_3) \in A \times A \times \mid a_i \neq a_j \text{ si } i \neq j \; i = 1, 2, 3\}$. Pero cada $(a_1, a_2, a_3) \in B$ se puede ver de la forma $((a_1, a_2), a_3)$. Como hemos visto el número de parejas (a_1, a_2) con $a_1 \neq a_2$ es O_n^2 y como cada una de estas determina $n - 2$ elecciones para a_3, habrá entonces

$$O_n^3 = O_n^2(n-2) = n(n-1)(n-2) = \frac{n!}{(n-3)!}$$

funciones inyectivas de I_3 en A.

(3) Encontremos ahora el número de subconjuntos con dos elementos de un conjunto A con n elementos.
Sea $\mathfrak{A} = \{f : I_2 \longrightarrow A \mid f \text{ es inyectiva}\}$. Entonces por (2) $card(\mathfrak{A}) = O_n^2$. Dada $f \in \mathfrak{A}$, existe $g \in \mathfrak{A}$ tal que $f \neq g$ y $Im(f) = Im(g)$. Esto es si $f(1) = a_1$ y $f(2) = a_2$, entonces $g : I_2 \longrightarrow A$ definida por $g(1) = a_2$ y $g(2) = a_1$ satisface que $Im(f) = Im(g)$ y $f \neq g$. Por cada subconjunto B con dos elementos de A, existen sólo dos funciones distintas f y g tales que $Im(f) = Im(g) = B$. Para cada $B \subseteq A$ tal que $card(B) = 2$ denotemos por f_B y g_B a las dos únicas funciones en $\mathfrak{A}$ tales que $Im(f_B) = B = Im(g_B)$.
Luego

$$\mathfrak{A} = \bigcup_{\substack{B \subseteq A \\ card(B)=2}} \{f_B, g_B\} \text{ donde es claro que } \{f_B, g_B\} \cap \{f_{B'}, g_{B'}\} = \varnothing \text{ si } B \neq B'.$$

Por lo tanto, por el teorema 3.1.17,

$$card(\mathfrak{A}) = card\Big(\bigcup_{\substack{B \subseteq A \\ card(B)=2}} \{f_B, g_B\}\Big) = \sum_{\substack{B \subseteq A \\ card(B)=2}} card(\{f_B, g_B\}) = \sum_{\substack{B \subseteq A \\ card(B)=2}} 2 = C_n^2 \cdot 2.$$

Por lo tanto $O_n^2 = 2 \cdot C_n^2$, es decir, $C_n^2 = \frac{O_n^2}{O_2^2} = \frac{O_n^2}{2!}$.
Para contar el número de subconjuntos con tres elementos de un conjunto con n elementos, lo podemos hacer de una manera análoga a la anterior, es decir, considerando $\mathfrak{A} = \{f : I_3 \longrightarrow A \mid f \text{ es inyectiva}\}$ y se puede ver que cada $f \in \mathfrak{A}$, determina un subconjunto de A con 3 elementos. Para cada $B \subseteq A$ tal que $card(B) = 3$, existen O_3^3 funciones en $\mathfrak{A}$ tal que tienen como imagen a B. Luego $O_n^3 = card(\mathfrak{A}) = O_3^3 C_n^3$, es decir, $C_n^3 = \frac{O_n^3}{O_3^3} = \frac{O_n^3}{3!}$.

Con estos ejemplos, aunque son pocos, podemos proponer las siguientes fórmulas:

$$OR_n^m = n^m, \quad O_n^m = n \cdot (n-1) \cdot \ldots \cdot (n-m+1) = \frac{n!}{(n-m)!}$$
$$\text{y} \qquad C_n^m = \frac{O_n^m}{O_m^m} = \frac{n!}{m! \cdot (n-m)!}.$$

Demostremos en general las igualdades anteriores.

Teorema 4.1.8. *Para cada $n \in \mathbb{N}$ y $m \in \mathbb{N}$, $OR_n^m = n^m$.*

Demostración. Por inducción sobre $m \geq 1$. Sea A un conjunto con n elementos.

(i) $m = 1$
Claramente el número de funciones de I_1 en A es n, pues el número de maneras en que podemos escoger la imagen de 1, que es el único elemento del dominio I_1, es n (tantas como elementos de A).
Por lo tanto $OR_n^1 = n = n^1$.

(ii) Supongamos que la fórmula es cierta para m, es decir, $OR_n^m = n^m$.
Cada función $f : I_{m+1} \longrightarrow A$ es una extensión de una función $g : I_m \longrightarrow A$ que es $g = f|_{I_m}$, así que basta contar de cuántas maneras podemos extender una función $g : I_m \longrightarrow A$ a una función $f : I_{m+1} \longrightarrow A$, es decir, para cada función $g : I_m \longrightarrow A$ debemos encontrar el número de funciones $f : I_{m+1} \longrightarrow A$ tales que $f|_{I_m} = g$.
Dada una función $g : I_m \longrightarrow A$, para extenderla a I_{m+1} debemos dar la imagen de $m+1$ y esto lo podemos hacer de n maneras ya que puede ser cualquier elemento de A. Por lo tanto, por la proposición 4.1.6 y por hipótesis de inducción $OR_n^m = n^m$, se tiene que

$$OR_n^{m+1} = n \cdot OR_n^m = n \cdot n^m = n^{m+1}. \blacksquare$$

Teorema 4.1.9. *Para cada $n \in \mathbb{N}$ y $m \in \mathbb{N}$, con $1 \leq m \leq n$,*

$$O_n^m = n \cdot (n-1) \cdot \ldots \cdot (n-m+1) = \frac{n!}{(n-m)!}.$$

Demostración. Por inducción sobre $m \geq 1$.

(i) $m = 1$. Sea A un conjunto con $n \geq 1$ elementos.
$O_n^1 =$ # de funciones inyectivas de $I_1 = \{1\}$ en A. Como $\{1\}$ tiene un único elemento, cualquier función $f : I_1 \longrightarrow A$ es inyectiva y por lo tanto hay n funciones inyectivas. Entonces $O_n^1 = n = \frac{n!}{(n-1)!}$.

(ii) Supóngase cierta la fórmula para $m \geq 1$, es decir, para toda n tal que $1 \leq m \leq n$, $O_n^m = \frac{n!}{(n-m)!}$. Demostrémoslo para $m+1$. Sea A un conjunto

con n elementos tal que $1 \leq m+1 \leq n$. Cada función inyectiva $f : I_{m+1} \longrightarrow A$ es extensión de una función inyectiva $g : I_m \longrightarrow A$ ya que $f|_{I_m}$ es inyectiva. Así que bastará contar de cuántas maneras podemos extender una función inyectiva de I_m en A a una función inyectiva de I_{m+1} en A.
Si $g : I_m \longrightarrow A$ es una función inyectiva y queremos extenderla a una función inyectiva $g : I_{m+1} \longrightarrow A$, solamente debemos escoger la imagen de $m+1$ teniendo en cuenta que esa imagen no puede ser ninguno de los valores $g(1), \ldots, g(m)$ en A ya que queremos que esta extensión siga siendo inyectiva. Entonces debemos escoger la imagen de $m+1$ de entre los elementos de $A - \{g(1), \ldots, g(m)\}$. Pero el número de elementos de este último conjunto, por ser $g(1), \ldots, g(m)$ todos distintos entre sí, es $n - m$ (teorema 3.1.16 (2)). Ahora, puesto que por cada función inyectiva de I_m en A, hay $(n-m)$ maneras de extender a una función inyectiva de I_{m+1} en A y por hipótesis de inducción hay $O_n^m = \frac{n!}{(n-m)!}$ funciones inyectivas de I_m en A, por la proposición 4.1.6 tenemos

$$\begin{aligned} O_n^{m+1} &= (n-m) \cdot O_n^m \\ &= (n-m) \cdot \tfrac{n!}{(n-m)!} = \tfrac{n!}{(n-m-1)!} = \tfrac{n!}{(n-(m+1))!}. \blacksquare \end{aligned}$$

Corolario 4.1.10. $P_n = n!$.

Demostración. Por definición $P_n = O_n^n = \frac{n!}{(n-n)!} = \frac{n!}{0!} = n!$. ∎

Teorema 4.1.11. *Para cada $n \in \mathbb{N}$ y $m \in \mathbb{N}$, con $0 \leq m \leq n$, $C_n^m = \frac{n!}{m!\cdot(n-m)!}$.*

Demostración. Sea A un conjunto con n elementos. El caso $m = 0$ es claro ya que A tiene un único subconjunto con 0 elementos, que es el conjunto vacío, así que

$$C_n^0 = 1 = \frac{n!}{n!} = \frac{n!}{0!(n-0)!}.$$

Supongamos que $m > 0$. Cada ordenación de los elementos de A tomados de m en m (funciones inyectivas de I_m en A) determina un subconjunto de A con m elementos. Si denotamos por $\mathfrak{O}$ al conjunto de las ordenaciones de A tomados de m en m y por $\mathfrak{C}$ al conjunto de las combinaciones de los elementos de A tomados de m en m, se tiene una función

$$\Phi : \mathfrak{O} \longrightarrow \mathfrak{C}$$

dada por $\Phi(f) = Im(f)$. Sea $f \in \mathfrak{O}$ y sea

$$f(1) = a_1, \ldots, f(m) = a_m.$$

Entonces $Im(f) = \{a_1, \ldots, a_m\}$. Cada $g \in \mathfrak{S}$ tal que $Im(g) = Im(f)$ determina una permutación de los elementos $a_1, \ldots, a_m$ que es $g(1), \ldots, g(m)$.
Inversamente, cada permutación de $a_1, \ldots, a_m$ determina una función inyectiva $g : I_m \longrightarrow A$ tal que $Im(g) = \{a_1, \ldots, a_m\}$ y por lo tanto por cada subconjunto B de A con m elementos hay $P_m = m!$ (corolario 4.1.10) funciones inyectivas de I_m en A cuya imagen es B. Entonces $m! \cdot C_n^m = O_n^m$, es decir,

$$C_n^m = \frac{n!}{m!(n-m)!}. \blacksquare$$

El siguiente resultado es de gran ayuda para resolver ciertos problemas.

Proposición 4.1.12. *Si un evento A se puede dar de m maneras y un evento B se puede dar de n maneras y si k es el número de resultados del evento A que coinciden con algún resultado del evento B, entonces el número de maneras en que se puede dar el evento A o el evento B es* $m + n - k$.

Demostración. Sea A' el conjunto de resultados que se pueden dar del evento A y B' el conjunto de resultados que se pueden dar del evento B. Por hipótesis, $card(A') = m$, $card(B') = n$. Sea $card(A' \cap B') = k$. El número de maneras en que se puede dar el evento A o el evento B es igual a la cardinalidad de $A' \cup B'$. Pero, por (3) del teorema 3.1.16,

$$card(A' \cup B') = card(A') + card(B') - card(A' \cap B') = m + n - k. \blacksquare$$

Daremos a continuación ejemplos de distintos tipos de problemas.

Ejemplo 4.1.13. Con 7 lienzos de distintos colores se quiere confeccionar una bandera que consta de tres colores distintos. ¿Cuántas maneras hay de confeccionar una bandera?
Como el orden en que se dan los colores es importante, debemos escoger 3 colores distintos ordenados de un total de 7 colores distintos. Entonces la selección se puede hacer de $O_7^3 = \frac{7!}{(7-3)!} = \frac{7!}{4!}$.

Ejemplo 4.1.14. Suponga que se tienen dos símbolos distintos y que se quiere representar cada letra del alfabeto con una sucesión de estos dos símbolos de tal manera que a letras distintas les correspondan sucesiones distintas. Una sucesión es de longitud n si consta de n símbolos. Se considera que dos sucesiones serán iguales si son de la misma longitud y en los lugares correspondientes de ambas sucesiones aparece el mismo símbolo. ¿Cuál es el valor mínimo de n para que

cada letra del alfabeto sea representada por una sucesión de longitud a lo más n considerando que el alfabeto tiene 27 letras?
Como los símbolos se pueden repetir y el orden en que se dan es importante, entonces
Si $n = 1$, el número de sucesiones que constan de 1 símbolos es

$$OR_2^1 = 2^1 = 2 < 27.$$

Si $n = 2$, el número de sucesiones que constan de 2 símbolos es

$$OR_2^2 = 2^2 = 4 < 27.$$

Si $n = 3$, el número de sucesiones que constan de 3 símbolos es

$$OR_2^3 = 2^3 = 8 < 27.$$

Si $n = 4$, el número de sucesiones que constan de 4 símbolos es

$$OR_2^4 = 2^4 = 16 < 27.$$

Si $n = 5$, el número de sucesiones que constan de 5 símbolos es

$$OR_2^5 = 2^5 = 32 \geq 27.$$

Entonces, como $2 > 27$, $2+4 = 6 < 27$, $2+4+8 = 14 < 27$, $2+4+8+16 = 30 > 27$, $n = 4$ será la mínima n con la propiedad deseada. En el caso en que todas las letras usen el mismo número de símbolos, $n = 5$ será la mínima n.

Ejemplo 4.1.15. De un conjunto de 20 personas se quiere nombrar a dos de ellas para que las representen. ¿Cuántas selecciones se pueden hacer?
Como el orden no importa, la selección se podrá hacer de

$$C_{20}^2 = \frac{20!}{2!(20-2)!} = \frac{20!}{2 \cdot 18!} = \frac{20 \cdot 19}{2} = 10 \cdot 19 = 190 \text{ maneras.}$$

Ejemplo 4.1.16. Se quiere sentar a 10 personas alrededor de una mesa redonda con 10 sillas. ¿De cuántas maneras se les puede sentar teniendo en cuenta el mobiliario que está alrededor?
Colocar a las 10 personas en 10 lugares se puede hacer de $O_{10}^{10} = 10!$ maneras. ¿Y si no importa los objetos que están al rededor?
Esto significa que para cada arreglo, al girarlo se considera el mismo ya que se su posición respecto a su alrededor no importa, entonces por cada arreglo hay 10 que se repiten. Por lo tanto habrá $\frac{O_{10}^{10}}{10!} = \frac{10!}{10} = 9!$ maneras.

Ejemplo 4.1.17. Si se tuvieran 11 bancas en lugar de 10 en el ejemplo 4.1.16, ¿cuántas maneras habrá de sentar a las 10 teniendo en cuenta el mobiliario?
Como sobraría una banca y esta podría ser cualquiera de las 11, entonces para cada banca que escojamos como la banca vacía, tendríamos 10! modos de sentar a las personas. Por lo tanto habrá $11 \cdot 10!$ maneras de sentarlos.

Ejemplo 4.1.18. De un grupo de álgebra de 35 alumnos y un grupo de cálculo de 40 alumnos se quiere escoger un representante de cada grupo. Se sabe que 15 alumnos pertenecen a ambos grupos. Si una persona aparece como representante de álgebra y en otra aparece como representante de cálculo, estas representaciones se considerarán distintas. ¿Cuántas representaciones se pueden escoger?
Denotamos por A al conjunto de alumnos de álgebra y por C al conjunto de alumnos de cálculo. Si A y C fueran ajenos, habría 35×40 maneras de escoger cada pareja de representantes. El caso aquí es que $A \cap C \neq \emptyset$. Del total de parejas posibles que son los elementos de $A \times C$ debemos restar las parejas (a, a) de las cuales hay 15. Entonces habrá $35 \cdot 40 - 15 = 1385$ maneras de escoger a los representantes.

Teorema 4. 1.19*. Si A es un conjunto de cardinalidad finita n, entonces* $card(\mathscr{P}(A)) = 2^n$.

Demostración. Sea $\mathscr{F} = \{f : A \to \{1, -1\} \mid f \text{ es función}\}$. Por el teorema 4.1.8 $card(\mathscr{F}) = 2^n$. Así que para demostrar que $card(\mathscr{P}(A)) = 2^n$ bastará exhibir una función biyectiva de $\mathscr{P}(A)$ en $\mathscr{F}$.
Sea entonces $\phi : \mathscr{P}(A) \to \mathscr{F}$ definida por $\phi(B) = f_B$ donde $f_B : A \to \{-1, 1\}$ está dada por

$$f_B(x) = \begin{cases} 1 & si\ x \in B \\ -1 & si\ x \notin B \end{cases}$$

Veamos que ϕ es biyectiva.

$1/^o$ ϕ es inyectiva. Supongamos $\phi(B) = \phi(C)$, es decir, $f_B = f_C$. Entonces

$$B = \{x \in A \mid f_B(x) = 1\} = \{x \in A \mid f_C(x) = 1\} = C.$$

$2/^o$ ϕ es suprayectiva. Sea $g \in \mathscr{F}$ y sea $B = \{x \in A \mid g(x) = 1\}$. Es claro que $g = f_B$ y por lo tanto $\phi(B) = f_B = g$. ∎

§ 4.2. Teorema del binomio

Veremos aquí algunas propiedades de los números C_n^m y aprovecharemos para verificar que C_n^m es efectivamente un número natural. Para ello recordemos que $C_n^m = \frac{n!}{m!(n-m)!}$.

Teorema 4.2.1. ***(Pascal)*** *Sea* $1 \leq m \leq n-1$. *Entonces* $C_{n-1}^{m-1} + C_{n-1}^m = C_n^m$.

Demostración.

$$\begin{aligned} C_{n-1}^m + C_{n-1}^{m-1} &= \frac{(n-1)!}{m!(n-1-m)!} + \frac{(n-1)!}{(m-1)!(n-1-(m-1))!} = \frac{(n-1)!}{m!(n-m-1)!} + \frac{(n-1)!}{(m-1)!(n-m)!} \\ &= \frac{(n-1)!)(n-m)}{m!(n-m)!} + \frac{(n-1)!m}{m!(n-m)!} = \frac{(n-1)!(n-m)+(n-1)!m}{m!(n-m)!} \\ &= \frac{n!}{m!(n-m)!} = C_n^m \,. \end{aligned}$$ ∎

Teorema 4.2.2. *C_n^m es un número natural.*

Demostración. Por inducción sobre n

(1) $n = 0$. En este caso, la única posibilidad para m es $m = 0$ y así

$$C_0^0 = \frac{0!}{0!0!} = 1 \in \mathbb{N}.$$

(2) Supongamos el resultado cierto para $n - 1 \geq 0$. Entonces $C_{n-1}^m \in \mathbb{N}$ para toda $m \in \mathbb{N}$. Demostraremos que $C_n^m \in \mathbb{N}$. Si $m = n$, entonces $C_m^n = C_n^n = 1 \in \mathbb{N}$, así que podemos suponer $m < n$.
Por el teorema 4.2.1, $C_n^m = C_{n-1}^m + C_{n-1}^{m-1}$ y como $C_{n-1}^m, C_{n-1}^{m-1} \in \mathbb{N}$ por hipótesis de inducción, entonces $C_n^m \in \mathbb{N}$. ∎

A los coeficientes del desarrollo del binomio $(a+b)^n$ se les llama ***coeficientes binomiales*** debido al siguiente:

Teorema 4.2.3. ***(del Binomio)*** *Para todo $n \in \mathbb{N}$ y cualesquiera números reales a, b, se tiene que*

$$(a+b)^n = \sum_{i=0}^{n} C_n^i a^{n-i} \cdot b^i.$$

Demostración. Por inducción sobre n.

(1) $n = 0$, $(a+b)^0 = 1$ y $\sum_{i=0}^{0} C_0^i a^{n-i} \cdot b^i = C_0^0 a^0 \cdot b^0 = 1$ y por lo tanto $(a+b)^0 = \sum_{i=0}^{0} C_0^i a^{0-i} \cdot b^i$.

(2) Supongamos cierto el teorema para $n-1$, es decir,

$$(a+b)^{n-1} = \sum_{i=0}^{n-1} C_{n-1}^i a^{n-1-i} \cdot b^i.$$

$$\begin{aligned}
(a+b)^n &= (a+b)(a+b)^{n-1} \\
&= (a+b) \sum_{i=0}^{n-1} C_{n-1}^i a^{n-1-i} \cdot b^i \\
&= a \sum_{i=0}^{n-1} C_{n-1}^i a^{n-1-i} \cdot b^i + b \sum_{i=0}^{n-1} C_{n-1}^i a^{n-1-i} \cdot b^i \\
&= \sum_{i=0}^{n-1} C_{n-1}^i a^{n-i} \cdot b^i + \sum_{i=0}^{n-1} C_{n-1}^i a^{n-1-i} \cdot b^{i+1}.
\end{aligned}$$

Como $C_{n-1}^n = 0$, entonces $\sum_{i=0}^{n-1} C_{n-1}^i a^{n-i} \cdot b^i = \sum_{i=0}^{n} C_{n-1}^i a^{n-i} \cdot b^i$. Por otro lado,

$$\sum_{i=0}^{n-1} C_{n-1}^i a^{n-1-i} \cdot b^{i+1} = \sum_{i=1}^{n} C_{n-1}^{i-1} a^{n-i} \cdot b^i = \sum_{i=0}^{n} C_{n-1}^{i-1} a^{n-i} \cdot b^i,$$

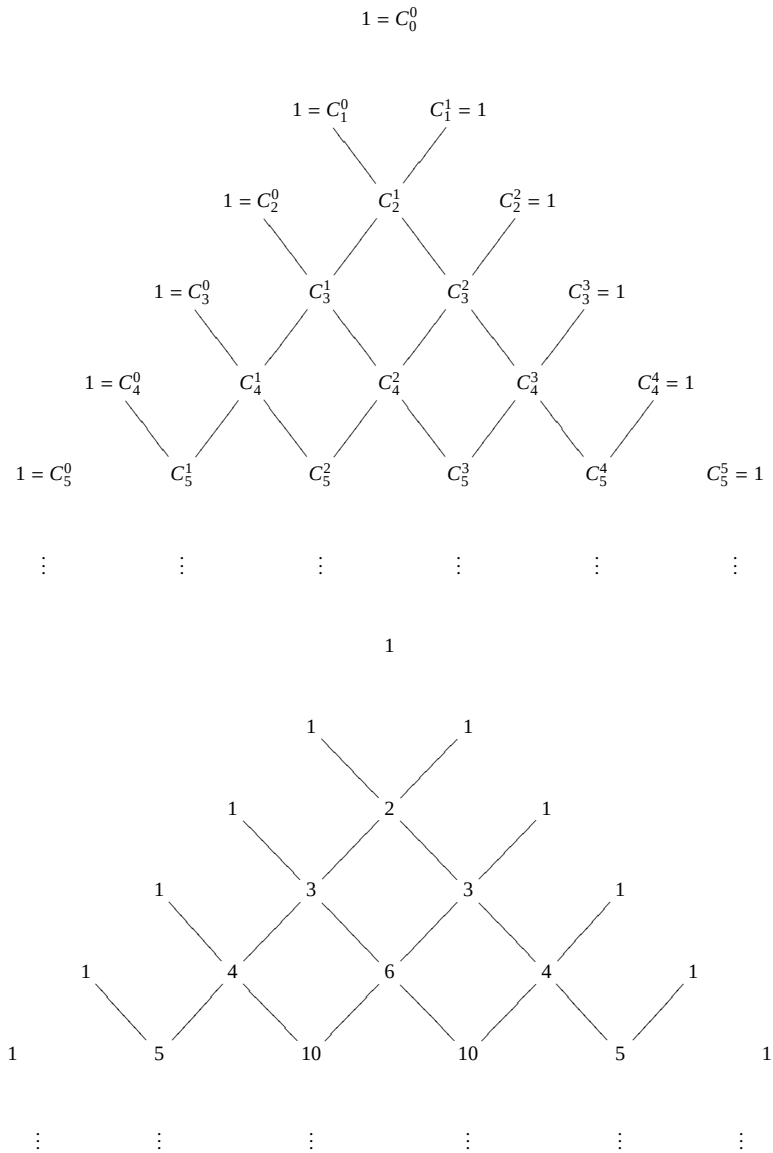
donde definimos $C_{n-1}^{-1} = 0$. Entonces

$$\begin{aligned}
(a+b)^n &= \sum_{i=0}^{n-1} C_{n-1}^i a^{n-i} \cdot b^i + \sum_{i=0}^{n-1} C_{n-1}^{i-1} a^{n-i} \cdot b^i. \\
&= \sum_{i=0}^{n} \left(C_{n-1}^i + C_{n-1}^{i-1} \right) a^{n-i} \cdot b^i.
\end{aligned}$$

Por el teorema 4.2.1, $C_{n-1}^i + C_{n-1}^{i-1} = C_n^i$ y por lo tanto

$$(a+b)^n = \sum_{i=0}^{n} C_n^i a^{n-i} \cdot b^i. \blacksquare$$

Al siguiente diagrama se le conoce como triángulo de Pascal y en él aparecen, en el renglón $n + 1$, los coeficientes binomiales del desarrollo del binomio $(a + b)^n$.



En este triángulo se puede apreciar, aplicando el Teorema de Pascal, que a partir del tercer renglón, cada número, que no está en ninguna de las dos orillas, es suma de los dos que están a su izquierda y a su derecha en el renglón anterior.

§ § Ejercicios sección 4.1.

4.1.1. [5] Muestre que la función F definida en la demostración del lema 4.1.7 es biyectiva.

4.1.2. Suponga que en un librero hay 5 textos de álgebra, 3 de geometría, 6 de cálculo y 4 de estadística. Encuentre el número n de formas en que un estudiante puede escoger:

(1) uno de los libros;
(2) un libro de cada tema.

Respuesta: 18, 360.

4.1.3. Entre A y B hay cuatro líneas de autobuses, y entre B y C tres líneas de autobuses. Encuentre el número n de formas en que una persona puede viajar en autobús:

(1) de A a C pasando por B;
(2) en viaje redondo de A a C pasando por B;
(3) en viaje redondo de A a C pasando por B pero sin usar una linea de autobús más de una vez.

Respuesta: 12, 144, 72.

4.1.4. Las placas de coche en nuestro país constan de tres números y tres letras. ¿Cuántas placas se pueden hacer con estas condiciones?

Respuesta: 19683000.

4.1.5. Dados los dígitos 0, 1, 2, 3 y 4.

(1) ¿Cuantos números naturales de tres cifras distintas pueden formarse con ellos?.
(2) Es claro que el menor de estos números es 102 y el mayor 432 ¿qué lugar ocupa el número 324?.

Respuesta: 48, ocupa el lugar 33.

[5] Parte del teorema 4.1.7 pág. 174.

4.1.6. ¿Cuántos números naturales, incluido el cero, hay que sean menores que 1000, si cada número está constituido por cifras diferentes?

Respuesta: 739.

4.1.7. En un juego de lotería, una apuesta consiste en elegir 6 números comprendidos entre 1 y 49. Se realiza el sorteo extrayendo 6 de los 49 números que forman la denominada combinación ganadora (C.G.); se extrae también un séptimo número, llamado el número adicional.

(1) ¿Cuántas posibles apuestas hay?
(2) ¿Cuántas maneras hay de acertar los seis números de la combinación ganadora?
(3) ¿Y de acertar cinco números de la C.G. y el adicional?
(4) ¿Y de acertar sólo cinco números de la C.G., sin el adicional?
(5) ¿Y de acertar sólo cuatro números de la C.G.?
(6) ¿Y de acertar sólo un número de la C.G.?
(7) ¿Y de no acertar ningún números de la C.G.?

Respuesta: 13983816, 1, 6, 252, 54180, 5775588, 6577753.

4.1.8. En un lugar donde venden hamburguesas se advierte al cliente que su hamburguesa puede ir con todo lo siguiente o sin ello: salsa de tomate, mostaza, mayonesa, lechuga, tomate, cebolla, pepinillos, queso o setas. ¿Cuántos tipos diferentes de hamburguesas son posibles?

Respuesta: 2^9.

4.1.9. Supongamos que cada persona tiene tres iniciales en un alfabeto de 26 letras. ¿Cuántos habitantes debe tener una población como mínimo para que sea posible afirmar que hay dos habitantes con las iniciales repetidas?

Respuesta: 17577.

4.1.10. Un anagrama es una palabra que resulta de escribir las letras de otra palabra en otro orden. No hace falta que tenga un significado, es decir, que un anagrama podría no estar en el diccionario.
¿Cuántos anagramas tiene la palabra

(1) MÉXICO;
(2) ANAGRAMA;
(3) CUERNAVACA;

(4) MATEMÁTICA;
(5) ÁLGEBRA;
(6) PARÁBOLA;
(7) PARANGARICUTIRIMÍCUARO?

Respuesta: 720, 1680, 302400, 151200, 2520, 6720, $\frac{22!}{4!4!4!2!2!}$.

4.1.11.

(1) ¿Cuántos anagramas tiene la palabra MOCOSO, donde las tres O no estén juntas?
(2) ¿Cuántos anagramas tiene la palabra TRABAJAN, donde las tres *A* estén juntas?
(3) ¿Cuántos anagramas tiene la palabra AYUNTAMIENTO, en las que siempre se comience y termine por una vocal?
(4) ¿Cuántos anagramas tiene la palabra CERÁMICA, donde no haya dos vocales juntas?
(5) ¿Cuántos anagramas tiene la palabra PAISANO, en las que no se cambie el orden de las vocales?
(6) ¿Cuántos anagramas tiene la palabra LECTURA, en las que tanto las vocales como las consonantes estén en orden alfabético?
(7) ¿Cuántos anagramas tiene la palabra ESPIRALES, donde se alternen las vocales y las consonantes?

Respuesta: 96, 720, 13608000, 720, 210, 35, 720.

4.1.12. Un palíndromo es una palabra que no se altera al invertir el orden de sus letras (por ejemplo la palabra *RECONOCER*)

(1) Si una letra puede aparecer más de dos veces, ¿cuántos palíndromos de cinco letras hay? ¿Y de seis letras?
(2) Repítase el inciso anterior con la condición de que ninguna letra aparezca más de dos veces.

Respuesta: 26^3 (para cinco o seis letras), 15600.

4.1.13. Con n vocales diferentes y m consonantes diferentes, ¿Cuántas palabras de longitud k, sin dos vocales o dos consonantes consecutivas, se pueden formar?

Respuesta: Si k es par: $2 \cdot \left(\frac{n!}{(n-\frac{k}{2})!} \right)^2$; y si k es impar: $2 \cdot \frac{n!}{(\frac{k+3}{2})!} \frac{n!}{(\frac{k+1}{2})!}$.

4.1.14. En un librero hay $m + n$ libros diferentes, de los cuales m son de color negro, y n son rojos. ¿Cuántos arreglos existen de estos libros, en los que los libros negros ocupen los primeros m lugares? ¿Cuantas posiciones hay, en las que todos los libros negros se hallen juntos?

Respuesta: $m!n!$, $m!(n + 1)!$.

4.1.15. Se tiene un librero con k niveles, cada uno con un libro de álgebra, otro de biología y otro de cálculo. Si se escogió un libro por cada nivel del librero, ¿de cuántas maneras se pueden escoger n libros de álgebra, m libros de biología, y el resto de cálculo?

Respuesta: $\frac{k!}{n!m!(k-n-m)!}$.

4.1.16. Una persona tiene 7 libros de matemáticas, y otra, 9. ¿De cuántos modos pueden cambiar un libro de uno por uno del otro? ¿Y se si se intercambian dos libros de uno por dos del otro?

Respuesta: 63, 756.

4.1.17.

(1) En una reunión deben intervenir 5 personas: A, B, C, D y E. ¿De cuántas maneras se pueden distribuir en la lista de oradores, con la condición de que B no debe intervenir inmediatamente antes que A?
(2) El mismo problema, pero con la condición de que A deba intervenir inmediatamente antes que B.

Respuesta: 60, 24.

4.1.18. En los incisos siguientes se supone que hay 20 pelotas: 6 rojas, 6 azules y 8 verdes.

(1) ¿De cuántas maneras se pueden escoger cinco pelotas si todas las pelotas se consideran distintas? (por ejemplo si estuvieran numeradas del 1 al 20)
(2) ¿De cuántas maneras se pueden escoger cinco pelotas si las del mismo color se consideran idénticas?
(3) ¿De cuántas maneras se pueden escoger dos rojas, tres azules y dos verdes, si las pelotas del mismo color son idénticas? (por ejemplo las rojas están numeradas del 1 al 16, las azules lo mismo y las verdes del 1 al 8)

4.1.19. ¿De cuántas maneras pueden formar una fila cinco personas? ¿De cuantas formas si dos de las personas se niegan a hacerlo una detrás de otra?

Respuesta: 120, 72.

4.1.20. Un autobús, en el que se encuentran n pasajeros debe efectuar m paradas. ¿De cuántos modos pueden distribuirse los pasajeros entre estas paradas?. El mismo problema, si se tiene en cuenta sólo la cantidad de pasajeros que se bajaron en una parada prefijada?

Respuesta: m^n, C_{m-1}^{m+n-1}

4.1.21.

(1) ¿De cuántas maneras pueden colocarse siete personas alrededor de una mesa circular?
(2) ¿Cuantas formas son posibles si dos personas insisten en sentarse juntas?

Respuesta: 720, 240.

4.1.22. ¿De cuántas maneras se pueden sentar alrededor de una mesa redonda a 5 hombres y 5 mujeres de modo que no haya juntas dos personas de un mismo sexo?

Respuesta: 28800.

4.1.23. ¿De cuántas maneras se pueden sentar alrededor de una mesa redonda a 7 hombres y 7 mujeres de modo que no haya juntas dos mujeres juntas?

Respuesta: 50803200.

4.1.24. ¿Cuántas colecciones distintas de 5 jóvenes se pueden formar de un grupo de 10 niños y 15 niñas que

(1) tenga exactamente 2 niñas;
(2) que tenga a lo más 2 niñas?

Respuesta: 12600, 16002.

4.1.25. Un grupo de 15 personas quiere dividirse en 3 equipos de 5 personas cada uno.

(1) Si cada uno tendrá una labor específica distinta a la demás, ¿de cuántas formas distintas es posible hacer la distribución?
(2) Si todos los equipos tendrán la misma labor, ¿de cuántas formas distintas es posible hacer la distribución?

Respuesta: 756756, 126126.

4.1.26. Se va a elegir un comité de 12 personas de un grupo de diez hombres y diez mujeres. ¿De cuántas formas se puede elegir éste:

(1) si no hay restricciones;
(2) si debe haber seis hombres y seis mujeres;
(3) si debe haber un número par de mujeres;
(4) si debe haber más mujeres que hombres;
(5) si debe haber ocho hombres como mínimo?

Respuesta: C_{12}^{20}, $C_6^{10} \cdot C_6^{10}$, $\sum_{i=1}^{5} C_{2i}^{10} \cdot C_{12-2i}^{10}$, $\sum_{i=7}^{10} C_i^{10} \cdot C_{12-i}^{10}$, $\sum_{i=8}^{10} C_i^{10} \cdot C_{12-i}^{10}$.

4.1.27. En un examen de 20 preguntas con dos opciones, ¿de cuántas formas pueden marcarse las preguntas para que

(1) 7 estén correctas y 13 equivocadas;
(2) 10 estén correctas y 10 equivocadas;
(3) cuando menos 17 están correctas?

Respuesta: 77520, 184756, 1351.

4.1.28. Un entrenador debe escoger a 11 alumnos del último curso para jugar en un equipo de fútbol. Si puede hacer su elección de 12376 formas, ¿cuántos alumnos del último curso se pueden elegir?

Respuesta: 17.

4.1.29. ¿Cuántos arreglos distintos pueden efectuarse con n elementos, en la que dos de ellos, a y b no estén juntos? ¿Y en las que no lo estén tres, a, b, c (en cualquier orden)?

Respuesta: $n! - 2(n-1)!$, $n! - 6(n-2)!$.

4.1.30. Un coro está formado por 10 participantes. ¿De cuántos modos se puede escoger 6 participantes durante tres días, de forma que cada día el coro tenga distinta composición?

Respuesta: 9129120.

4.1.31. Un grupo formado por 10 parejas de casados se divide en 5 grupos de a 4 personas para un paseo en bote.

(1) ¿De cuántas formas se las puede dividir de manera que en cada bote haya dos hombres y dos mujeres?
(2) ¿En cuántos casos un hombre dado quedará en el mismo bote que su esposa?

(3) ¿En cuántos casos dos hombres dados quedarán en un sólo bote junto con sus mujeres?

Respuesta: $\frac{(10!)^2}{5!\cdot 2^{10}}$, $\frac{(9!)^2}{4!\cdot 2^8}$, $17\cdot\frac{(8!)^2}{4!\cdot 2^8}$.

La baraja inglesa consta de 52 cartas. Cada carta tiene un símbolo llamado **número** que puede ser cualquiera de los 13 símbolos siguientes: *A*, 2, 3, 4, 5, 6, 7, 8, 9, 10, *J*, *Q* o *K*, y otro símbolo llamado **palo** que puede ser cualquiera de los 4 siguientes: ♠ (espada), ♡ (corazón), ♢ diamante o ♣ (trébol). Las espadas y tréboles en color negro y los corazones y diamantes en color rojo.

4.1.32. ¿De cuántas maneras se puede escoger, de una baraja completa, una carta de cada palo? Lo mismo, pero con la condición de que entre las cartas escogidas no haya ningún par igual, es decir, dos reyes, dos diez, etc.

Respuesta: 28561, 17160.

4.1.33. ¿De cuántas maneras se puede escoger, de una baraja completa, una carta de cada palo de forma que las de palos rojos y las de palos negros formen parejas (por ejemplo, los nueves de espadas y de tréboles y los reyes de diamantes y de corazones)?

Respuesta: 169.

4. 1.34. De una baraja que contiene 52 cartas se han extraído 10. ¿En cuántos casos entre ellas habrá por lo menos un as? ¿En cuántos habrá exactamente un as? ¿En cuántos habrá no menos de dos ases? ¿Y exactamente dos ases?

Respuesta: $C_{10}^{52}-C_{10}^{48}$, $4C_9^{48}$, $C_{10}^{52}-C_{10}^{48}-4C_9^{48}$, $C_2^4C_8^{48}$.

4. 1.35. ¿De cuántas formas se pueden escoger 6 cartas de una baraja de 52, de manera que entre ellas haya de cada uno de los cuatro palos?

Respuesta: $304\cdot 13^4$.

4.1.36. Se llama mano de pókar cualquier colección de 5 cartas de la baraja. La siguiente nomenclatura es usual:
Par: dos cartas del mismo número.
Tercia: tres cartas del mismo número.
Pókar: cuatro cartas del mismo número.
Full: una tercia y un par.
Flor: cinco cartas del mismo palo.

Corrida: cinco cartas con numeración consecutiva (según el orden en que se escribieron arriba, pero permitiendo *A* también como número final, enseguida de *K*).
Flor imperial: que sea flor y corrida.

(1) ¿Cuántas manos de pókar hay?
(2) ¿Cuántas manos de pókar hay que no tengan un par?
(3) ¿Cuántas manos de pókar tienen por lo menos un par?
(4) ¿Cuántas manos de pókar tienen exactamente un par?
(5) ¿Cuántas manos de pókar tienen tercia exactamente (es decir, que no sea full ni pókar)?
(6) ¿Cuántas manos de pókar tienen dos pares (distintos) exactamente?
(7) ¿Cuántas manos de pókar tienen full?
(8) ¿Cuántas manos de pókar hay que tengan pókar?
(9) ¿Cuántas manos de pókar hay que tengan flor?
(10) ¿Cuántas manos de pókar tienen corrida?
(11) ¿Cuántas manos de pókar hay que sean flor imperial?
(12) ¿Cuántas manos de pókar hay con sólo cartas rojas?
(13) ¿Cuántas manos de pókar hay con tres cartas rojas y dos negras?
(14) ¿Cuántas manos de pókar hay que tengan algún joto, J, alguna kuina, Q y algún rey, K?

Respuesta: 2598960, 1317888, 1281072, 68640, 54912, 123552, 3744, 624, 5148, 10240, 40.

4. 1.37. En el juego de pókar de 7 se juegan con las cartas 8, 9, 10, *J*, *Q*, *K*, *A* pertenecientes a cuatro palos diferentes. Cada jugador recibe cinco cartas.

(1) ¿De cuántas maneras puede recibir cartas un jugador?
(2) ¿Cuántas de ellas son escalera (cinco cartas consecutivas o *A*, 8, 9, 10, *J*)?
(3) ¿Cuántas de ellas son color (cinco cartas del mismo palo que no forman escalera)?
(4) ¿Cuántas de ellas son full (tres cartas del mismo símbolo y dos con otro mismo símbolo, distinto del anterior)?

Respuesta: 98280, 4096, 68, 1008.

4. 1.38. El siguiente problema se refiere al conjunto usual de 28 fichas de dominó en que cada ficha muestra dos números de la colección 0, 1, 2, 3, 4, 5 y 6 (posiblemente repetidos). Una mano consta de 7 fichas.

(1) ¿Cuántas manos distintas de dominó hay?
(2) ¿Cuántas manos distintas hay en las que aparezcan 2 mulas? (Una mula es una ficha doble)
(3) ¿Cuántas manos distintas hay en las que aparezcan 4 fichas con el mismo número? (los números van del 0 al 6)
(4) ¿Cuántas manos distintas hay en las que aparezcan 2 mulas y 4 de las fichas tengan un mismo número?

4.1.39. Si queremos hacer un juego de dominó que vaya de 0 a n, Cuántas fichas tendrá?

Respuesta: $\frac{(n+2)\cdot(n+1)}{2}$.

4.1.40. ¿De cuántas formas se pueden escoger en el tablero de ajedrez dos casillas, una blanca y una negra? ¿Y si no hay limitaciones en lo que respecta al color de las casillas escogidas?

Respuesta: 1024, 4032.

4.1.41. ¿De cuántas formas se pueden escoger en el tablero de ajedrez una casilla blanca y una negra que no estén en una misma horizontal ni vertical?

Respuesta: 768.

4.1.42. ¿De cuántas formas se pueden colocar 12 fichas blancas y 12 negras en las casillas negras de un tablero de ajedrez?

Respuesta: $C_{12}^{32} \cdot C_{12}^{20}$.

4.1.43. Considere un polígono regular de n lados. ¿Cuántas diagonales se pueden trazar en este polígono?

Respuesta: $C_2^n - n$.

4.1.44. Si disponemos de 5 puntos no colineales, ¿cuál es el máximo número de triángulos que se podrán formar?

Respuesta: 10.

4.1.45. ¿Cuántos triángulos determinan los vértices de un polígono regular de n lados? ¿Cuántos, si ningún lado del polígono se usa como lado del triángulo?

Respuesta: C_3^n, $C_3^n - n(n-4) - n$ para $n \geq 4$.

4. 1.46. Dé un argumento combinatorio para mostrar que si n y k son enteros positivos con $n = 3k$, entonces $\frac{n!}{(3!)^k}$ es un entero.

4.1.47. Demuestre que $C_n^0 + C_n^1 + \cdots + C_n^n = 2^n$.

4. 1.48. Dé un argumento combinatorio para mostrar que si n y k son enteros positivos con $n = 3k$, entonces $\frac{n!}{(3!)^k}$ es un entero.

4.1.49. De cuántas formas es posible distribuir 10 monedas (idénticas) entre cinco niños si

(1) no hay restricciones;
(2) cada niño recibe al menos una moneda;
(3) el niño mayor recibe al menos dos monedas.

Respuesta: C_{14}^{10}, C_9^5, C_{12}^8.

4.1.50. Por un cierto canal de comunicación se va a transmitir un mensaje usando 12 símbolos. Además de los 12 símbolos, el transmisor enviará un total de 45 espacios en blanco entre los símbolos con tres espacios como mínimo entre cada par de símbolos consecutivos. ¿De cuántas maneras se puede mandar el mensaje?

Respuesta: $(12!)C_{22}^{12}$.

4.1.51. Determine el número de soluciones enteras de la ecuación

$$x_1 + x_2 + x_3 + x_4 = 7, \qquad \text{donde } x_i \geq 0, \text{ para toda } 1 \leq i \leq 4$$

Respuesta: 120.

4. 1.52. ¿De cuántas formas puede colocar Juan 24 libros diferentes en cuatro repisas de modo que haya al menos un libro en cada repisa? (Para cualesquiera de estas disposiciones, considere que en cada repisa los libros deben ser colocados uno junto al otro , y el primer libro a la izquierda)

Respuesta: $(24!)C_{23}^{20}$.

4.1.53. ¿De cuántas formas puede colocar 12 canicas del mismo tamaño en cinco recipientes distintos si

(1) todas las canicas son negras;
(2) cada canica es de distinto color?

Respuesta: C_{16}^{12}, 5^{12}.

4.1.54. En su tienda de flores, Margarita desea colocar 15 plantas diferentes en cinco anaqueles del escaparate. ¿De cuántas formas puede colocarlas de tal manera que cada anaquel tenga al menos una planta, pero no mas de cuatro?

Respuesta: $(15!)\left[C_{14}^{10} - C_5^1 C_{10}^6 + C_5^2 C_6^2\right]$.

4.1.55. El profesor Ballesteros acaba de escribir el examen final para un curso de matemáticas avanzadas. Este examen tiene 12 preguntas que en total valen 200 puntos. ¿De cuántas maneras puede asignar el profesor Ballesteros los 200 puntos si

(1) cada pregunta debe valer al menos 10 puntos, pero no mas de 25 puntos;
(2) cada pregunta debe valer al menos 10 puntos, pero no mas de 25 puntos y el valor de los puntos para cada pregunta debe ser múltiplo de 5?

§§ Ejercicios sección 4.2.

4.2.1. Utilizar el Teorema del Binomio y el Triángulo de Pascal para desarrollar la expresión:

(1) $(2x - 5y)^4$
(2) $(2a - 3b^2)^8$
(3) $(a + 2b - \frac{c}{2})^4$
(4) $(x + y)^6 + (x - y)^6$

4.2.2. Encontrar el término que no contiene a x en el desarrollo de

(1) $\left(x^5 + \frac{2}{x}\right)^5$;
(2) $\left(x - \frac{1}{x^3}\right)^{2n}$;
(3) $(x^{55} + 2)\left(x - \frac{1}{x^4}\right)^{105}$;
(4) $\left(\sqrt{x} + \frac{1}{\sqrt[4]{x}}\right)^9$.

4.2.3. Utilizar el teorema del binomio y el triángulo de Pascal para desarrollar la expresión:

(1) $(2x - 5y)^4$
(2) $(2x - y)^5$
(3) $\left(2a - 3b^2\right)^7$
(4) $\left(2a^4 + 6b^3\right)^6$
(5) $(x + y)^6 + (x - y)^6$

(6) $\left(x+2y-\frac{z}{2}\right)^4$

4.2.4. Determínese la suma de todos los coeficientes de

(1) $(x+y)^3$.
(2) $(x+y)^{10}$.
(3) $(x+y+z)^3$.
(4) $(w+x+y+z)^5$.

4.2.5. Resolver las ecuaciones:

(1) $C_7^x = C_7^{x+3}$;
(2) $3 \cdot C_x^4 = 5 \cdot C_x^2$.

4.2.6. El segundo, tercer y cuarto término en el desarrollo de $(x+y)^n$ son 240, 720 y 1080 respectivamente. Encuentre los valores de x, y, n.

4.2.7. En el desarrollo de $\left(1+\frac{x}{a}\right)^n$, los tres primeros términos son $1+30x+360x^2$. Encuentre los valores de a y n.

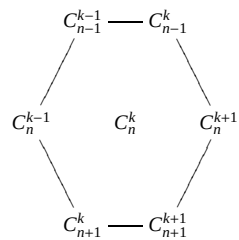
4.2.8. En el desarrollo de $\left(x^4+\frac{1}{3}y^2\right)^n$, en el noveno término aparece $x^{32}y^{18}$. Encontrar el valor de n y el coeficiente correspondiente al noveno término.

4.2.9. En el desarrollo binomial $\left(\frac{x}{a}-y^2\right)^{15}$, el coeficiente de y^{22} es $-\frac{455}{27}$. Encuentre el valor de a.

4.2.10. Muestre que:

(1) $C_n^k = C_n^{n-k}$.
(2) Si $k \neq 0$, entonces $C_r^k = \frac{r}{k} \cdot C_{r-1}^{k-1}$.
(3) Si $k < r$, entonces $C_r^k = \frac{r}{r-k} \cdot C_r^{k-1}$.
(4) $C_r^m \cdot C_m^k = C_r^k \cdot C_{r-k}^{m-k}$.

4.2.11. Para $n, k \in \mathbb{N} - \{0\}$, con $n \geq k+1$, consideremos C_n^k. Fijémonos en el hexágono que se forma a su alrededor, éste tiene la forma



Demuestre la propiedad del hexágono $C_{n-1}^{k-1} \cdot C_n^{k+1} \cdot C_{n+1}^k = C_{n-1}^k \cdot C_{n+1}^{k+1} \cdot C_n^{k-1}$.

4.2.12. Muestre,

$$\frac{1}{n+1} \cdot C_{2n}^n = C_{2n-1}^{n-1} - C_{n+1}^{2n-1} = C_n^{2n} - C_{n-1}^{2n}.$$

4. 2.13. Demuestre que la suma de todos los números situados por encima del n-ésimo renglón del triángulo de Pascal es igual a $2^n - 1$.

4.2.14. Dé un argumento combinatorio para mostrar que para los enteros n, r con $n \geq r \geq 2$,

$$C_{n+2}^r = C_n^r + 2 \cdot C_n^{r-1} + C_n^{r-2}.$$

4.2.15. Demuestre que

$$C_{n+1}^{k+1} = C_n^k + C_{n-1}^k + C_{n-2}^k + \cdots + C_k^k.$$

4.2.16. Utilizar el Teorema del Binomio para probar la fórmula

$$C_n^0 + C_n^2 + C_n^4 + \cdots = C_n^1 + C_n^3 + C_n^5 + \cdots .$$

¿Qué interpretación se puede dar a esta fórmula en términos de subconjuntos de un conjunto?

4.2.17. Utilizando el teorema del binomio calcule las siguientes sumas:

(1) $C_n^0 + C_n^1 + C_n^2 + \cdots + C_n^n$;
(2) $C_n^0 - C_n^1 + C_n^2 + \cdots + (-1)^n C_n^n$;
(3) $C_n^0 + 2 \cdot C_n^1 + 2^2 \cdot C_n^2 + \cdots + 2^n \cdot C_n^n$;
(4) $C_n^0 + 2 \cdot C_n^1 + 3 \cdot C_n^2 + \cdots + n \cdot C_n^n$ $(n \geq 1)$;
(5) $C_n^0 - 2 \cdot C_n^1 + 3 \cdot C_n^2 - \cdots + (-1)^{n-1} n \cdot C_n^n$ $(n \geq 1)$;
(6) $C_n^0 - C_n^1 + C_n^2 - \cdots + (-1)^m \cdot C_n^m$ $(m \leq n)$;
(7) $C_n^k + C_{n+1}^k + C_{n+2}^k + \cdots + C_{n+m}^k$ $(k \leq m)$;

4.2.18. Probar que para cualquier número natural se tiene la fórmula

$$\left(C_n^0\right)^2 + \left(C_n^1\right)^2 + \left(C_n^2\right)^2 + \cdots + \left(C_n^n\right)^2 = C_{2n}^n.$$

Sugerencia: Examinar el coeficiente de x^n al desarrollar ambos miembros de la igualdad $(1 + x)^{2n} = (1 + x)^n (1 + x)^n$.

4.2.19. Demostrar que si m, n y k son números naturales tales que $k < n$ y $k < m$, se cumple:

$$C_{n+m}^{k} = \sum_{j=0}^{k} C_{m}^{j} \cdot C_{n}^{k-j}$$

Sugerencia: Examinar $(x+y)^{n+m} = (x+y)^{n}(x+y)^{m}$.

4.2.20. Haga el diagrama del triángulo de Pascal hasta su décimo renglón.

4.2.21. Demostrar que, en cada uno de los renglones del triángulo de Pascal, el número mayor es el central (o los dos centrales), es decir, que

$$C_{r}^{n} > C_{r-1}^{n} \qquad \text{si} \quad r < \frac{1}{2}(n+1).$$

Toda la evolución de la que sabemos procede de lo vago a lo definido.
Guisepe Peano
1839 - 1914

Capítulo **5**

Sistema de los números naturales

En el capítulo 2 presentamos los números naturales con las dos operaciones binarias, suma y producto, con sus respectivas propiedades. También introdujimos una relación de orden con la poderosa propiedad de ser buen orden y ahí mismo vimos que es equivalente al principio de inducción completa.
La información que hemos supuesto como conocida puede reducirse, ya que ciertas propiedades se pueden concluir de otras, es decir, con menos información de partida podríamos haber establecido el resto. Por ejemplo, el producto se puede definir a través de la suma si ésta se conoce. Así pues, la pregunta que nos podríamos hacer es ¿cuál es la mínima información que se debe tener de $\mathbb{N}$ para, a partir de ahí, desarrollar lo ya conocido?
Giuseppi Peano (1853 –1932) en 1889 estableció esta mínima estructura que se conoce como Sistema de Peano y a partir de ella definió la suma y el producto que tienen las propiedades que conocemos.
Los conceptos relevantes en estos axiomas son, la existencia en $\mathbb{N}$ de un elemento distinguido que es el 0, una función $s : \mathbb{N} \longrightarrow \mathbb{N}$ que corresponde intuitivamente a la función sucesor (página 135) y el Principio de Inducción.
Basados en estos tres conceptos, definiremos en general un Sistema de Peano, introduciremos una suma, un producto y demostraremos sus respectivas propiedades. Es importante mencionar que para definir estas operaciones utilizaremos el llamado Teorema de Recursión (teorema 5.1.6) el cual resulta fundamental. Probaremos además que dos sistemas de Peano, salvo por la naturaleza de su elementos,

se pueden ver como el mismo sistema en un sentido que definiremos más adelante. Por último, construiremos un conjunto que satisfará estos axiomas, mostrando con esto que efectivamente existe un modelo de los números naturales.

§ 5.1. Sistemas de Peano

Definición 5.1.1. *Un* **Sistema de Peano** *es una terna* $\mathbf{(N, n_0, s)}$*, donde* N *es un conjunto,* $n_0 \in N$ *y* $s : N \longrightarrow N$ *es una función tal que*

(1) $n_0 \notin Im(s)$*;*
(2) s *es inyectiva;*
(3) Para cada $T \subseteq N$*, si*
  (i) $n_0 \in T$*,*
  (ii) *Para toda* $n \in N$*,* $n \in T$ *implica* $s(n) \in T$

Entonces $T = N$.

Nota 5.1.2. LLamaremos a N el ***conjunto soporte*** y a n_0 el ***elemento distinguido*** de N.

Las siguientes dos proposiciones son consecuencia inmediata de la definición de un Sistema de Peano.

Proposición 5.1.3. *Si* (N, n_0, s) *es un Sistema de Peano, entonces*

$$Im(s) = N - \{n_0\}.$$

Demostración. Demostraremos que $N = Im(s) \cup \{n_0\}$ y para hacerlo mostraremos que $Im(s) \cup \{n_0\} \subseteq N$ satisface las hipótesis de la condición (3) de la definición de Sistema de Peano
$1^\circ /$ $n_0 \in Im(s) \cup \{n_0\}$ es evidente.
$2^\circ /$ Sea $n \in N$ y supongamos que $n \in Im(s) \cup \{n_0\}$. Entonces $s(n) \in Im(s) \cup \{n_0\}$. Por que $Im(s) \cup \{n_0\} = N$. Y como $n_0 \notin Im(s)$, entonces $Im(s) = N - \{n_0\}$. ∎

Proposición 5.1.4. *Si* (N, n_0, s) *es un Sistema de Peano, entonces* N *es infinito.*

Demostración. Basta demostrar que existe una función biyectiva de N en un subconjunto propio de N. Esta función está dada precisamente por s, ya que es inyectiva y por la proposición 5.1.3 $Im(s) = \mathbb{N} - \{n_0\}$. Por último como $N - \{n_0\} \subsetneq N$, N debe ser infinito. ∎

Definiremos ahora cuándo dos Sistemas de Peano son *isomorfos* y ahí se puede ver por qué se pueden considerar como lo mismo, estructuralmente hablando.

Definición 5.1.5. *Se dirá que dos Sistemas de Peano* (N, n_0, s) *y* (N', n_0', s') *son* **isomorfos***, si existe una función biyectiva* $\psi : N \longrightarrow N'$ *tal que* $\psi(n_0) = n_0'$ *y* $\psi(s(n)) = s'(\psi(n))$ *para toda* $n \in N$*. esto es, el siguiente diagrama conmuta, lo que significa que* $\psi \circ s = s' \circ \psi$*.*

$$\begin{array}{ccc} n_0 & & N \xrightarrow{s} N \\ {\scriptstyle\psi}\downarrow & \qquad & {\scriptstyle\psi}\downarrow \quad\quad \downarrow{\scriptstyle\psi} \\ n_0' & & N' \xrightarrow[s']{} N' \end{array}$$

Lo que dice la definición 5.1.5 es que para que dos Sistemas de Peano (N, n_0, s) y (N', n_0', s') sean isomorfos, se debe identificar, mediante una función biyectiva $\psi : N \longrightarrow N'$ a los elementos de N con los elementos de N' de tal manera que el elemento distinguido n_0 de N se identifique con el elemento distinguido n_0' de N', y para cada $n \in N$, el sucesor de n debe aplicarse en el sucesor, de $\psi(n)$ en N'.
Para demostrar que cualesquiera dos Sistemas de Peano son isomorfos necesitamos presentar un muy importante teorema, llamado Teorema de Recursión, que nos permitirá definir conceptos en un Sistema de Peano que involucran a cada elemento de éste y que nos asegura que estas definiciones están bien dadas.
Puede ser que en un principio el lector no visualice muy bien lo que este teorema dice, pero afortunadamente daremos varios ejemplos aquí de su utilización y que probablemente disipará el poco entendimiento que al principio se puede tener de este teorema.

Teorema 5.1.6 *(Teorema de Recursión). Sea* (N, n_0, s) *un Sistema de Peano y sean* X *un conjunto,* $x_0 \in X$ *y* $\varphi : X \longrightarrow X$ *una función. Entonces existe una única función* $\psi : N \longrightarrow X$ *tal que* $\psi(n_0) = x_0$ *y* $\psi(s(n)) = \varphi(\psi(n))$ *para toda* $n \in N$*. Esto es, el siguiente diagrama conmuta:*

$$\begin{array}{ccc} n_0 & & N \xrightarrow{s} N \\ \downarrow & \qquad & {\scriptstyle\psi}\downarrow \quad\quad \downarrow{\scriptstyle\psi} \\ x_0 & & X \xrightarrow[\varphi]{} X \end{array} \qquad \varphi \circ \psi = \psi \circ s$$

Demostración. Recordamos que una función de N en X es un conjunto ψ de parejas ordenadas $(n, x) \in N \times X$ tal que $(n, x), (n, x') \in \psi$ implica $x = x'$ y $Dom(\psi) = N$.

Existencia

Sea $\mathcal{U} = \{A \subseteq N \times X \mid (n_0, x_0) \in A \text{ y } (n, x) \in A \Longrightarrow (s(n), \varphi(x)) \in A\}$. Como $\mathcal{U} \neq \emptyset$, ya que $N \times X \in \mathcal{U}$, podemos tomar la intersección de todos los elementos de $\mathcal{U}$.

Afirmamos que $\psi = \bigcap_{A \in \mathcal{U}} A$ es la función buscada.

$1^{\underline{o}}$ $\psi \in \mathcal{U}$

Es inmediato de la definición de ψ.

$2^{\underline{o}}$ $Dom(\psi) = N$

Recordamos que $Dom(\psi) = \{n \in N \mid \text{existe } x \in X \text{ tal que } (n, x) \in \psi\} \subseteq N$. Demostraremos que $Dom(\psi) = N$ aplicando (3) de la definición de Sistema de Peano.

(i) $n_0 \in Dom(\psi)$ ya que $(n_0, x_0) \in A$ para toda $A \in \mathcal{U}$ y así

$$(n_0, x_0) \in \bigcap_{A \in \mathcal{U}} A = \psi.$$

(ii) Supongamos que $n \in Dom(\psi)$. Mostraremos que $s(n) \in Dom(\psi)$.
$n \in Dom(\psi)$ implica que $(n, x) \in \psi$ para alguna $x \in X$, y como $\psi \in \mathcal{U}$, entonces $(s(n), \varphi(x)) \in \psi$. Luego $s(n) \in Dom(\psi)$ y por lo tanto de (i) y (ii), se tiene que $Dom(\psi) = N$.

$3^{\underline{o}}$ ψ es función

Como $Dom(\psi) = N$, probaremos que para cada $n \in N$, existe una única $x \in X$ tal que $(n, x) \in \psi$. Para esto sea

$$S = \{n \in N \mid \text{existe una única } x \in X \text{ tal que } (n, x) \in \psi\}.$$

Como es de esperar demostraremos que $S = N$ aplicando (3) de la definición de Sistema de Peano.

(i) $n_0 \in S$. Sabemos que $(n_0, x_0) \in \psi$, así que supongamos que $(n_0, x_1) \in \psi$ para algún $x_1 \in X$ con $x_0 \neq x_1$ y consideramos el conjunto $A = \psi - \{(n_0, x_1)\}$. Demostraremos que $A \in \mathcal{U}$, lo que nos lleva a un absurdo ya que en este caso se tendría que $A \subsetneq \psi \subseteq A$. $(n_0, x_0) \in A$ ya que $(n_0, x_0) \in \psi$ y $(n_0, x_0) \neq (n_0, x_1)$ y si $(n, x) \in A$, por ser éste elemento de ψ, entonces

$$(s(n), \varphi(x)) \in \psi.$$

Por otro lado, $s(n) \neq n_0$ debido a que, por la proposición 5.1.3, $n_0 \notin Im(s)$ y entonces $(s(n), \varphi(x)) \in \psi - \{(n_0, x_1)\} = A$. Por lo tanto $A \in \mathcal{U}$,

que hemos visto nos lleva a un absurdo. Así que no puede existir $x_1 \in X$, $x_1 \neq x_0$ tal que $(n_0, x_1) \in \psi$, por lo que $n_0 \in S$

(ii) Supongamos que $n \in S$ y sea x el único elemento de X tal que $(n, x) \in \psi$. Entonces $(s(n), \varphi(x)) \in \psi$. Supongamos que $(s(n), y) \in \psi$, con $y \neq \varphi(x)$ y sea $A = \psi - \{(s(n), y)\}$. Probaremos que $A \in \mathcal{U}$.

1º $(n_0, x_0) \in A$ puesto que $(n_0, x_0) \in \psi$ y como $n_0 \neq s(n)$ para toda $n \in N$, se tiene que $(n_0, x_0) \neq (s(n), y)$.

2º Supongamos que $(m, k) \in A$. Para ver que $(s(m), \varphi(k)) \in A$ debemos mostrar que $(s(m), \varphi(k)) \neq (s(n), y)$. Pero si $(s(m), \varphi(k)) = (s(n), y)$, entonces $s(m) = s(n)$ y $\varphi(k) = y$, y por ser s inyectiva, debe ser $m = n$ y así $(m, k) = (n, k) \in A \subseteq \psi$. Sin embargo, por hipótesis de inducción x es el único elemento de X tal que $(n, x) \in \psi$, así que debe ser $k = x$, lo que implica $\varphi(x) = \varphi(k) = y$, esto contradice la hipótesis. Por lo tanto debe suceder que $(s(m), \varphi(k)) \neq (s(n), y)$ y así $(s(m), \varphi(k)) \in A$, que no puede ser, ya que esto implicaría que $A \subsetneq \psi \subseteq A$. Por lo tanto $s(n) \in S$

Entonces $S = N$.
Hemos demostrado que $\psi : N \longrightarrow X$ es una función tal que

$$\psi(s(n)) = \varphi(x) = \varphi(\psi(n)) \text{ y } \psi(n_0) = x_0.$$

Unicidad
Supongamos que existe otra función $\psi' : N \longrightarrow X$ tal que $\psi'(s(n)) = \varphi(\psi'(n))$ y $\psi'(n_0) = x_0$. Demostraremos, por (3) de la definición de Sistema de Peano, que $\psi' = \psi$.

1º $\psi'(n_0) = x_0 = \psi(n_0)$.

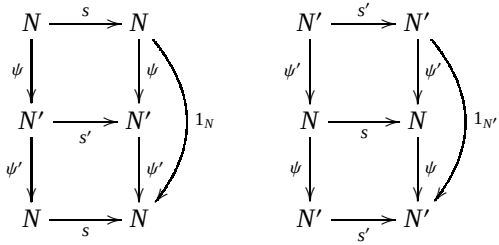
2º Supongamos que $\psi'(n) = \psi(n)$. Demostraremos que $\psi'(s(n)) = \psi(s(n))$.

$$\psi'(s(n)) = \varphi(\psi'(n)) = \varphi(\psi(n)) = \psi(s(n)).$$ ∎

Teorema 5.1.7. *Cualesquiera dos Sistemas de Peano son isomorfos.*

Demostración. Sean (N, n_0, s) y (N', n_0', s') Sistemas de Peano. Por el Teorema de Recursión, existen una función $\psi : N \longrightarrow N'$ tal que $\psi(n_0) = n_0'$ y $\psi(s(n)) =$

$s'(\psi(n))$ y una función $\psi' : N' \longrightarrow N$ tal que $\psi'(n'_0) = n_0$ y $\psi'(s'(n)) = s(\psi'(n))$



La composición $(\psi' \circ \psi) : N \longrightarrow N$ es tal que

$$(\psi' \circ \psi)(n_0) = n_0 \;\; y \;\; (\psi' \circ \psi)(s(n)) = s((\psi' \circ \psi)(n))$$

y como la función identidad, $1_N : \mathbb{N} \to \mathbb{N}$ dada por $1_{\mathbb{N}}(n) = n$, también satisface $1_N(n_0) = n_0$ y que $1_N(s(n)) = s(1_N(n))$, se tiene, por la unicidad dada en el Teorema de Recursión, $\psi' \circ \psi = 1_N$.
De la misma manera se demuestra que $\psi \circ \psi' = 1_{N'}$.
Por lo tanto ψ es biyectiva con $\psi(n_0) = n_0$ y $\psi(s(n)) = s'(\psi(n))$ y además es única con esta propiedad. ∎

Ya que hemos demostrado que existe un único Sistema de Peano, salvo isomorfismo, de aquí en adelante denotaremos por $\mathbb{N}$ al conjunto soporte de un Sistema de Peano, por $\boldsymbol{s}$ a la función dada en el Sistema de Peano y la llamaremos la ***función sucesor***, y al elemento $\boldsymbol{n_0} \in \mathbb{N}$ lo denotaremos por $\mathbf{0}$ y a la propiedad (3) de la definición de Sistema de Peano, la llamaremos Principio de Inducción Completa. Más adelante, cuando definamos la suma, el producto y el orden, se encontrará el sentido de llamar a s la función sucesor. Más concretamente, demostraremos que si $1 = s(0)$, entonces $s(n) = n + 1$, y también demostraremos que para toda $n \in \mathbb{N}$ entre n y $n + 1$ no existe ningún número natural, es decir, dado $n \in \mathbb{N}$, no existe $m \in \mathbb{N}$ tal que $n < m < n + 1$, lo que claramente justifica el hecho de que a $n + 1$ lo llamemos el sucesor de n.
Los ***números naturales*** serán entonces los elementos de cualquier Sistema de Peano, lo que no debe causar ningún conflicto pues, como podrá apreciarse en lo que sigue, no es la naturaleza de los elementos de un Sistema de Peano lo importante, sino las propiedades que se obtienen de él como consecuencia de la definición, de tal manera que las definiciones que daremos de las operaciones y del orden en un Sistema de Peano, dependerán únicamente de las propiedades que definen al Sistema de Peano y no de cómo son sus elementos.

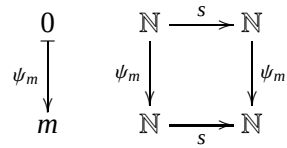
Introducimos la definición de suma en un Sistema de Peano por recursión (esto significa que usamos el Teorema de Recursión) de la siguiente manera:
Dado $m \in \mathbb{N}$

(1) $m + 0 = m$;
(2) $m + s(n) = s(m + n)$ para toda $n \in \mathbb{N}$.

que es una simplificación del siguiente teorema:

Teorema 5.1.8. *Sea* $(\mathbb{N}, 0, s)$ *un Sistema de Peano. Entonces existe una única función* $\psi : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ *tal que para cada* $m \in \mathbb{N}$, $\psi(m, 0) = m$ *y* $\psi(m, s(n)) = s(\psi(m, n))$ *para toda* $n \in \mathbb{N}$.

Demostración.
Existencia: Sea $m \in \mathbb{N}$, m fijo: Tomando $X = \mathbb{N}$, $\varphi = s$ y $x_0 = m$ en el Teorema de Recursión, se tiene que existe una única función $\psi_m : \mathbb{N} \longrightarrow \mathbb{N}$ tal que $\psi_m(0) = m$ y $\psi_m(s(n)) = s(\psi_m(n))$.



Haciendo esto para cada $m \in \mathbb{N}$, podemos definir $\psi : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ por $\psi(m, n) = \psi_m(n)$ y claramente ψ satisface las condiciones del teorema, ya que

$$\psi(m, 0) = \psi_m(0) = m \ \ y \ \ \psi(m, s(n)) = \psi_m(s(n)) = s(\psi_m(n)) = s(\psi(m, n)).$$

Unicidad: Supongamos que $\psi_1 : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ también satisface el teorema. Probaremos que para cada $m, n \in \mathbb{N}$, $\psi_1(m, n) = \psi(m, n)$.
Sea $m \in \mathbb{N}$, m fijo y sea $T = \{n \in \mathbb{N} \mid \psi_1(m, n) = \psi(m, n)\} \subseteq \mathbb{N}$. Probaremos que $T = \mathbb{N}$, usando el Principio de Inducción Completa.

$1^{\underline{o}}$ $0 \in T$, ya que $\psi_1(m, 0) = m = \psi(m, 0)$.

$2^{\underline{o}}$ Supongamos que $n \in T$, es decir, $\psi_1(m, n) = \psi(m, n)$. Como ambas funciones satisfacen el teorema, se tiene que

$$\psi_1(m, s(n)) = s(\psi_1(m, n)) \ y \ \psi(m, s(n)) = s(\psi(m, n))$$

y como, por hipótesis de inducción, $\psi_1(m,n) = \psi(m,n)$, entonces $s(\psi_1(m,n)) = s(\psi(m,n))$, lo que significa que $\psi_1(m,s(n)) = \psi(m,s(n))$ y entonces $s(n) \in T$. Por lo tanto $T = \mathbb{N}$ y así $\psi_1(m,n) = \psi(m,n)$ para toda $n \in \mathbb{N}$. Pero como m es arbitrario, concluimos entonces que $\psi_1 = \psi$. ∎

Notación 5.1.9. *$\psi(m,n) =$* ***$m + n$*** *y la llamaremos* ***la suma de m y n.***

Con esta notación la suma satisface que $m + 0 = m$ para toda $m \in \mathbb{N}$ y que $m + s(n) = s(m + n)$ para todas $m, n \in \mathbb{N}$.

Notación 5.1.10. *Denotamos por* **1** *al sucesor de* 0*, es decir,* $s(0) = 1$*. No hay ningún conflicto en cuanto a esto ya que* $s(0)$ *hace justamente el papel del* 1 *conocido en los naturales, e. d.,* $m \cdot s(0) = m$ *para todo* $m \in \mathbb{N}$*. (véase teorema 5.1.16)*

Corolario 5.1.11. *Sea* $(\mathbb{N}, 0, s)$ *un Sistema de Peano. Entonces* $s(n) = n + 1$ *para toda* $n \in \mathbb{N}$

Demostración. $n + 1 = n + s(0) = s(n + 0) = s(n)$. ∎

Veamos ahora las propiedades que tiene la suma recién definida en $\mathbb{N}$.

Teorema 5.1.12. *Sean* $m, n, r \in \mathbb{N}$ *arbitrarios. Entonces*

(1) $(m + n) + r = m + (n + r)$ *(propiedad asociativa)*
(2) $m + n = n + m$ *(propiedad conmutativa)*
(3) $m + 0 = m$ *(existencia de elemento neutro)*
(4) *Si* $n + m = r + m$*, entonces* $n = r$ *(ley de cancelación)*
(5) *Si* $n \neq 0$*, entonces* $n + m \neq 0$ *para toda* $m \in \mathbb{N}$

Demostración. Demostraremos (1), (4) y (5) dejamos como ejercicio la demostración de (2). En cuanto a (3) la proposición se cumple por definición.

(1) Recordamos del teorema 5.1.8, que para toda $m \in \mathbb{N}$, la función $\psi_m : \mathbb{N} \longrightarrow \mathbb{N}$ es la única que satisface $\psi_m(0) = m$ y $\psi_m(s(n)) = s(\psi_m(n))$.
Para cualesquiera $m, n, r \in \mathbb{N}$, se tiene que
(i) $(\psi_m \circ \psi_n)(0) = \psi_m(\psi_n(0)) = \psi_m(n + 0) = \psi_m(n) = m + n = \psi_{m+n}(0)$.
(ii) Sabemos que $\psi_{m+n}(s(r)) = s(\psi_{m+n}(r))$. Pero también

$$(\psi_m \circ \psi_n)(s(r)) = s((\psi_m \circ \psi_n)(r))$$

porque

$$\begin{aligned}(\psi_m \circ \psi_n)(s(r)) &= \psi_m(\psi_n(s(r)))\\ &= \psi_m(s(\psi_n(r)))\\ &= s(\psi_m(\psi_n(r)))\\ &= s((\psi_m \circ \psi_n)(r)).\end{aligned}$$

Por lo tanto, por unicidad, $\psi_{m+n} = \psi_m \circ \psi_n$.
Luego $\psi_{m+n}(r) = (\psi_m \circ \psi_n)(r)$ para toda $r \in \mathbb{N}$ y como

$$\psi_{m+n}(r) = (m + n) + r$$

y

$$(\psi_m \circ \psi_n)(r) = \psi_m(\psi_n(r)) = \psi_m(n + r) = m + (n + r),$$

entonces

$$(m + n) + r = m + (n + r).$$

(4) Sea $T = \{m \in \mathbb{N} \mid n + m = r + m \text{ implica } n = r\} \subseteq \mathbb{N}$.
1º $0 \in T$ ya que, por (3), $n + 0 = r + 0$ implica $n = r$.
2º Supongamos que $m \in T$, es decir $n + m = r + m$ implica $n = r$. Debemos demostrar que $s(m) \in T$ y para esto supongamos que $n + s(m) = r + s(m)$. Como $n + s(m) = s(n + m)$ y $r + s(m) = s(r + m)$, entonces se tiene que $s(n + m) = s(r + m)$ y por ser s inyectiva, debe ser que $n + m = r + m$, que por hipótesis de inducción implica $n = r$. Por lo tanto $s(m) \in T$.
Entonces $T = \mathbb{N}$.

(5) Supongamos $n \neq 0$ y sea $T = \{m \in \mathbb{N} \mid n + m \neq 0\}$
1º $0 \in T$ ya que $n + 0 = n \neq 0$.
2º Supongamos que $m \in T$ y veamos que $s(m) \in T$. $n + s(m) = s(n + m) \neq 0$ por la proposición 5.1.3. Por lo tanto $T = \mathbb{N}$. ∎

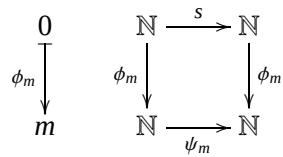
Nota 5.1.13. El inciso (5) de este último teorema es equivalente a la proposición 2.1.4.

Para introducir el producto en un Sistema de Peano, además del Teorema de Recursión, usaremos la suma ya definida.

Teorema 5.1.14. *Sea* $(\mathbb{N}, 0, s)$ *un Sistema de Peano. Entonces existe una única función* $\phi : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ *tal que para cualesquiera* $m, n \in \mathbb{N}$, $\phi(m, 0) = 0$ *y* $\phi(m, s(n)) = \phi(m, n) + m$.

Demostración.
Existencia
Sea $m \in \mathbb{N}$ fijo. En el Teorema de Recursión tomamos $X = \mathbb{N}$, $\psi_m : \mathbb{N} \longrightarrow \mathbb{N}$

dada por $\psi_m(n) = n + m$ y $x_0 = 0$. Entonces existe una única función $\phi_m : \mathbb{N} \longrightarrow \mathbb{N}$ tal que $\phi_m(0) = 0$ y $\psi_m(\phi_m(n)) = \phi_m(s(n))$.



Definimos $\phi : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ por $\phi(m, n) = \phi_m(n)$. Esta ϕ es la función buscada ya que

$$\phi(m, 0) = \phi_m(0) = 0 \text{ y } \phi(m, s(n)) = \phi_m(s(n)) = \psi_m(\phi_m(n)) = \psi_m(\phi(m, n)) = \phi(m, n) + m.$$

Unicidad
Supongamos que $\phi' : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ satisface también que

$$\phi'(m, 0) = 0 \ \ y \ \ \phi'(m, s(n)) = \phi'(m, n) + m,$$

para toda $m, n \in \mathbb{N}$. Para $m \in \mathbb{N}$, m fijo, sea $T = \{n \in \mathbb{N} \mid \phi'(m, n) = \phi(m, n)\}$. Probaremos que $T = \mathbb{N}$.

1º $0 \in T$ ya que por hipótesis $\phi'_1(m, 0) = 0 = \phi(m, 0)$.

2º Sea $n \in T$, es decir se debe cumplir, $\phi'(m, n) = \phi(m, n)$. Probaremos que $\phi'(m, s(n)) = \phi(m, s(n))$.

$$\phi'(m, s(n)) = \phi'(m, n) + m = \phi(m, n) + m = \phi(m, s(n)).$$

Entonces $s(n) \in T$. Por lo tanto $T = \mathbb{N}$ y así $\phi'(m, n) = \phi(m, n)$ para todas $m, n \in \mathbb{N}$. ∎

Notación 5.1.15. *Así como lo hicimos para la suma, denotamos*

$$\phi(m, n) = \boldsymbol{m \cdot n}$$

y lo llamaremos el ***producto de m y n****.*

Con esta notación, tenemos definido el producto por recursión como sigue:
Dado $m \in \mathbb{N}$ fijo,

(1) $m \cdot 0 = 0$;
(2) $m \cdot s(n) = m \cdot n + m$ para toda $n \in \mathbb{N}$.

Las propiedades del producto en $\mathbb{N}$ son:

Teorema 5.1.16. *Sean $m, n, r \in \mathbb{N}$ y $1 = s(0)$. Entonces*

(1) $(m \cdot n) \cdot r = m \cdot (n \cdot r)$ *(propiedad asociativa)*
(2) $m \cdot n = n \cdot m$ *(propiedad conmutativa)*
(3) $m \cdot 1 = m$ *(existencia de neutro multiplicativo: 1)*
(4) $r \cdot (m + n) = r \cdot m + r \cdot n$ *(distributividad del producto respecto a la suma)*
(5) *Si* $n \neq 0$ *y* $m \neq 0$, *entonces* $n \cdot m \neq 0$
(6) *Si* $n \neq 0$ *y* $n \cdot m = n \cdot r$, *entonces* $m = r$ *(ley de la cancelación)*

Demostración. Demostraremos (3), (4), (5) y (6) y dejamos como ejercicio (1) y (2).

(3) $m \cdot 1 = m \cdot s(0) = m \cdot 0 + m = 0 + m = m$.

(4) Sean $r, m \in \mathbb{N}$ fijos y sea $T = \{n \in \mathbb{N} \mid r \cdot (m + n) = r \cdot m + r \cdot n\} \subseteq \mathbb{N}$. Demostraremos por inducción que $T = \mathbb{N}$.
1º $0 \in T$ ya que $r \cdot (m + 0) = r \cdot m = r \cdot m + 0 = r \cdot m + r \cdot 0$.
2º Supongamos que $n \in T$, es decir, $r \cdot (m + n) = r \cdot m + r \cdot n$.

$$\begin{aligned} r \cdot (m + s(n)) &= r \cdot s(m + n) = r \cdot (m + n) + r = (r \cdot m + r \cdot n) + r \\ &= r \cdot m + (r \cdot n + r) = r \cdot m + r \cdot s(n). \end{aligned}$$

Por lo tanto $s(n) \in T$. Luego $T = \mathbb{N}$

(5) Sea $n \neq 0$ y sea $A = \{m \in \mathbb{N} \mid m \cdot n \neq 0\}$. Afirmamos que $A = \mathbb{N} - \{0\}$.
Como $Im(s) = \mathbb{N} - \{0\}$ (proposición 5.1.3), demostraremos que $A = Im(s)$.
Por ser $r \cdot 0 = 0$ para toda $r \in \mathbb{N}$, entonces $0 \notin A$ y por lo tanto

$$A \subseteq \mathbb{N} - \{0\} = Im(s).$$

Sea ahora $m \in Im(s)$. Entonces $m = s(t)$ para alguna $t \in \mathbb{N}$ y así

$$n \cdot m = n \cdot s(t) = n \cdot t + n$$

y como $n \neq 0$, por (5) del teorema 5.1.12, se tiene que $n \cdot t + n \neq 0$, es decir, $n \cdot m \neq 0$ y por lo tanto $m \in A$.
Concluimos entonces que $A = \mathbb{N} - \{0\}$ y con esto hemos demostrado que si $n \neq 0$ y $m \neq 0$, entonces $n \cdot m \neq 0$.

(6) Sea $m \neq 0$ y $T = \{n \in \mathbb{N} \mid m \cdot n = m \cdot r \; implica \; n = r\}$. Probaremos que $T = \mathbb{N}$.
1º $0 \in T$. Si $m \cdot 0 = m \cdot r$, entonces $m \cdot r = 0$ y por el inciso (5) ya que $m \neq 0$ debe ser $r = 0$.
2º Supongamos $n \in T$ y supongamos $m \cdot s(n) = m \cdot r$. Como $m \neq 0$ y $s(n) \neq 0$, por el inciso (5) $m \cdot s(n) \neq 0$ y por lo tanto $r \neq 0$. Entonces $r = s(r')$ para alguna $r' \in \mathbb{N}$. Luego

$$\begin{aligned} m \cdot s(n) = m \cdot r &= m \cdot s(r') \\ m \cdot n + m &= mr' + m \quad \text{(por definición de producto)} \\ m \cdot n &= mr' \quad \text{(por el teorema 5.1.12 (4))} \\ n &= r' \quad \text{(por hipótesis de inducción)} \end{aligned}$$

Entonces $s(n) = s(r') = r$. Por lo tanto $T = \mathbb{N}$. ∎

Usando el Teorema de Recursión podemos definir, para cada $a \in \mathbb{N}$ y $n \in \mathbb{N}$, a^n. En el teorema de recursión tomamos $X = \mathbb{N}$, $x_0 = 1$ y $\phi_a : \mathbb{N} \longrightarrow \mathbb{N}$ la función definida por $\phi_a(n) = a \cdot n$. Entonces existe una única función $F_a : \mathbb{N} \to \mathbb{N}$ tal que $F(s(n)) = \phi_a(F(n))$ y $F(0) = 1$. Como $s(n) = n + 1$ (corolario 5.1.11) se tiene

$$F_a(n + 1) = \phi_a(F_a(n)) = a \cdot F_a(n).$$

Definimos $a^n = F_a(n)$

(1) $a^0 = F(0) = 1$;
(2) $a^{n+1} = F_a(n + 1) = F_a(s(n)) = \phi_a(F_a(n)) = \phi_a(a^n) = a \cdot a^n$.

Generalmente, cuando queremos definir por recursión algún concepto, no es necesario escribir X, φ y x_0 del Teorema de Recursión, la definición se puede presentar de manera más simplificada como se muestra en la definición de a^n. Otro ejemplo de esto es la definición del factorial de una número natural.

(1) 0!=1;
(2) $(n + 1)! = (n + 1) \cdot n!$; para toda $n \in \mathbb{N}$.

En este caso es un poco más complicado exhibir X, x_0 y φ. Veamos: si en el Teorema de Recursión tomamos $X = \mathbb{N} \times \mathbb{N}$, $x_0 = (0, 1)$ y $\varphi : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \times \mathbb{N}$ dada por $\varphi(n, m) = (s(n), s(n) \cdot m)$.

$$\begin{array}{ccc} 0 & & \mathbb{N} \xrightarrow{\ s\ } \mathbb{N} \\ {\scriptstyle\psi}\downarrow & & {\scriptstyle F}\downarrow \qquad\qquad \downarrow{\scriptstyle F} \\ (0,1) & & \mathbb{N}\times\mathbb{N} \xrightarrow[\ \varphi\ ]{} \mathbb{N}\times\mathbb{N} \end{array}$$

Entonces existe una única función $F : \mathbb{N} \longrightarrow \mathbb{N} \times \mathbb{N}$ tal que $F(s(n)) = \varphi(F(n))$ y $F(0) = (0, 1)$. Para los primeros números naturales y denotando por $2 = s(1), 3 = s(2), 4 = s(3)$, etc; tenemos:

$F(0) = (0, 1)$
$F(1) = F(s(0)) = \varphi(F(0)) = \varphi(0, 1) = (s(0), s(0) \cdot 1) = (1, 1)$
$F(2) = F(s(1)) = \varphi(F(1)) = \varphi(1, 1) = (s(1), s(1) \cdot 1) = (2, 2 \cdot 1)$
$F(3) = F(s(2)) = \varphi(F(2)) = \varphi(2, 2 \cdot 1) = (s(2), s(2) \cdot 2 \cdot 1) = (3, 3 \cdot 2 \cdot 1)$

$F(4) = F(s(3)) = \varphi(F(3)) = \varphi(3, 3 \cdot 2 \cdot 1) = (s(3), s(3) \cdot 3 \cdot 2 \cdot 1) = (4, 4 \cdot 3 \cdot 2 \cdot 1)$.
Entonces, para cada $n \in \mathbb{N}$, definimos el factorial de n, $n!$ como $(p_2 \circ F)(n)$, donde p_2 es la proyección de $F(n)$ en la segunda coordenada. Se tiene entonces que

$0! = (p_2 \circ F)(0) = p_2(F(0)) = p_2((0, 1)) = 1;$
$1! = (p_2 \circ F)(1) = p_2(F(1)) = p_2((1, 1)) = 1;$
$2! = (p_2 \circ F)(2) = p_2(F(2)) = p_2((2, 2 \cdot 1)) = 2 \cdot 1 = 2 \cdot 1!;$
$3! = (p_2 \circ F)(3) = p_2(F(3)) = p_2((3, 3 \cdot 2 \cdot 1)) = 3 \cdot 2 \cdot 1 = 3 \cdot 2!;$
$4! = (p_2 \circ F)(4) = p_2(F(4)) = p_2((4, 4 \cdot 3 \cdot 2 \cdot 1)) = 4 \cdot 3 \cdot 2 \cdot 1 = 4 \cdot 3!.$
y en general, se puede ver que, si $F(n) = (n, n!)$, entonces

$$\begin{aligned}(n+1)! &= s(n)! \\ &= (p_2 \circ F)(s(n)) \\ &= p_2((\varphi \circ F)(n)) \\ &= p_2(\varphi(n, n!)) \\ &= p_2(s(n), s(n) \cdot n!) \\ &= p_2(n+1, (n+1) \cdot n!) \\ &= (n+1) \cdot n!\end{aligned}$$

La definición de orden en un sistema de Peano es exactamente la misma que presentamos en el capítulo 2 (definición 2.1.3) que es;
Dados $m, n \in \mathbb{N}$, diremos que m es menor que n, $m < n$, si existe $r \in \mathbb{N} - \{0\}$ tal que $m + r = n$, o equivalentemente, $m \leq n$ si existe $r \in \mathbb{N}$ tal que $m + r = n$. En ese mismo capítulo demostramos que es un orden parcial para lo cual aceptamos sin demostrar la proposición 2.1.4 y que ya hemos demostrado aquí (teorema 5.1.12 (5)). Así que las propiedades del orden (y que fueron demostradas ahí) se mantienen. Así mismo probamos que el principio de inducción (inciso 3 de la definición de sistema de Peano) es equivalente a que este orden es un buen orden.

§ 5.2. Presentación de un sistemas de Peano

En las sección anterior desarrollamos la Teoría de los Sistemas de Peano. Sin embargo hasta el momento no hemos exhibido un conjunto que sea un Sistema de Peano. La finalidad de esta sección es mostrar tal conjunto (modelo), que fue introducido en 1923 por John von Neuman (1903-1957) y cuya definición es la siguiente:

Definición 5.2.1. *Sea N el conjunto cuyos elementos son aquellos conjuntos que son obtenidos al aplicar repetidamente las siguientes reglas:*

(I) $\varnothing \in N$;

(II) Si $n \in N$, entonces $n \cup \{n\} \in N$.

Notación 5.2.2. *Si $n \in N$, denotamos a $n \cup \{n\}$ por $s(n)$ y a $\varnothing$ por 0.*

No será casualidad que $s(n) = n \cup \{n\}$ es el sucesor de n en los términos dados en la sección 5.1, pág. 204.
Según la definición de N y adelantándonos a utilizar los símbolos conocidos para los números naturales, tenemos

$$\begin{aligned}
\varnothing &= 0\\
s(0) &= 1 = 0 \cup \{0\} = \varnothing \cup \{\varnothing\} = \{\varnothing\} = \{0\}\\
s(1) &= 2 = 1 \cup \{1\} = \{\varnothing\} \cup \{\{\varnothing\}\} = \{\varnothing, \{\varnothing\}\} = \{0, 1\}\\
s(2) &= 3 = 2 \cup \{2\} = \{\varnothing, \{\varnothing\}\} \cup \{\{\varnothing, \{\varnothing\}\}\} = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\} = \{0, 1, 2\}\\
s(3) &= 4 = 3 \cup \{3\} = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\} \cup \{\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}\}\\
&= \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}\} = \{0, 1, 2, 3\}
\end{aligned}$$

Hemos definido para cada $n \in N$, $s(n) = n \cup \{n\}$. Esta asociación determina una función $s : N \longrightarrow N$ dada por $s(n) = n \cup \{n\}$ para toda $n \in N$. Con esto completamos la información para mostrar que $(N, 0, s)$ es un Sistema de Peano y antes de hacerlo necesitamos la siguiente

Proposición 5.2.3. *Para cualesquiera $m, n \in N$, si $m \in n$, entonces $m \subseteq n$.*

Demostración. Sea $m \in N$ y consideramos el subconjunto de N,

$$A = \{n \in N \mid m \notin n \text{ o } m \subseteq n\}.$$

Demostraremos que $A = N$, usando la definición de N (definición 5.2.1) y con esto se habrá demostrado la proposición ya que dados $m, n \in N$, se tiene que $m \in n$ o $m \notin n$, lo que significa que si $m \in n$, debido a que $A = N$, entonces deberá ser $m \subseteq n$.

$1^{\underline{o}}$ $0 \in A$ ya que $m \notin 0 = \varnothing$.

$2^{\underline{o}}$ Supongamos que $n \in N$, es decir, $m \notin n$ o $m \subseteq n$. Veremos que $s(n) \in A$ considerando las dos posibilidades para n.

1^{er} **caso:** $m \notin n$.

Como $m \in s(n)$ o $m \notin s(n)$, demostraremos que en el caso que $m \in s(n)$ se debe cumplir forzosamente que $m \subseteq n$. Así pues, supongamos que $m \in s(n)$. Entonces $m \in n \cup \{n\}$, lo que implica que $m \in n$ o $m = n$. Pero $m \in n$ no se da, ya que, por hipótesis, $m \notin n$, por lo que $m = n$ y por lo tanto $m = n \subseteq n \cup \{n\} = s(n)$. Entonces $s(n) \in A$.

2^{o} **caso:** $m \subseteq n$.

Como $m \subseteq n \subseteq n \cup \{n\} = s(n)$, entonces $s(n) \in A$.

Hemos demostrado que cada elemento de N es elemento de A, y como $A \subseteq N$, entonces $A = N$. ∎

Estamos ahora en condiciones de mostrar que el conjunto N junto con $0 = \varnothing$ y la función sucesor $s : N \longrightarrow N$ mencionada en el párrafo anterior a la proposición 5.2.3, es un Sistema de Peano.

Teorema 5.2.4. *La terna* $(N, 0, s)$ *es un Sistema de Peano.*

Demostración. Debemos demostrar que se satisfacen las tres propiedades dadas en la definición 5.1.1.

(1) $0 \notin Im(s)$. Esto se debe a que, para toda $n \in N$, $n \in s(n)$ y por lo tanto $s(n) \neq \varnothing$.

(2) s es inyectiva. Supongamos que $n \neq m$ y $s(m) = s(n)$. Entonces

$$m \cup \{m\} = n \cup \{n\}.$$

Como $m \in m \cup \{m\}$, entonces $m \in n \cup \{n\}$, y por ser $m \neq n$, se debe tener que $m \in n$, que por la proposición 5.2.3, implica $m \subseteq n$. Análogamente se demuestra que $n \subseteq m$ y por lo tanto $m = n$ y así s es inyectiva.

(3) En realidad la definición de N es una reformulación del Principio de Inducción ya que si $A \subseteq N$ tal que

(I) $0 \in A$

(II) Si $n \in A$, entonces $s(n) \in A$, como los elementos de N se obtiene mediante aplicaciones repetidas de (1) y (2)

Entonces debe ser $A = N$. ∎

Hemos construido un modelo, en la Teoría de Conjuntos, para un Sistema de Peano, y por lo tanto a este conjunto se le aplican todos los resultado vistos en las dos secciones anteriores. Describir la suma y el producto en N (como Sistema de Peano) en términos de los conjuntos que son elementos de N, aunque es posible, no tiene mucho caso hacerlo aquí. Sabemos que esa suma y producto existen, con las propiedades ya mencionadas en la sección 5.1.

De aquí en adelante, como ya hemos mencionado anteriormente, el conjunto de los números naturales será un Sistema de Peano, sin preocuparnos cuál es la naturaleza de los elementos del conjunto y a los cuales denotaremos con los símbolos que conocemos, que es,

$$\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}.$$

En cuanto al orden es más fácil describirlo y es como sigue

$$m < n \text{ si y sólo si } m \subsetneq n.$$

§ § Ejercicios sección 5.1.

5.1.1. [1] Sean $m, n, r \in \mathbb{N}$ arbitrarios. Entonces $m + n = n + m$.

5.1.2. [2] Sean $m, n, r \in \mathbb{N}$ arbitrarios. Entonces.
(1) $(m \cdot n) \cdot r = m \cdot (n \cdot r)$ (propiedad asociativa)
(2) $m \cdot n = n \cdot m$ (propiedad conmutativa)

5.1.3. Sea (N, n_0, s) es un Sistema de Peano, y sea $f : N \longrightarrow N'$ una función biyectiva.

(1) Defínase $n_0' = f(n_0) \in N'$ y $s' = f \circ s \circ f^{-1} : N' \longrightarrow N'$. Muestre que (N', n_0', s') es también un Sistema de Peano.
(2) Sea $a \in N'$ un elemento cualquiera. Dé una función $s' : N' \longrightarrow N'$ de modo que (N', a, s') sea un Sistema de Peano.

5.1.4. Suponga que (N, n_0, s) y (N', n_0', s') son dos Sistemas de Peano; $+_1$, $\cdot_1$ y $+_2$, $\cdot_2$ son las operaciones de suma y multiplicación respectivamente de estos sistemas y $\psi : N \longrightarrow N'$ el isomorfismo definido en la demostración del Teorema 5.1.4. Demuestra que ψ es un isomorfismo respecto a la suma y multiplicación, es decir, para todo $n, m \in N$

$$\psi(n +_1 m) = \psi(n) +_2 \psi(m) \qquad \text{y} \qquad \psi(n \cdot_1 m) = \psi(n) \cdot_2 \psi(m).$$

5.1.5. Sea $\varphi : X \longrightarrow X$ y $x_0 \in X$. Entonces por el Teorema de recursión existe una única función $\psi : \mathbb{N} \longrightarrow X$ tal que $\psi(0) = x_0$ y $\psi(s(n)) = \varphi(\psi(n))$.
Muestre que si φ es inyectiva y $a \notin Im(\varphi)$, entonces ψ es inyectiva.

5.1.6. Sean $N = \{0, 1\}$, $n_0 = 0$ y $s : N \longrightarrow N$ tal que $s(0) = 1$, $s(1) = 1$.

(1) ¿Qué propiedades cumple (N, n_0, s) de la definición de Sistema de Peano?
(2) Sean $X = N$, $x_0 = 0$ y $\varphi = s$. Muestre que no existe ninguna función $\psi : N \longrightarrow N$ tal que

[1] Parte del Teorema 5.1.12 pág. 206.
[2] Parte del Teorema 5.1.16 pág. 209.

(I) $\psi(n_0) = x_0$
(II) $\psi(s(n)) = \varphi(\psi(n))$
para todo $n \in N$.

5.1.7. Sean $N = \mathbb{N} \cup \{\star\}$, $n_0 = 0$ y

$$s(n) = \begin{cases} n+1 & \text{si } n \in \mathbb{N} \\ \star & \text{si } n = \star \end{cases}$$

(1) ¿Que propiedades cumple (N, n_0, s) de la definición de Sistema de Peano?
(2) Sean $X = \mathbb{N}$, $x_0 = 0$ y $\varphi : N \longrightarrow N$ definida por $\varphi(n) = n + 1$. Muestre que no existe ninguna función $\psi : N \longrightarrow N$ tal que
(I) $\psi(n_0) = x_0$
(II) $\psi(s(n)) = \varphi(\psi(n))$
para todo $n \in N$.

5.1.8. Sean $m, n \in \mathbb{N}$ arbitrarios. Muestre que $m+n = 0$ si y sólo si $m = 0$ o $n = 0$.

5.1.9. Sean $m, n, r \in \mathbb{N}$ arbitrarios. Muestre que $n \cdot m = 0$ si y sólo si $m = 0$ o $n = 0$.

5.1.10. Sean $m, n, k \in \mathbb{N}$ arbitrarios. Muestre que

(1) $0^0 = 1$
(2) $0^k = 0$ si $k \neq 0$
(3) $1^k = 1$
(4) $(n^m)^k = n^{m \cdot k}$

5.1.11. Muestre con un ejemplo que no es cierto en general que

(1) $n^{m^k} = (n^m)^k$
(2) $n^m = m^n$

5.1.12. Muestre que para cualesquiera dos conjuntos X, Y, elementos $x_0 \in X$, $y_0 \in Y$, y funciones $\varphi : X \times Y \longrightarrow X$ y $\varphi' : X \times Y \longrightarrow Y$ existen funciones únicas

$$\psi : \mathbb{N} \longrightarrow X \qquad \text{y} \qquad \psi' : \mathbb{N} \longrightarrow Y$$

que satisfacen

(1) $\psi(0) = x_0$
$\psi(s(n)) = \varphi(\psi(n), \psi'(n))$

(2) $\psi'(0) = y_0$
$\psi'(s(n)) = \varphi'(\psi(n), \psi'(n))$

5.1.13. Muestre que para cualesquiera tres funciones

$$\alpha : Y \longrightarrow X\,, \quad \beta : X \times \mathbb{N} \times Y \longrightarrow X \quad \text{y} \quad \delta : \mathbb{N} \times Y \longrightarrow Y$$

existe una única función $\psi : \mathbb{N} \times Y \longrightarrow X$ que satisface
$\psi(0, y) = \alpha(y)$
$\psi(s(n), y) = \beta(\psi(n, \delta(n, y)), n, y)$.

5.1.14.

(1) Muestre que hay una única función $\psi : \mathbb{N} \longrightarrow \mathbb{N}$ tal que,
$\psi(0) = 2$
$\psi(s(n)) = 3 + \psi(n)$
para todo $n \in \mathbb{N}$.
(2) Dé una definición explícita de la función ψ anterior.

5.1.15.

(1) Muestre que hay una única función $\psi : \mathbb{N} \longrightarrow \mathbb{N}$ tal que,
$\psi(0) = 2$
$\psi(s(n)) = \psi(n) + 2n + 3$
para todo $n \in \mathbb{N}$.
(2) Dé una definición explícita de la función ψ anterior.

5.1.16. Dé una definición recursiva para cada una de las siguientes sucesiones de naturales $a_0, a_1, a_2, \ldots$ donde

(1) $a_n = 7n$
(2) $a_n = 3n + 7$
(3) $a_n = 7$
(4) $a_n = (n + 1)(n + 2)$
(5) $a_n = 7^n$
(6) $a_n = 11n + 3$
(7) $a_n = n^2$
(8) $a_n = 2 - (-1)^n$

5.1.17. (1) Sea $a_1, a_2, a_3, \ldots$ una sucesión aritmética con diferencia d (es decir, para todo n, $a_n = a_n + d$), Probar que para $n \geq 2$ se tiene $a_n = a_1 + (n - 1)d$.

(2) Una sucesión o progresión geométrica con razón r es una sucesión de números $a_1, a_2, a_3, \ldots$ en que cada uno se obtiene del anterior multiplicando por el número r (es decir, para $n \geq 2$, $a_n = a_{n-1}r$). Dar una definición no recursiva para la sucesión geométrica con $a_1 = 5$ y $r = \frac{1}{2}$.

5.1.18. La sucesión de Fibonacci $f_1, f_2, f_3, \ldots$ se define como sigue $f_1 = 1$, $f_2 = 1$ y, para $n \geq 3$, $f_n = f_{n-1} + f_{n-2}$. Construir los primeros 10 términos de la sucesión de Fibonacci y probar la siguiente fórmula que nos proporciona una definición no recursiva de la sucesión:

$$f_n = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}.$$

§§ Ejercicios sección 5.2.

5.2.1. Suponga que (N, n_0, s) y (N', n_0', s') son dos Sistemas de Peano; $\leq_1$, $\leq_2$ son los respectivos ordenes y $\psi : N \longrightarrow N'$ el isomorfismo definido en la demostración del Teorema 5.1.4. Demuestra que ψ preserva el orden, es decir, para todo $n, m \in N$

$$n \leq_1 m \iff \psi(n) \leq_2 \psi(m).$$

5.2.2. Sean $m, n, p, q \in \mathbb{N}$ tales que $m + n = p + q$. Muestre que

$$m < p \iff q < n.$$

5.2.3. Sean $m, n, p, q \in \mathbb{N}$ tales que $n < m$ y $q < p$. Muestre que

$$mq + np < mp + nq.$$

Construcción de un Sistema de Peano

5. 2.4. Diga si los siguientes conjuntos son números naturales, justificando su respuesta:

(1) $\varnothing$
(2) $\{\varnothing, \{\varnothing\}\}$
(3) $\{\varnothing\}$
(4) $\{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \{\varnothing, \{\varnothing\}\}\}$
(5) $\{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}\}$
(6) $\{0, 1, 2, \ldots, n, n \cup \{n\}, \ldots\}$

5.2.5. Decimos que un conjunto x es transitivo si para todo $y \in x$, entonces $x \subseteq y$.

(1) ¿Cuáles de los conjuntos del ejercicio anterior son transitivos?
(2) ¿Qué diferencia hay entre un número natural y un conjunto transitivo?
(3) Pruebe o dé contraejemplos para las siguientes proposiciones
(I) Si X y Y son transitivos, entonces $X \cup Y$ es transitivo.
(II) Si X y Y son transitivos, entonces $X \cap Y$ es transitivo.
(III) X es transitivo si y sólo si $X \subseteq \mathcal{P}(X)$
(IV) Si $X \in Y$ y Y es transitivo, entonces X es transitivo.
(V) Si $X \subseteq Y$ y Y es transitivo, entonces X es transitivo.

Positivo dividido por positivo, o negativo por negativo, es afirmativo. Cifra dividida por cifra es nada. Positivo dividido por negativo es negativo. Negativo dividido por afirmativo es negativo. Positivo o negativo dividido por cero es una fracción con eso por denominador.

Brahmagupta
598 - 660

***Capítulo* 6**

Los números enteros

En el Capítulo 2 (véase pág. 133) se introdujo la diferencia $(m-n)$ de dos números naturales m y n, solamente cuando $m \geq n$. Para generalizar esta diferencia para cualesquiera numeros naturales, debemos construir un conjunto que contenga a los números naturales y donde esta diferencia no tenga restricciones, es decir, que esté definida para cualesquiera $n, m \in \mathbb{N}$.

Los números naturales resultan insuficientes para ser utilizados, por ejemplo, en las transacciones comerciales. Si una persona tiene $1,000$ pesos y debe 600 pesos, el balance entre lo que tiene y lo que debe se puede obtener realizando la diferencia entre $1,000$ y 600 (puesto que $1,000 > 600$) y que es 400. Anteponemos el símbolo $-$ a lo que se debe y denotando por $1,000 + (-600)$ a este balance, obtenemos que $1,000 + (-600) = 400$.

Sin embargo si se debiera más de lo que se tiene, esta diferencia no se puede realizar en los números naturales. Por ejemplo, si esta persona debiera $1,300$ pesos, es claro que lo que tiene no le alcanza para pagar toda la deuda. Sabemos que si abona $1,000$ pesos a la deuda, todavía quedaría debiendo 300 pesos. A diferencia del caso anterior, en éste no podemos hacer la diferencia $(1,000 - 1,300)$ ya que $1,000 < 1,300$. Siguiendo con la notación que hemos dado anteriormente podríamos denotar este balance por $1,000 + (-1,300) = -300$ y con esto estamos diciendo que después de abonar 1000 pesos a la deuda todavía se deben 300 pesos. En realidad lo que hicimos fue que a $1,300$ le restamos $1,000$ y al resultado, que fue 300, por el hecho de representar una deuda le anteponemos el símbolo $-$

a 300 para obtener -300. Resumiendo, el resultado lo obtenemos de la siguiente manera: $1,000 + (-1,300) = -(1,300 - 1,000) = -300$.
La idea entonces es agregar a los números naturales una "copia" de ellos donde igualdades como $1000 + (-1300) = -300$ tengan sentido. Esta copia consistiría en considerar el "conjunto" $-\mathbb{N} = \{-n \mid n \in \mathbb{N}\}$. Así pues el conjunto de los número enteros, que denotaremos por $\mathbb{Z}$, será el conjunto $\mathbb{N} \cup (-\mathbb{N})$ y el reto será definir las operaciones en este nuevo conjunto de tal manera que extienda las operaciones definidas en los números naturales, es decir, deberemos definir en el conjunto de los números enteros una suma y un producto, de tal manera que cuando dos números enteros sean naturales, la suma y el producto de ellos como números enteros deberá coincidir con la suma y producto, respectivamente, considerados como números naturales. La misma idea prevalecerá con el orden que se defina en el conjunto $\mathbb{Z}$.

§ 6.1. Presentación de los números enteros

Existen varias maneras de introducir formalmente el conjunto de los números enteros. Sin embargo la presentación que haremos aquí será de manera intuitiva; por cada número natural n consideremos un objeto que denotaremos por $-n$, sin decir exactamente quién es este objeto en la teoría de conjuntos.

En el capítulo 8 se construyen los enteros de una manera formal y es ahí donde queda claro qué objeto de la teoría de conjuntos es $-n$. Además la definición de suma y producto que damos aquí coincide plenamente con las introducidas en dicho capítulo.

Sea $-\mathbb{N} = \{-n \mid n \in \mathbb{N}\}$. El conjunto de los números enteros es $\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N})$. Entonces $a \in \mathbb{Z}$ si y sólo si $a = n$ o $a = -n$ para algún $n \in \mathbb{N}$.

Nota 6.1.1. Para definir la suma y el producto en $\mathbb{Z}$ debemos considerar las cuatro posibilidades que existen para una pareja a y b de números enteros, que son

$$\begin{array}{ll} (1)\ a = m, b = n; & (2)\ a = -m, b = -n; \\ (3)\ a = m, b = -n; & (4)\ a = -m, b = n. \end{array} \qquad (*)$$

En el capítulo 2 definimos la diferencia $n - m$ de dos números naturales n y m cuando $m \leq n$. Usando este concepto definimos la suma, considerando los cuatro casos que se pueden presentar para los enteros a y b dado en la nota 6.1.1, de la siguiente manera.

Definición 6.1.2. *Sean a y b números enteros, la suma de a y b está dada por*

$$a+b=\begin{cases} m+n & si\ (1); \\ -(m+n) & si\ (2); \\ m-n & si\ (3)\ y\ n\leq m; \\ -(n-m) & si\ (3)\ y\ m<n; \\ n-m & si\ (4)\ y\ m\leq n; \\ -(m-n) & si\ (4)\ y\ n<m. \end{cases}$$

Para probar las propiedades de la suma en cada una de ellas debemos considerar los seis casos, por lo que el proceso resulta muy largo, motivo por el cual no demostraremos la propiedades asociativa y conmutativa. Estas demostraciones pueden verse en el capítulo 8.

Teorema 6.1.3. Propiedades de la suma. *Sean* $a, b, c \in \mathbb{Z}$.

(1) $(a+b)+c=a+(b+c)$ *(propiedad asociativa)*
(2) $a+b=b+a$ *(propiedad conmutativa)*
(3) $a+0=a$ *(existencia de neutro aditivo)*
(4) *Existe* $a' \in \mathbb{Z}$ *tal que* $a+a'=0$ *(existencia de inverso aditivo)*

Demostración. Demostraremos (3) y (4), dejando como ejercicio (1) y (2) (ver ejercicio 6.1.1)
Como $a \in \mathbb{Z}$, entonces $a=m$ o $a=-m$, donde $m \in \mathbb{N}$.

(3) (*i*) Si $a=m$, por definición, $a+0=m+0=m=a$.
(*ii*) Si $a=-m$, como $0 \leq m$, entonces $a+0=-m+0=-(m-0)=-m=a$.
En ambos casos se tiene que $a+0=a$.
(4) (*i*) Sea $a=m$, entonces tomando $a'=-m$, se tiene
$a+a'=m+(-m)=m-m=0$.
(*ii*) Para $a=-m$, tomando $a'=m$, se tiene
$a+a'=(-m)+m=m-m=0$. ∎

A partir de estas propiedades, se pueden obtener otras más. Estas nuevas propiedades, como se verá en la Sección 2 de este capítulo, son resultado directo de las que acabamos de dar, y donde se puede apreciar que la naturaleza de los elementos de $\mathbb{Z}$ no es relevante.

En cuanto a la definición del producto de enteros, ésta es mucho más simple.
Considerando los mismo cuatro casos que se pueden presentar, como lo hicimos para la suma, definimos para cualesquiera enteros a y b, el producto de ellos como:

Definición 6.1.4.

$$a \cdot b = \begin{cases} m \cdot n & si\ (1)\ o\ (2)\ de\ (*) \\ -(m \cdot n) & si\ (3)\ de\ (*)\ y\ m \neq 0 \\ -(m \cdot n) & si\ (4)\ de\ (*)\ y\ n \neq 0 \\ 0 & si\ (a = 0\ y\ b = -n\ )\ o\ (a = -m\ y\ b = 0) \end{cases}$$

Queda claro que la suma y producto definidos en $\mathbb{Z}$ son una extensión de las correspondientes operaciones en $\mathbb{N}$.
Veamos las propiedades que satisface el producto.

Teorema 6.1.5. *(**Propiedades del Producto**) Sean $a, b, c \in \mathbb{Z}$. Entonces*

(1) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *(propiedad asociativa)*
(2) $a \cdot b = b \cdot a$ *(propiedad conmutativa)*
(3) $a \cdot 1 = a$ *(existencia de neutro multiplicativo)*
(4) $a \cdot (b + c) = a \cdot b + a \cdot c$ *(ley distributiva del producto respecto a la suma)*

Demostración. Dejamos como ejercicio la demostración de (2) y (3). (ver ejercicio 6.1.2)

(1) Probaremos esta propiedad sólo para 4 de los 8 casos que se pueden presentar, quedando como ejercicio la demostración de los restantes casos. (ver ejercicio 6.1.2)
Para $m, n, r \in \mathbb{N}$, consideramos los siguientes cuatro casos, en donde en cada uno de ellos usamos el hecho de que el producto es asociativo en $\mathbb{N}$.
(i) $a = m, b = n, c = r$.
En este caso es inmediato que $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ ya que $a, b, c \in \mathbb{N}$ y sabemos que el producto en $\mathbb{N}$ es asociativo.
(ii) $a = m, b = -n, c = -r$.

$$\begin{aligned} (a \cdot b) \cdot c &= (m \cdot (-n)) \cdot (-r) \\ &= [-(m \cdot n))] \cdot (-r) && \text{(definición del producto en } \mathbb{Z}) \\ &= (m \cdot n) \cdot r && \text{(definición del producto en } \mathbb{Z}) \\ &= m \cdot (n \cdot r) && \text{(asociatividad del producto en } \mathbb{N}) \\ &= m \cdot [(-n) \cdot (-r)] && \text{(definición del producto en } \mathbb{Z}) \\ &= a \cdot (b \cdot c) \end{aligned}$$

(iii) $a = -m, b = -n, c = -r$.

$$\begin{aligned}(a\cdot b)\cdot c &= [(-m)\cdot(-n)]\cdot(-r)\\ &= (m\cdot n))\cdot(-r) && \text{(definición del producto en } \mathbb{Z})\\ &= -[(m\cdot n)\cdot r] && \text{(definición del producto en } \mathbb{Z})\\ &= -[m\cdot(n\cdot r)] && \text{(asociatividad del producto en } \mathbb{N})\\ &= (-m)\cdot(n\cdot r) && \text{(definición del producto en } \mathbb{Z})\\ &= (-m)\cdot[(-n)\cdot(-r)] && \text{(definición del producto en } \mathbb{Z})\\ &= a\cdot(b\cdot c)\end{aligned}$$

(iv) $a = m$, $b = n$, $c = -r$.

$$\begin{aligned}(a\cdot b)\cdot c &= (m\cdot n)\cdot(-r)\\ &= -[(m\cdot n)\cdot r] && \text{(definición del producto en } \mathbb{Z})\\ &= -[m\cdot(n\cdot r)] && \text{(asociatividad del producto en } \mathbb{N})\\ &= m\cdot[-(n\cdot r)] && \text{(definición del producto en } \mathbb{Z})\\ &= m\cdot[n\cdot(-r)] && \text{(definición del producto en } \mathbb{Z})\\ &= a\cdot(b\cdot c)\end{aligned}$$

(4) Demostraremos sólo 2 de los 8 casos y dejamos como ejercicio los casos restantes. (ver ejercicio 6.1.2)

(i) $a = m$, $b = -n$, $c = -r$.

$$\begin{aligned}a\cdot(b+c) &= m\cdot[(-n)+(-r)]\\ &= m\cdot[-(n+r)] && \text{(definición de la suma en } \mathbb{Z})\\ &= -[m\cdot(n+r)] && \text{(definición del producto en } \mathbb{Z})\\ &= -[m\cdot n+m\cdot r)] && \text{(propiedad distributiva en } \mathbb{N})\\ &= [-(m\cdot n)]+[-(m\cdot r)] && \text{(definición de la suma en } \mathbb{Z})\\ &= [m\cdot(-n)]+[m\cdot(-r)] && \text{(definición del producto en } \mathbb{Z})\\ &= a\cdot b+a\cdot c\end{aligned}$$

(iii) $a = m$, $b = n$, $c = -r$.

En este caso se considerarán dos subcasos, que son $r \le n$ o $n < r$.

(i') Si $r \le n$, entonces $(n-r) \in \mathbb{N}$.

$$\begin{aligned}a\cdot(b+c) &= m\cdot[n+(-r)]\\ &= m\cdot(n-r) && \text{(definición de la suma en } \mathbb{Z})\\ &= m\cdot n-m\cdot r && \text{(proposición 2.1.10 (6))}\\ &= m\cdot n+(-m\cdot r) && \text{(definición de la suma en } \mathbb{Z})\\ &= m\cdot n+m\cdot(-r) && \text{(definición del producto en } \mathbb{Z})\\ &= a\cdot b+a\cdot c\end{aligned}$$

(ii') Si $n < r$, entonces $(r-n) \in \mathbb{N}$.

$$\begin{aligned}
a \cdot (b + c) &= m \cdot [n + (-r)] \\
&= m \cdot [-(r - n)] && \text{(definición de la suma en } \mathbb{Z}) \\
&= -[m \cdot (r - n)] && \text{(definición del producto en } \mathbb{Z}) \\
&= -[m \cdot r - m \cdot n)] && \text{(proposición 2.1.10 (6))} \\
&= (m \cdot n) + (-(m \cdot r)) && \text{(definición de la suma en } \mathbb{Z}\ (m \cdot n < m \cdot r)) \\
&= (m \cdot n) + (m \cdot (-r)) && \text{(definición del producto en } \mathbb{Z}) \\
&= a \cdot b + a \cdot c \ \blacksquare
\end{aligned}$$

§ 6.2. Anillos

Antes de continuar el estudio de los números enteros, nos detendremos un poco para ver a este conjunto como una "estructura algebraica" en el sentido de considerar a $\mathbb{Z}$ junto con la suma y el producto que ya hemos definido. Esta estructura algebraica de los números enteros, $(\mathbb{Z}; +, \cdot)$ es un ejemplo de un concepto más general que es el de anillo y cuya definición y consecuencias inmediatas de éstas, estudiamos en esta sección para aplicarlas a los números enteros. Veamos pues la definición de anillo.

Definición 6.2.1. *Una* ***anillo*** $(R, +, \cdot)$ *es un conjunto* R *junto con dos operaciones binarias que llamaremos suma y producto y denotamos por* $+$ *y* $\cdot$ *respectivamente, que satisfacen las siguientes propiedades para cualesquiera* $x, y, z \in R$.

(1) $(x + y) + z = x + (y + z)$; *(asociatividad de la suma)*

(2) $x + y = y + x$; *(conmutatividad de la suma)*

(3) *Existe un elemento en* R*, denotado por* 0*, tal que* $x + 0 = 0 + x = x$ *(existencia de neutro aditivo)*

(4) *Para todo* $x \in R$*, existe* $w \in R$ *tal que* $w + x = x + w = 0$ *(existencia del inverso aditivo)*

(5) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ *(asociatividad del producto)*

(6) *Existe un elemento, denotado por* 1*, tal que* $x \cdot 1 = 1 \cdot x = x$ *(asociatividad del producto)*

(7) $\begin{aligned} x \cdot (y + z) &= x \cdot y + x \cdot z; \\ (x + y) \cdot z &= x \cdot z + y \cdot z. \end{aligned}$ *(distributividad del producto respecto a la suma)*

Si el producto en un anillo es conmutativo diremos que el anillo es un ***anillo conmutativo***.

Nota 6.2.2. Hemos usado los símbolos + y · para denotar las operaciones definidas en el anillo y debe quedar claro que se trata únicamente de una notación, lo que significa que, en general, la suma y el producto + y · definidos en un anillo no tienen nada que ver con la suma y producto definidos en $\mathbb{Z}$. Esto es, en cada caso concreto para un conjunto R se deberá especificar cómo están definidas la suma y el producto. También, en general, hemos denotado por 0 y por 1 al neutro aditivo y al neutro multiplicativo respectivamente. Sin embargo, la única relación que hay entre estos con el 0 y el 1 de los números enteros son las propiedades que los definen, de tal manera que, estos elementos 0 y 1, estarán determinados por la naturaleza de los elementos del conjunto R dado y las operaciones ahí definidas. En resumen, 0 y 1 son simplemente notaciones para el neutro aditivo y multiplicativo respectivamente en un anillo R. Cuando veamos ejemplos distintos a $(\mathbb{Z}, +, \cdot)$, esto se podrá ver con más claridad.

Como ya hemos mencionado anteriormente, un ejemplo de anillo es $(\mathbb{Z}, +, \cdot)$ y más adelante tendremos oportunidad de dar algunos más.

Proposición 6.2.3. $(\mathbb{Z}, +, \cdot)$ *es un anillo conmutativo.*

Como consecuencia inmediata de la definición de anillo tenemos

Proposición 6.2.4. *Sea* $(R, +, \cdot)$ *un anillo y sean* $x, y, z \in R$.

(1) *Si* $x + y = x + z$ *o* $y + x = z + x$, *entonces* $y = z$. *(ley de cancelación para la suma).*

(2) *El neutro aditivo es único.*

(3) *El inverso aditivo es único.*

(4) *El neutro multiplicativo es único.*

(5) $x \cdot 0 = 0 \cdot x = 0$.

Demostración.

(1) Supongamos $x + y = x + z$ y sea w un inverso aditivo de x. Sumado w a ambos lados de la igualdad obtenemos

$$\begin{aligned} w + (x + y) &= w + (x + z) && \\ (w + x) + y &= (w + x) + z && \text{(por la asociatividad de la suma)} \\ 0 + y &= 0 + z && \text{(debido a que } w + x = 0 \text{ por ser } w \text{ inverso aditivo de } x\text{)} \\ y &= z && \text{(debido a que 0 es neutro aditivo)} \end{aligned}$$

Como la suma es conmutativa, automáticamente se cumple el otro caso.

(2) Supongamos que 0 y $0'$ son neutros aditivos en R. Entonces

$$\begin{aligned} 0 &= 0 + 0' && \text{(por ser } 0' \text{ neutro aditivo)} \\ 0' &= 0 + 0' && \text{(por ser 0 neutro aditivo)} \end{aligned}$$

Por lo tanto $0 = 0'$.

(3) Supongamos que w y w' son inversos aditivos de x.

$$\begin{aligned} w &= w + 0 && \text{(propiedad del neutro aditivo)} \\ &= w + (x + w') && (w' \text{ es inverso aditivo de } x) \\ &= (w + x) + w' && \text{(asociatividad de la suma)} \\ &= 0 + w' && (w \text{ es inverso aditivo de } x) \\ &= w' && \text{(propiedad del neutro aditivo)} \end{aligned}$$

(4) La demostración es análoga a la demostración dada en (2).

(5) Por ser 0 el neutro en R, tenemos que $0 + 0 = 0$. Entonces

$$\begin{aligned} x \cdot (0 + 0) &= x \cdot 0 \\ x \cdot 0 + x \cdot 0 &= x \cdot 0 && \text{(ley distributiva)} \\ x \cdot 0 + x \cdot 0 &= x \cdot 0 + 0 && \text{(propiedad del neutro aditivo)} \\ x \cdot 0 &= 0 && \text{(ley de cancelación para la suma)} \end{aligned}$$

De la misma manera se demuestra que $0 \cdot x = 0$. ∎

Debido a que $(\mathbb{Z}; +, \cdot)$ es un anillo, automáticamente se satisfacen en $\mathbb{Z}$ las propiedades dadas en la proposición 6.2.4.

Notación 6.2.5*. Como el inverso aditivo de cada elemento en un anillo es único, dada $a \in R$, denotamos por* $\boldsymbol{-a}$ *al inverso aditivo de a. Entonces $-a$ es el único elemento en R que satisface*

$$a + (-a) = (-a) + a = 0.$$

Nota 6.2.6. Considerando la notación del inverso aditivo de cada elemento de un anillo que acabamos de introducir y por otro lado tomando en cuenta que los elementos de $\mathbb{Z}$ son de la forma n o de la forma $-n$, donde $n \in \mathbb{N}$, lo primero que uno pensaría es que esto nos lleva a una confusión puesto que para cada número natural n, por un lado $-n$ denota el inverso aditivo de n y por otro $-n$ denota un elemento de los que hemos agregado a $\mathbb{N}$ para obtener $\mathbb{Z}$. Afortunadamente esta confusión no se da ya que $-n$ visto como uno de los elementos que hemos agregado a $\mathbb{N}$ es precisamente el inverso aditivo de n, esto es, $n + (-n) = 0$.

Nota 6.2.7. Debido a que $0 + 0 = 0$ y a la unicidad del inverso aditivo, se tiene que $-0 = 0$.

Proposición 6.2.8. *Sea $(R; +, \cdot)$ un anillo. Entonces $-a = (-1) \cdot a$, para cada $a \in R$.*

Demostración. Basta demostrar que $(-1) \cdot a$ es el inverso aditivo de a.

$$\begin{aligned}(-1) \cdot a + a &= (-1) \cdot a + 1 \cdot a && \text{(propiedad del neutro multiplicativo)}\\ &= ((-1) + 1)a && \text{(ley distributiva)}\\ &= 0 \cdot a && \text{(inverso aditivo)}\\ &= 0 && \text{(porposición 6.2.4 (5))}\end{aligned}$$

Por la unicidad del inverso aditivo, tenemos que $-a = (-1)a$. ∎

Proposición 6.2.9. *Sea $(R; +, \cdot)$ un anillo y sean $a, b \in R$. Entonces*

(1) $-(-a) = a$.
(2) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$. *En particular,* $(-1) \cdot b = -b$.
(3) $(-a) \cdot (-b) = a \cdot b$.

Demostración.

(1) $-(-a)$ denota el inverso de $-a$ y por otro lado a es el inverso de $-a$ ya que $(-a) + a = 0$, por lo que, debido a que el inverso es único, $-(-a) = a$.
(2) Mostraremos que tanto $(-a) \cdot b$ y $a \cdot (-b)$ son ambos inversos de $a \cdot b$ y por lo tanto ambos deben ser iguales a $-(a \cdot b)$, debido a la unicidad del inverso aditivo,
$$a \cdot b + (-a) \cdot b = (a + (-a)) \cdot b = 0 \cdot b = 0,$$
$$a \cdot b + a \cdot (-b) = a \cdot (b + (-b)) = a \cdot 0 = 0.$$
(3) Como $a \cdot b$ es el inverso de $-(a \cdot b)$ (inciso (1)), para demostrar la igualdad requerida, mostraremos que $(-a) \cdot (-b)$ es el inverso de $-(a \cdot b)$ y para esto usamos el inciso (2), que es, $-(a \cdot b) = (-a) \cdot b$,
$$-(a \cdot b) + (-a) \cdot (-b) = (-a) \cdot b + (-a) \cdot (-b) = (-a) \cdot (b + (-b)) = (-a) \cdot 0 = 0.$$ ∎

Definición 6.2.10. *Sea $(R; +, \cdot)$ un anillo y $a, b \in R$. La diferencia de a y b, denotada por $\boldsymbol{a - b}$, es $a - b = a + (-b)$.*

La diferencia satisface las siguientes propiedades.

Teorema 6.2.11. *Sea $(R; +, \cdot)$ un anillo y sean $a, b, c, d \in R$. Entonces*

(1) $a - a = 0$,
(2) $-(a + b) = -a - b$,
(3) $(a - b) + (c - d) = (a + c) - (b + d)$,
(4) $a \cdot (b - c) = a \cdot b - a \cdot c$,
(5) $(a - b) \cdot (c - d) = (a \cdot c + b \cdot d) - (a \cdot d + b \cdot c)$.

Demostración. Demostraremos (2) y (4) y dejamos como ejercicio la demostración de (1), (3) y (5). (Ver ejercicio 6.2.1)

(2) Por la proposición 6.2.9, $-(a + b) = (-1) \cdot (a + b)$ y por ser el producto distributivo respecto a las suma, se tiene que

$$(-1) \cdot (a + b) = (-1) \cdot a + (-1) \cdot b = -a + (-b) = -a - b.$$

(4)

$$\begin{aligned} a \cdot (b - c) &= a \cdot (b + (-c)) \\ &= a \cdot b + a \cdot (-c) && \text{(propiedad distributiva)} \\ &= a \cdot b + (-(a \cdot c)) && \text{(proposición 6.2.9 (2))} \\ &= a \cdot b - a \cdot c && \text{(por definición)} \end{aligned}$$ ∎

Proposición 6.2.12. *Sean $a, b \in \mathbb{Z}$. Si $a \cdot b = 0$, entonces $a = 0$ o $b = 0$.*

Demostración. Supongamos que $a \cdot b = 0$. Demostraremos que $a = 0$ o $b = 0$ en cada uno de los distintos casos que se pueden presentar para a y b y donde consideramos $m, n \in \mathbb{N}$.

Caso 1. $a = m$, $b = n$. Como $a, b \in \mathbb{N}$, por la proposición 2.1.2 (2) tenemos que debe ser $a = 0$ o $b = 0$.

Caso 2. $a = -m$, $b = -n$.

$$\begin{aligned} 0 &= a \cdot b && \text{(hipótesis)} \\ &= (-m) \cdot (-n) && \text{(propiedad distributiva)} \\ &= m \cdot n && \text{(proposición 6.2.9 (3))} \end{aligned}$$

Luego por la proposición 2.1.2 (2), $m = 0$ o $n = 0$ y así $a = -0 = 0$ o $b = -0 = 0$.

Caso 3. $a = m$, $b = -n$.

$$\begin{aligned} 0 &= -0 && \text{(nota 6.2.7)} \\ &= -(a \cdot b) && \text{(hipótesis)} \\ &= -[m \cdot (-n)] \\ &= -[-(m \cdot n)] && \text{(definición de producto en } \mathbb{Z}) \\ &= m \cdot n && \text{(proposición 6.2.9 (3))} \end{aligned}$$

Por lo tanto $m = 0$ o $n = 0$. Luego $a = 0$ o $b = -0 = 0$

Caso 4. $a = -m$, $b = n$. Como el producto en $\mathbb{Z}$ es conmutativo, este caso se reduce al tercer caso. ∎

A los anillos que satisfacen las propiedades dadas en la proposición 6.2.12, se les da un nombre especial que es

Definición 6.2.13. *Un anillo conmutativo* $(R; +, \cdot)$ *se llama* **dominio entero** *en el caso en que para cualesquiera* $x, y \in R$, *si* $x \cdot y = 0$, *entonces* $x = 0$ *o* $y = 0$.

La proposición 6.2.12 dice entonces que $(\mathbb{Z}; +, \cdot)$ es un dominio entero.
Un elemento x de un anillo conmutativo R se llama ***divisor de cero*** si existe $y \in R$, $y \neq 0$, tal que $x \cdot y = 0$. Según esta definición, 0 siempre será un divisor de cero debido a que $0 \cdot y = 0$ para todo $y \in R$. Así pues, un anillo conmutativo será dominio si no tiene divisores de cero, con excepción de 0.
El siguiente resultado nos da una propiedad equivalente para que un anillo conmutativo sea un dominio entero.

Teorema 6.2.14. *Un anillo conmutativo* R *es un dominio entero si y sólo si valen las leyes de cancelación para el producto, es decir, para toda* $x, y, z \in R$, *si* $x \cdot y = x \cdot z$ *y* $x \neq 0$, *entonces* $y = z$.

Demostración.

$\Longrightarrow$) Supongamos que R es un dominio entero y supongamos que $x \cdot y = x \cdot z$, con $x \neq 0$. Entonces $0 = x \cdot y - x \cdot z = x \cdot (y - z)$ y por lo tanto $x = 0$ o $y - z = 0$. Como, por hipótesis, $x \neq 0$, debe tenerse que $y - z = 0$, que es, $y = z$.

$\Longleftarrow$) Supongamos que $x, y \in R$ son tales que $x \cdot y = 0$. En el caso $x = 0$ no hay nada que demostrar, así que supondremos que $x \neq 0$. Demostraremos que $y = 0$.
Se tiene entonces que $x \cdot y = 0 = x \cdot 0$ con $x \neq 0$, por lo que por hipótesis, $y = 0$. ∎

Corolario 6.2.15. *En* $(\mathbb{Z}; +, \cdot)$ *valen las leyes de cancelación para el producto.*

Por último es importante resaltar que la diferencia $a - b$ que definimos para número naturales a y b, donde $b \leq a$ coincide con la diferencia $a - b$ cuando son considerados números enteros, ya que en este caso, $a + (-b)$ se definió justamente como la diferencia $a - b$ en $\mathbb{N}$.

§ 6.3. Orden en los enteros

Así como hemos extendido la suma y el producto en $\mathbb{N}$ a una suma y producto en $\mathbb{Z}$, respectivamente, extenderemos el orden dado en $\mathbb{N}$ a un orden en $\mathbb{Z}$, esto es, definiremos un orden en $\mathbb{Z}$ que también denotaremos $<$, de tal manera que para cualesquiera números naturales n y m se tiene que $n < m$ en $\mathbb{N}$ si y sólo si $n < m$ en $\mathbb{Z}$. Lo interesante aquí es que este orden lo podemos definir exactamente igual a como lo hicimos en $\mathbb{N}$.

Definición 6.3.1. *Dados dos números enteros a y b, diremos que* ***a es menor que b****, y lo denotamos $a < b$ (o $b > a$), si existe $m \in \mathbb{N}$, $m \neq 0$ tal que $a + m = b$.*

Evidentemente la relación dada en la definición 6.3.1 restringida a $\mathbb{N}$ (es decir cuando
$a, b \in \mathbb{N}$) coincide con la relación de orden que hemos definido en $\mathbb{N}$.
Veamos que $<$ es un orden parcial en $\mathbb{Z}$.

Teorema 6.3.2. *$<$ es un orden parcial en $\mathbb{Z}$.*

Demostración.

(1) $a \not< a$ para toda $a \in \mathbb{Z}$, ya que en caso contrario, existiría $m \in \mathbb{N}$, $m \neq 0$ tal que $a + m = a = a + 0$, lo que implicaría, por la ley de cancelación en la suma, que $m = 0$, lo que no puede ser por hipótesis.
(2) Supongamos que $a < b$ y $b < c$. Entonces existen $m, n \in \mathbb{N}$, $m \neq 0, n \neq 0$ tales que $a + m = b$ y $b + n = c$. Sumando n a la primera igualdad en ambos lados tenemos $(a + m) + n = b + n = c$, y por la propiedad asociativa de la suma, tenemos que $a + (m + n) = c$, donde $m + n \neq 0$ por la proposición 2.1.4. Por lo tanto $a < c$. ∎

En el caso en que usemos $\leq$, tendríamos que $a \leq b$ si y sólo si existe $m \in \mathbb{N}$ tal que $a + m = b$. Es decir cuando usamos $\leq$ no se pide $m \neq 0$.

Proposición 6.3.3. *Sean $m, n \in \mathbb{N}$. Entonces*

(1) *$-n < -m$ si y sólo si $m < n$. En particular para $m \neq 0$, $-m < 0$.*
(2) *$-m \leq n$ y si $m \neq 0$, entonces $-m < n$.*

Demostración.

(1) $\Longrightarrow$) Supongamos que $-n < -m$. Por definición, existe $r \in \mathbb{N}$, $r \neq 0$ tal que $-n + r = -m$. Sumando $n + m$ a ambos lados de la igualdad, obtenemos que $m + r = n$. Por lo tanto $m < n$.

$\Longleftarrow$) Si $m < n$, entonces $m + r = n$ para algún $r \in \mathbb{N}$, con $r \neq 0$. Multiplicando por (-1), tenemos que $-m - r = -n$ y así $-m = -n + r$. Por lo tanto $-n < -m$. En particular si $m \neq 0$, $0 < m$. Luego $-m < -0 = 0$.

(2) $-m \leq n$ ya que $-m + (m + n) = n$, donde $m + n \in \mathbb{N}$, y si $m \neq 0$, entonces se tendrá que $m + n \neq 0$ por la proposición 2.1.4. Luego $-m < n$. ∎

Corolario 6.3.4. $\mathbb{N} = \{x \in \mathbb{Z} \mid x \geq 0\}$.

Demostración. Por el inciso (1) de la proposición 6.3.3, para toda $n \in \mathbb{N}$, $n \geq 0$. Ahora, si $x \in \mathbb{Z}$ y $x \geq 0$, entonces existe $m \in \mathbb{N}$ tal que $0 + m = x$, Luego $x \in \mathbb{N}$. ∎

De acuerdo a la proposición 6.3.3, los enteros escritos en orden ascendente son

$$\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots$$

Así como en los números naturales el orden es total, lo mismo sucede para el orden que hemos definido para los números enteros.

Teorema 6.3.5. *El orden $<$ en $\mathbb{Z}$ es total.*

Demostración. Sean $a, b \in \mathbb{Z}$. Veremos que en cada uno de los 4 casos que se pueden presentar, $a \leq b$ o $b \leq a$. Para esto, sean $m, n \in \mathbb{N}$. Debido a que el orden en $\mathbb{Z}$ restringido a $\mathbb{N}$ coincide con el de los naturales y ya hemos visto que este orden es total, entonces $m \leq n$ o $n \leq m$. Supongamos que $m \leq n$.

Caso 1; $a = m$, $b = n$. Entonces $a \leq b$.
Caso 2; $a = -m$, $b = -n$. Como $m \leq n$, entonces por la proposición 6.3.3 (2), $a = -n \leq -m = b$.
Caso 3; $a = m$, $b = -n$. Por la proposición 6.3.3 (2), $b = -n \leq m = a$.
Caso 4; $a = -m$, $b = n$. Por la proposición 6.3.3 (2), $a = -m \leq n = b$. ∎

La propiedad del orden que se tiene en $\mathbb{N}$, que es la de ser buen orden, no se conserva en $\mathbb{Z}$, es decir, existen subconjuntos no vacíos de $\mathbb{Z}$ que no tienen elemento mínimo, por ejemplo, en el ejercicio 6.3.1, se pide demostrar que $A = \{-n \mid n \in \mathbb{N}\}$ no tiene elemento mínimo.
En la siguiente proposición presentamos las propiedades de $<$ y en cada una de ellas ponemos entre paréntesis la propiedad correspondiente para $\leq$.

Proposición 6.3.6. *Sean $a, b, c, d \in \mathbb{Z}$.*

(1) *$a \leq b$ si y sólo si $-b \leq -a$.*
(2) *Si $a < b$, entonces $a + c < b + c$ $\quad (a \leq b \Longrightarrow a + c \leq b + c)$.*

(3) *Si* $a < b$ *y* $c < d$, *entonces* $a + c < b + d$ $\quad (a \leq b, c \leq d \Longrightarrow a + c \leq b + d)$.
(4) *Si* $a < b$ *y* $0 < c$, *entonces* $a \cdot c < b \cdot c$ $\quad (a \leq b, 0 \leq c \Longrightarrow a \cdot c \leq b \cdot c)$.
(5) *Si* $0 < a < b$ *y* $0 < c < d$, *entonces* $0 < a \cdot c < b \cdot d$
$(0 \leq a \leq b, 0 \leq c \leq d \Longrightarrow 0 \leq a \cdot c \leq b \cdot d)$.
(6) *Si* $a < b$ *y* $c < 0$, *entonces* $b \cdot c < a \cdot c$ $\quad (a \leq b, c \leq 0 \Longrightarrow b \cdot c \leq a \cdot c)$.
(7) *Si* $a \neq 0$, *entonces* $0 < a^2$ $\quad (0 \leq a^2)$.

Demostración. Demostraremos los incisos (3), (5), (6) y (7) y los restantes quedan como ejercicio (ver ejercicio 6.3.3)

(3) Sea $a < b$ y $c < d$. Entonces existen $r, t \in \mathbb{N} - \{0\}$ tales que $a + r = b$ y $c + t = d$. Sumando ambas igualdades obtenemos $(a + c) + (r + t) = b + d$ y puesto que $r + t \in \mathbb{N} - \{0\}$ por la proposición 2.1.4, $a + c < b + d$.
(5) Sea $0 < a < b$ y $0 < c < d$. Entonces existen $r, t \in \mathbb{N} - \{0\}$ tales que $a + r = b$ y $c + t = d$. Multiplicando estas dos igualdades tenemos $(a + r) \cdot (c + t) = b \cdot d$ y así $a \cdot c + (a \cdot t + r \cdot c + r \cdot t) = b \cdot d$, donde $a \cdot t + r \cdot c + r \cdot t \in \mathbb{N} - \{0\}$ debido a las proposiciones 2.1.2 (2) y 2.1.4. Por último $0 < a \cdot c$ se debe al inciso (4).
(6) Sean $a < b$ y $c < 0$. Entonces $a + r = b$ para alguna $r \in \mathbb{N} - \{0\}$. Multiplicando por c, $a \cdot c + r \cdot c = b \cdot c$, de donde $a \cdot c = b \cdot c - r \cdot c = b \cdot c + [-(r \cdot c)]$. Ahora, $-(r \cdot c) = r \cdot (-c)$ y como $r > 0$ y $-c > 0$ (inciso (1)), entonces por el inciso (5), $r(-c) > 0$ y por lo tanto $b \cdot c < a \cdot c$.
(7) Sea $a \neq 0$. Entonces $0 < a$ o $a < 0$. Se obtiene que $0 < a^2$, en el primer caso aplicando el inciso (4) y en el segundo caso usando el inciso (6). ∎

Notación 6.3.7. *Denotemos por* $\mathbb{Z}^-$ *al conjunto* $\{-n \in \mathbb{Z} \mid n \in \mathbb{N} - \{0\}\}$ *y* $\mathbb{Z}^+ = \mathbb{N} - \{0\}$.

Proposición 6.3.8. *Si* $A \subseteq \mathbb{Z}^-$; $A \neq \emptyset$, *entonces A tiene máximo.*

Demostración. Sea $A \subseteq \mathbb{Z}^-$. Entonces $-A = \{-n \in \mathbb{Z} \mid n \in A\} \subseteq \mathbb{N}$ ya que para todo $x \in A$, $x < 0$ y por lo tanto $-x > 0$ y por el corolario 6.3.4, entonces $-x \in \mathbb{N}$. Por el principio del buen orden, como $\emptyset \neq -A \subseteq \mathbb{N}$, entonces $-A$ tiene mínimo $a_0 = -x_0$ donde $x_0 \in A$. Luego $a_0 = -x_0 \leq -x$ para todo $x \in A$, y por el inciso (5) de la proposición 6.3.6, entonces $x \leq x_0$ para todo $x \in A$, lo que significa que x_0 es le máximo de A. ∎

Proposición 6.3.9. *Si* $\emptyset \neq A \subseteq \mathbb{N}$ *y A es finito, entonces A tiene máximo.*

Demostración. Sea $A' = \{y \in \mathbb{N} \mid x < y \ \forall\ x \in A\}$. Entonces $0 \notin A'$ y $A' \neq \varnothing$ ya que si $A = \{x_1, \ldots, x_n\}$, entonces $y = x_1 + \cdots + x_n + 1 \in A'$. Sea $y_0 = \min A'$. Debe ser $y_0 \neq 0$.
Afirmamos que $y_0 - 1$ es el máximo de A.
Como $x < y_0$ para toda $x \in A$, entonces $x \leq y_0 - 1$ para toda $x \in A$.
Por otra parte, $y_0 - 1 \in A$, pues si $y_0 - 1 \notin A$, entonces $y_0 - 1 \in A'$, y esto contradice que y_0 es el mínimo de A'. Luego $y_0 - 1$ es el máximo de A. ∎

Corolario 6.3.10. *Si $\varnothing \neq A \subseteq \mathbb{Z}$ y A es finito, entonces A tiene mínimo y máximo.*

Demostración. Es consecuencia de las proposiciones 6.3.8 y 6.3.9. ∎

Definición 6.3.11. *Un elemento x de un anillo $(R; +, \cdot)$ es una* ***unidad*** *si existe $x' \in R$ tal que $x \cdot x' = 1$.*

Proposición 6.3.12. *Un entero x es una unidad si y sólo si $x = 1$ o $x = -1$.*

Demostración.

⇒) Supongamos que x es una unidad. Entonces existe $x' \in \mathbb{Z}$ tal que $x \cdot x' = 1$. Evidentemente $x \neq 0$ y $x' \neq 0$. Si $x > 0$, entonces debe ser $x' > 0$, ya que si no se tendría $1 = x \cdot x' < 0$.
Ahora supongamos $x > 1$. Luego $1 = x \cdot x' > x'$ y que es un absurdo (corolario 2.1.15). Concluimos que $x = 1$. El caso en que $x < 0$ se demuestra de manera similar. (ejercicio 6.3.5)

⇐) Es claro que si $x = 1$ o $x = -1$, entonces $x \cdot x = 1 \cdot 1 = 1$ o $x \cdot x = (-1) \cdot (-1) = 1$. ∎

Teorema 6.3.13. *Sean $x_1, x_2, \ldots, x_n, y \in \mathbb{Z}$. Entonces*

(1) $\min\{x_1, x_2, \ldots, x_n\} + y = \min\{x_1 + y, x_2 + y, \ldots, x_n + y\}$,
(2) $\max\{x_1, x_2, \ldots, x_n\} + y = \max\{x_1 + y, x_2 + y, \ldots, x_n + y\}$,
(3) *Si* $0 \leq y$, *entonces* $y \cdot \min\{x_1, x_2, \ldots, x_n\} = \min\{x_1 \cdot y, x_2 \cdot y, \ldots, x_n \cdot y\}$,
(4) *Si* $y \leq 0$, *entonces* $y \cdot \min\{x_1, x_2, \ldots, x_n\} = \max\{x_1 \cdot y, x_2 \cdot y, \ldots, x_n \cdot y\}$,
(5) *Si* $0 \leq y$, *entonces* $y \cdot \max\{x_1, x_2, \ldots, x_n\} = \max\{x_1 \cdot y, x_2 \cdot y, \ldots, x_n \cdot y\}$,
(6) *Si* $y \leq 0$, *entonces* $y \cdot \max\{x_1, x_2, \ldots, x_n\} = \min\{x_1 \cdot y, x_2 \cdot y, \ldots, x_n \cdot y\}$.

Demostración. Demostraremos (1), (3) y (6) y dejando como ejercicios las demostraciones de (2), (4) y (5). (ver ejercicio 6.3.6)

Por el corolario 6.3.10, todos los subconjuntos dados en los incisos (1) a (6), por ser finitos, tienen mínimo y máximo.
Sea $x_i = \text{mín}\{x_1, x_2, \ldots, x_n\}$ y $x_j = \text{máx}\{x_1, x_2, \ldots, x_n\}$.

(1) $x_i \leq x_k$ para toda $k = 1, \ldots, n$ implica, por (2) de la proposición 6.3.6, $x_i + y \leq x_k + y$ para toda $k = 1, \ldots, n$ y por lo tanto

$$\text{mín}\{x_1 + y, x_2 + y, \ldots, x_n + y\} = x_i + y = \text{mín}\{x_1, x_2, \ldots, x_n\} + y.$$

(3) $x_i \leq x_k$ para toda $k = 1, \ldots, n$ implica, por (4) de la proposición 6.3.6, por ser $0 \leq y$, que $y \cdot x_i \leq y \cdot x_k$ para todo $k = 1, \ldots, n$. Por lo tanto

$$\text{mín}\{x_1 \cdot y, x_2 \cdot y, \ldots, x_n \cdot y\} = y \cdot x_i = y \cdot \text{mín}\{x_1, x_2, \ldots, x_n\}.$$

(6) $x_k \leq x_j$ para toda $k = 1, \ldots, n$ implica, por (6) de la proposición 6.3.6 que $y \cdot x_j \leq y \cdot x_k$ para toda $k = 1, \ldots, n$, ya que $y \leq 0$. Por lo tanto,

$$\text{mín}\{x_1 \cdot y, x_2 \cdot y, \ldots, x_n \cdot y\} = y \cdot x_j = y \cdot \text{máx}\{x_1, x_2, \ldots, x_n\}.$$ ∎

Por último, definimos el valor absoluto de un número entero.

Definición 6.3.14. *Dado un número entero a, su* **valor absoluto**, *denotado por* $\boldsymbol{|a|}$ *es* $|a| = max\{a, -a\}$.

Proposición 6.3.15. *Para todo número entero a se tiene*

$$|a| = \begin{cases} a & si \;\; a \geq 0 \\ -a & si \;\; a < 0. \end{cases}$$

Demostración. Recordamos que $-n \leq n$ para toda $n \in \mathbb{N}$.

1°/ Si $a \geq 0$, entonces $|a| = \text{máx}\{a, -a\} = a$.
2°/ Si $a < 0$, entonces $-a > 0$ y así $|a| = \text{máx}\{a, -a\} = -a$. ∎

Teorema 6.3.16. *Sean $a, b, c \in \mathbb{Z}$. Entonces*

(1) $|a| \geq 0$ *y* $|a| = 0$ *si y sólo si* $a = 0$.
(2) $|a| = |-a|$, $a \leq |a|$.
(3) $|a \cdot b| = |a| \cdot |b|$.
(4) *Si* $b \geq 0$, *entonces* $|a| \leq b$ *si y sólo si* $-b \leq a \leq b$.
(5) $|a + b| \leq |a| + |b|$.
(6) $a + |a| \geq 0$.

Demostración. Demostraremos (3), (4) y (5) quedando como ejercicio (1), (2) y (6). (ver ejercicio 6.3.7)

(3) Demostraremos la igualdad $|a \cdot b| = |a| \cdot |b|$ considerando los distintos casos que se pueden presentar.
(i) Si $a \geq 0$ y $b \geq 0$, entonces $a \cdot b \geq 0$. Luego $|a \cdot b| = a \cdot b = |a| \cdot |b|$.
(ii) Si $a \leq 0$ y $b \leq 0$, entonces $a \cdot b \geq 0$ por la proposición 6.3.6. Luego

$$|a \cdot b| = a \cdot b = (-a) \cdot (-b) = |a| \cdot |b|.$$

(iii) Si $a \geq 0$ y $b \leq 0$, entonces $a \cdot b \leq 0$. Luego $|a| \cdot |b| = a \cdot (-b) = -(a \cdot b) = |a \cdot b|$. El último caso a considerar es cuando $a \leq 0$ y $b \geq 0$ y su demostración es totalmente similar al caso (iii).

(4) Supongamos que $b \geq 0$.
$\Longrightarrow$) Si $|a| \leq b$, entonces, ya que $a \leq |a|$ y $-a \leq |a|$, se tiene que $a \leq b$ y $-a \leq b$, y multiplicando por (-1) la segunda desigualdad obtenemos $-b \leq a$ y de aquí obtenemos $-b \leq a \leq b$.
$\Longleftarrow$) Si $-b \leq a \leq b$, entonces $-b \leq a$ y $a \leq b$ y de aquí obtenemos, multiplicando la primera desigualdad por (-1), que $-a \leq b$ y $a \leq b$, entonces $|a| \leq b$ debido a que $|a| = a$ o $|a| = -a$.

(5) Como $-|a| \leq a \leq |a|$ y $-|b| \leq b \leq |b|$ (ejercicio 6.3.2), sumando ambas desigualdades obtenemos $-(|a| + |b|) \leq a + b \leq (|a| + |b|)$ y por el inciso (4) de este mismo teorema, llegamos a que $|a + b| \leq |a| + |b|$. ∎

§§ Ejercicios sección 6.1.

6.1.1. [1] Sean $a, b, c \in \mathbb{Z}$. Demuestre que
(2) $(a + b) + c = a + (b + c)$ (propiedad asociativa)
(3) $a + b = b + a$ (propiedad conmutativa)

6.1.2. [2] Sean $a, b, c \in \mathbb{Z}$. Entonces
(1) Para cada uno de los siguientes casos, con $m, n, r \in \mathbb{N}$
(a) $a = -m$, $b = -n$ y $c = r$.
(b) $a = -m$, $b = n$ y $c = -r$.
(c) $a = m$, $b = -n$ y $c = r$.
(d) $a = -m$, $b = n$ y $c = r$.
Demuestre que $a \cdot b = b \cdot a$ (propiedad conmutativa)
(2) $a \cdot b = b \cdot a$ (propiedad conmutativa)
(3) $a \cdot 1 = a$ (existencia de neutro multiplicativo)

[1] Parte del Teorema 6.1.3 pág. 221.
[2] Parte del Teorema 6.1.5 pág. 222.

(4) Para cad a uno de los siguientes casos, con $m, n, r \in \mathbb{N}$
(a) $a = m$, $b = -n$ y $c = r$.
(b) $a = -m$, $b = n$ y $c = r$.
(c) $a = -m$, $b = n$ y $c = -r$.
(d) $a = -m$, $b = -n$ y $c = r$.
(e) $a = m$, $b = n$ y $c = r$.
(f) $a = -m$, $b = -n$ y $c = -r$.
Demuestre que $a \cdot (b + c) = a \cdot b + a \cdot c$ (ley distributiva del producto respecto a la suma)

6.1.3. Dé una función biyectiva entre $\mathbb{N}$ y $\mathbb{Z}$.

6.1.4. Sea h la función de $\mathbb{Z}$ en $\mathbb{Z}$ tal que, para todo $n \in \mathbb{Z}$, $h(n) = n + 1$. Muestre que h es inyectiva.

6.1.5. Para cada uno de los siguientes enunciados dé un contraejemplo para mostrar su falsedad.

(1) Si $a, b, c \in \mathbb{Z}$ y $ac = bc$, entonces $a = b$.
(2) Si $A \subseteq \mathbb{Z}$ cumple que
(I) $0 \in A$.
(II) $n \in A$, implica $n + 1 \in A$.
entonces $A = \mathbb{Z}$.

6.1.6. Sea $A \subseteq \mathbb{Z}$ tal que

(1) $0 \in A$.
(2) $n \in A$, implica $n + 1 \in A$.
(3) $n \in A$, implica $n - 1 \in A$.

Muestre que $A = \mathbb{Z}$.

6.1.7. Sea $A \subseteq \mathbb{Z}$ tal que

(1) $0 \in A$.
(2) $n \in A$, implica $n + 1 \in A$.
(3) $n \in A$, implica $-n \in A$.

Muestre que $A = \mathbb{Z}$.

6.1.8. Sea $A \subseteq \mathbb{Z}$ tal que

(1) $A \neq \emptyset$
(2) $n \in A \iff n + 1 \in A$

Muestre que $A = \mathbb{Z}$.

§§ Ejercicios sección 6.2.

6.2.1. [3] Sea $(R;+,\cdot)$ un anillo y sean $a,b,c,d \in R$. Entonces

(1) $a-a=0$,
(3) $(a-b)+(c-d)=(a+c)-(b+d)$,
(5) $(a-b)\cdot(c-d)=(a\cdot c+b\cdot d)-(a\cdot d+b\cdot c)$.

6.2.2. Sea $(R,+,\cdot)$ un anillo y a,b,c,d elementos de R. Establezca las propiedades de anillo que se usan para demostrar los siguientes resultados.

(1) $(a+b)+c=b+(c+a)$
(2) $c(d+b)+ab=(a+c)b+cd$
(3) $d+a(c+c)=ab+(d+ac)$
(4) $a(bc)+(ab)d=ab(d+c)$

6.2.3. Sea $A=\mathbb{Z}\times\mathbb{Z}$. Defínase
$$\begin{aligned}(a_1,b_1)+(a_2,b_2) &= (a_1+a_2,b_1+b_2)\\ (a_1,b_1)\cdot(a_2,b_2) &= (a_1\cdot a_2,b_1\cdot b_2)\end{aligned}$$

(1) Muestre que $(A,+,\cdot)$ es un anillo.
(2) ¿Es éste un anillo conmutativo?
(3) ¿Es un dominio entero?

6.2.4. Sean R y S anillos. Defínase en $R\times S$

$$\begin{aligned}(r_1,s_1)+(r_2,s_2) &= (r_1+r_2,s_1+s_2)\\ (r_1,s_1)\cdot(r_2,s_2) &= (r_1\cdot r_2,s_1\cdot s_2)\end{aligned}$$

Muestre que

(1) $(R\times S,+,\cdot)$ es un anillo.
(2) $R\times S$ es un anillo conmutativo si y sólo si R y S son conmutativos.
(3)

6.2.5. Sea $R=\mathbb{Z}\times\mathbb{Z}$. Defínase

$$\begin{aligned}(x_1,y_1)+(x_2,y_2) &= (x_1+x_2,y_1+y_2)\\ (x_1,y_1)\cdot(x_2,y_2) &= (x_1\cdot x_2-y_1\cdot y_2,x_1y_2+x_2y_1)\end{aligned}$$

Muestre que $(R,+,\cdot)$ es un dominio entero.

[3] Parte del Teorema 6.2.11 pág. 227.

6.2.6. Consideremos el conjunto $\mathbb{Z}$ con las operaciones binarias $\oplus$ y $\odot$, definidas por

$$x \oplus y = x + y - 1, \qquad x \odot y = x + y - xy,$$

para cualesquiera $x, y \in \mathbb{Z}$.
Conteste las siguientes preguntas justificando sus respuestas:

(1) ¿es $(\mathbb{Z}, \oplus, \odot)$ un anillo?
(2) si sí es un anillo, ¿es conmutativo?
(3) si sí es anillo, ¿es un dominio entero?

6.2.7. Defina las operaciones binarias $\oplus$ y $\odot$ en $\mathbb{Z}$ como

$$x \oplus y = x + y - 7, \qquad x \odot y = x + y - 3xy,$$

para cualesquiera $x, y \in \mathbb{Z}$.
Explique por qué $(\mathbb{Z}, \oplus, \odot)$ no es un anillo.

6.2.8. Sean k, m enteros fijos. Encuentre todos los valores de k, m para los que $(\mathbb{Z}, \oplus, \odot)$ es un anillo con las operaciones binarias

$$x \oplus y = x + y - k, \qquad x \odot y = x + y - mxy,$$

para cualesquiera $x, y \in \mathbb{Z}$.

6.2.9. Sea A un conjunto y considere $\mathcal{P}(A)$ (el conjunto potencia de A). Definimos

$$\oplus : \mathcal{P}(A) \times \mathcal{P}(A) \longrightarrow \mathcal{P}(A) \quad y \quad \odot : \mathcal{P}(A) \times \mathcal{P}(A) \longrightarrow \mathcal{P}(A)$$

de la siguiente manera:

$$B \oplus C = (B - C) \cup (C - B) \quad \text{y} \quad B \odot C = B \cap C.$$

Conteste las siguientes preguntas justificando sus respuestas:

(1) ¿es $(\mathcal{P}(A), \oplus, \odot)$ un anillo?
(2) si sí es un anillo, ¿es conmutativo?
(3) si sí es anillo, ¿cuál es el?

6.2.10. Con las notaciones del ejercicio anterior, para el conjunto A, conserve $B \odot C = B \cap C$ pero defina $B \oplus C = A \cup B$. ¿Es $(\mathcal{P}(A), \oplus, \odot)$ un anillo?

6.2.11. Las tablas de abajo hacen de $(R, +, \cdot)$ un anillo, donde $R = \{s, t, x, y\}$.

$+$	s	t	x	y
s	y	x	s	t
t	x	y	t	s
x	s	t	x	y
y	t	s	y	x

$\cdot$	s	t	x	y
s	y	y	x	x
t	y	y	x	x
x	x	x	x	x
y	x	x	x	x

(1) ¿Cuál es el cero de este anillo?
(2) ¿Cuál es el inverso aditivo de cada elemento?
(3) ¿A qué elemento equivale $t(s + xy)$?
(4) ¿Es un anillo conmutativo?
(5) ¿Es un anillo con uno?
(6) Encuentre un par de divisores de cero.

6.2.12. Para $R = \{s, t, x, y\}$ defina + y $\cdot$ mediante la tabla

$+$	s	t	x	y
s	s	t	x	y
t	t	s	y	x
x	x	y	s	t
y	y	x	t	s

y la tabla parcial

$\cdot$	s	t	x	y
s	s	s	s	s
t	s	t		
x	s	t		y
y	s		s	

Eso hace de R un anillo.

(1) Use las propiedades de asociatividad y distributividad para completar la tabla del producto.
(2) ¿Es conmutativo este anillo ?
(3) ¿Es un anillo con uno? ¿Qué ocurre con las unidades?
(4) ¿Es este anillo un dominio entero?.

6.2.13. Muestre que $(\mathbb{Z}, +, \odot)$ es un anillo si definimos $a \odot b = 0$ para todo $a, b \in \mathbb{Z}$.

6.2.14. Muestre que $a^2 - b^2 = (a + b)(a - b)$ para todas las a y b en un anillo R si y sólo si R es conmutativo.

6.2.15. Sea $(R, +, \cdot)$ un anillo. Muestre que $R = \{0\}$ si y sólo si $1 = 0$.

6.2.16. Sea $(R, +, \cdot)$ un anillo tal que $a^2 = a \cdot a = a$. Demuestre que

(1) Para todo $a \in R$, $a + a = 0$.
(2) R es un anillo conmutativo.

6.2.17. Sea $(R, +, \cdot)$ un anillo con más de un elemento que cumple que para toda $a \in R$ con $a \neq 0$ existe un único $b \in R$ tal que $a \cdot b \cdot a = a$. Demuestre que

(1) R es un dominio entero.
(2) Si $a \in R$, $a \neq 0$ y b es el único tal que $a \cdot b \cdot a = a$, entonces $b \cdot a \cdot b = b$.
(3) R es un anillo con uno.

6.2.18. Sea $(R, +, \cdot)$ un dominio entero con uno. Si $x^2 = 1$ para algún $x \in R$, entonces $x = \pm 1$.

6.2.19. Sea $(R, +, \cdot)$ un dominio entero. Suponga que existe un elemento $a \in R$, $a \neq 0$, tal que $a^2 = a \cdot a = a$. Muestre que R es un anillo con uno. (cuidado de tomar como hipótesis la existencia del neutro multiplicativo)

6.2.20. (1) Los principiantes en álgebra escriben frecuentemente

$$(x + y)^2 = x^2 + y^2.$$

Dé un anillo $(R, +, \cdot)$ para el que sea cierto que $(x + y)^2 = x^2 + y^2$, cualesquiera que sean $x, y \in R$.
(2) Sea $(R, +, \cdot)$ un anillo tal que $(x + y)^2 = x^2 + y^2$, para todo $x, y \in R$. Muestre que

(I) $xy = -yx$ para todo $x, y \in R$.
(II) $x^2 + x^2 = 0$ para todo $x \in R$.
(III) Si R es un anillo con uno, entonces $x + x = 0$, para todo $x \in R$.

6.2.21. El conjunto de matrices de 2×2 sobre $\mathbb{Z}$ es el conjunto

$$M_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \quad a, b, c, d \in \mathbb{Z} \right\}$$

En $M_2(\mathbb{Z})$, dos matrices son iguales si sus elementos correspondientes son iguales en $\mathbb{Z}$.
Definimos + y $\cdot$ como

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}, \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$$

(1) Muestre que $(M_2(\mathbb{Z}), +, \cdot)$ es un anillo.

(2) ¿Es este un anillo con uno?
(3) ¿Es un anillo conmutativo?
(4) ¿Es un dominio entero?

§§ Ejercicios sección 6.3.

6.3.1. Demuestre que $A = \{-n \mid n \in \mathbb{N}\}$ no tiene elemento mínimo.

6.3.2. Sea $a \in \mathbb{Z}$. Demuestre que $-|a| \leq a \leq |a|$.

6.3.3. [4] Sean $a, b, c, d \in \mathbb{Z}$.

(1) $a \leq b$ si y sólo si $-b \leq -a$.
(2) Si $a < b$, entonces $a + c < b + c$ $\quad (a \leq b \Longrightarrow a + c \leq b + c)$.
(4) Si $a < b$ y $0 < c$, entonces $a \cdot c < b \cdot c$ $\quad (a \leq b, 0 \leq c \Longrightarrow a \cdot c \leq b \cdot c)$.

6.3.4. Sean $x, y, z, w \in \mathbb{Z}$. Muestre que

(1) Si $x < y$, entonces $x + z < y + z$.
(2) Si $x \leq y$, entonces $x + z \leq y + z$.
(3) Si $x < y$ y $0 < z$, entonces $x \cdot z < y \cdot z$.
(4) Si $x \leq y$ y $0 \leq z$, entonces $x \cdot z \leq y \cdot z$.
(5) Si $x < y$ entonces $-y < -x$.
(6) Si $x \leq y$ entonces $-y \leq -x$.
(7) Si $0 \leq x < y$, entonces $x^n < y^n$ para todo $n \in \mathbb{N}$.
(8) Si $0 \leq x \leq y$, entonces $x^n \leq y^n$ para todo $n \in \mathbb{N}$.
(9) Si $x < y$, entonces $z - y < z - x$.
(10) Si $x \leq y$, entonces $z - y \leq z - x$.
(11) Si $z, w \in \mathbb{Z} - \{0\}$ y $x \cdot z^2 = y \cdot w^2$, entonces $x > 0$ si y sólo si $y > 0$.
(12) $2xy \leq x^2 + y^2$.
(13) Si $x \neq y$, entonces $2xy < x^2 + y^2$
(14) $(xy + zw)^2 \leq (x^2 + z^2)(y^2 + w^2)$.
Sugerencia: Muestre que $[(x^2 + z^2)(y^2 + w^2) - (xy + zw)^2] \geq 0$.

6.3.5. Demuestre que si $x \in \mathbb{Z}$ es una unidad en $\mathbb{Z}$ y $0 < x$, entonces $x = -1$.

6.3.6. [5] Sean $x_1, x_2, \ldots, x_n, y \in \mathbb{Z}$. Entonces

(1) $\text{máx}\{x_1, x_2, \ldots, x_n\} + y = \text{máx}\{x_1 + y, x_2 + y, \ldots, x_n + y\}$,
(2) Si $y \leq 0$, entonces $y \cdot \text{mín}\{x_1, x_2, \ldots, x_n\} = \text{máx}\{x_1 \cdot y, x_2 \cdot y, \ldots, x_n \cdot y\}$,

[4] Parte de la proposición 6.3.6 pág. 231.
[5] Parte del teorema 6.3.13 pág. 233.

(3) Si $0 \leq y$, entonces $y \cdot \max\{x_1, x_2, \ldots, x_n\} = \max\{x_1 \cdot y, x_2 \cdot y, \ldots, x_n \cdot y\}$,

6.3.7. [6] Sean $a, b, c \in \mathbb{Z}$. Entonces

(1) $|a| \geq 0$ y $|a| = 0$ si y sólo si $a = 0$.
(2) $|a| = |-a|$, $a \leq |a|$.
(3) $a + |a| \geq 0$.

6.3.8. Sean $u, v, x \in \mathbb{Z}$ tales que $0 \leq u \leq v$. Muestre que

(1) $u^2 \leq x^2 \leq v^2 \iff (u \leq x \leq v \ \vee \ -v \leq x \leq -u)$;
(2) $u^2 < x^2 < v^2 \iff (u < x < v \ \vee \ -v < x < -u)$.

6.3.9.

(1) Sea f una función estrictamente creciente de $\mathbb{N}$ en $\mathbb{N}$, es decir, $f : \mathbb{N} \to \mathbb{N}$ es tal que, para todo $n, m \in \mathbb{N}$, si $n < m$, entonces $f(n) < f(m)$. Concluya que para todo $n \in \mathbb{N}$, $n \leq f(n)$.
(2) Compruebe que el inciso anterior sería falso si en vez de $\mathbb{N}$ habláramos del conjunto $\mathbb{Z}$ de todos los números enteros. Para ello defina una función estrictamente creciente $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ tal que para todo $n \in \mathbb{Z}$ $f(n) < n$.

6.3.10. Encuentre el conjunto solución en $\mathbb{Z}$ de cada una de las siguientes desigualdades.

(1) $2x \leq 5$.
(2) $3x + 7 < 8$.
(3) $5 < 2x \leq 9$.
(4) $-6 \geq 4x + 1 \geq -8$.
(5) $3 \leq 5x + 2 < 6$.
(6) $x(x + 3) > 0$.
(7) $(x - 5)(x + 2) \geq 0$.
(8) $x^2 + 3x + 4 \geq 2$.
(9) $x^2 + 5x + 6 \leq 2$.
(10) $x^2 + 2x + 1 \leq 0$.

6.3.11. Sean $a, b, c \in \mathbb{Z}$. Demuestre que el valor absoluto es una función que satisface las propiedades siguientes:

(1) $|a| = |-a|$.
(2) $|a| \geq 0$ y $|a| = 0$ si y sólo si $a = 0$.

[6] Parte del teorema 6.3.16 pág. 234.

(3) $\pm a \leq |a|$.
(4) $|a^2| = a^2$.
(5) $a + |a| \geq 0$.
(6) $|a + b + c| \leq |a| + |b| + |c|$.
(7) $|a| - |b| \leq |a - b| \leq |a| + |b|$.
(8) Sea $c > 0$. Entonces $|a - b| < c$ si y sólo si $b - c < a < b + c$.

6. 3.12. Encuentre el conjunto solución en $\mathbb{Z}$ de cada una de las siguientes desigualdades (o ecuaciones).

(1) $|x + 3| = 7$.
(2) $|x + 5| = 0$.
(3) $|x - 2| = -2$.
(4) $|x| < 4$.
(5) $|x + 5| < 3$.
(6) $|2x - 8| \leq 5$.
(7) $|5x - 1| \leq 2$.
(8) $2 < |x| < 5$.
(9) $1 \leq |2x + 3| < 4$.
(10) $5 < |2x + 1| \leq 6$.
(11) $1 < 3|x|$.
(12) $|x^2 + 2| \geq 1$.

6.3.13. Sea $A \subseteq \mathbb{Z}$ con $A \neq \emptyset$. Muestre que

(1) Si A tiene una cota superior, entonces A tiene un elemento máximo.
(2) Si A tiene una cota inferior, entonces A tiene un elemento mínimo.

6.3.14. Sea $(R, +, \cdot)$ un anillo conmutativo. Se dice que un subconjunto R^+ de R es una **clase positiva** de R si cumple lo siguiente:

(1) $0 \in R^+$.
(2) Si $x, y \in R^+$, entonces $x + y \in R^+$ y $x \cdot y \in R^+$.
(3) Si $x \in R^+$, $x \neq 0$, entonces $x \in R^+$ ó $-x \in R^+$.

Para los siguiente suponga que $(R, +, \cdot)$ es un anillo conmutativo.

(1) Muestre que si R contiene un subconjunto positivo R^+, entonces R es un dominio entero.
(2) Si R es un dominio entero que contiene un subconjunto positivo R^+, muestre que $\{R^+, \{0\}, -R^+\}$ es una partición de R.

6.3.15. Se dice que un dominio entero $(R, +, \cdot)$ es un **dominio entero ordenado** si existe un orden total $(\leq)$ en R tal que para todo $x, y, z \in R$:

(1) Si $x \leq y$, entonces $x + z \leq y + z$.
(2) Si $z \geq 0$ y $x \leq y$, entonces $z \cdot x \leq z \cdot y$.

¿Es $(\mathbb{Z}; +, *)$ un dominio entero ordenado?

6.3.16.

(1) Sea $(R, +, \cdot)$ un dominio entero que contiene un subconjunto positivo R^+. Muestre que $(R, +, \cdot)$ es un dominio entero ordenado si se define el orden como sigue:
$$x \leq y \iff (y - x \in R^+ \ \vee \ y = x).$$
(2) Sea $(R, +, \cdot)$ un dominio entero ordenado con orden total $\leq$. Muestre que el subconjunto de R, $\{x \mid x > 0\}$, es un subconjunto positivo de R.

Es imposible encontrar la forma de convertir un cubo en la suma de dos cubos, una potencia cuarta en la suma de dos potencias cuartas, o en general cualquier potencia más alta que el cuadrado, en la suma de dos potencias de la misma clase. He descubierto para el hecho una demostración excelente. Pero este margen es demasiado pequeño para que (la demostración) quepa en él.
Pierre de Fermat
1601 - 1665

***Capítulo* 7**

Teoría de números

La teoría de números es una de las ramas más antiguas de la matemática. Y en sus inicios las contribuciones más significativas fueron hechas por los griegos, indus y chinos. Entre sus exponentes más importantes se encuentran Fermat, Euler y Gauss. En la teoría de números clásica se estudian las propiedades de los números enteros respecto a la suma y el producto, siendo un concepto básico la divisibilidad y con él comenzamos este capítulo.

§ 7.1. Divisibilidad

Definición 7.1.1*. Dados los enteros a y b, diremos que* ***a*** **divide a** ***b*** *o que b es divisible por a si existe un entero r tal que* $a \cdot r = b$.

Notación 7.1.2*. Si a divide a b lo denotamos por* $\boldsymbol{a \mid b}$ *y si a no divide a b lo denotamos* $\boldsymbol{a \nmid b}$

Ejemplo 7.1.3. $3 \mid 6$ ya que $3 \cdot 2 = 6$. También $-3 \mid 6$ pues $(-3)(-2) = 6$.

Ejemplo 7.1.4. Para cualquier entero a, $a \mid 0$ debido a que $a \cdot 0 = 0$. Nótese que a puede ser 0 y quizá esto pueda parecer extraño pues desde muy temprano en la escuela se enseña que no se puede dividir por cero. Sin embargo, una cosa es la definición que hemos dado $0 \mid 0$ y otra la expresión $\frac{0}{0}$ que no está permitida y que más adelante se aclarará de manera más puntual.

Veamos algunas propiedades que son inmediatas de la definición

Teorema 7.1.5. *Sean* $a, b, c \in \mathbb{Z}$.

(1) $1 \mid a$ *y* $-1 \mid a$.
(2) $a \mid a$. *En particular* $0 \mid 0$.
(3) *Si* $a \mid b$, *entonces* $-a \mid b$, $a \mid -b$ *y* $-a \mid -b$.
(4) $a \mid 0$.
(5) *Si* $0 \mid a$, *entonces* $a = 0$ *(el único elemento que es divisible por cero es cero).*
(6) *Si* $a \mid b$ *y* $b \mid c$, *entonces* $a \mid c$.
(7) *Si* $a \mid b$ *y* $a \mid c$, *entonces* $a \mid b + c$.
(8) *Si* $a \mid b$, *entonces* $a \mid b \cdot c$.
(9) *Si* $a \mid b$, *entonces* $a \cdot c \mid b \cdot c$.
(10) *Si* $a \mid b$ *y* $a \mid c$, *entonces* $a \mid b \cdot x + c \cdot y$ *para cualesquiera* $x, y \in \mathbb{Z}$.
(11) *Si* $a \mid b$ *y* $b \neq 0$, *entonces* $|a| \leq |b|$.
(12) *Si* $a \mid b$ *y* $b \mid a$, *entonces* $a = b$ *o* $a = -b$ *(esto es* $|a| = |b|$*).*

Demostración. Como se puede ver, (10) es consecuencia inmediata de (7) y (8) y el inciso (12) es consecuencia de (11). Demostraremos (6), (7), (8) y (11) y los restantes quedan como ejercicio, véase ejercicio 7.1.1.

(6) Supongamos que $a \mid b$ y $b \mid c$. Entonces existen $r, s \in \mathbb{Z}$ tales que $a \cdot r = b$ y $b \cdot s = c$. Multiplicando por s la primera igualdad obtenemos $a \cdot (r \cdot s) = b \cdot s = c$, luego $a \mid c$.
(7) Si $a \mid b$ y $a \mid c$, entonces existen $r, s \in \mathbb{Z}$ tales que $a \cdot r = b$ y $a \cdot s = c$. Sumando ambas igualdades $a(r + s) = b + c$ por lo que $a \mid b + c$.
(8) Si $a \mid b$, entonces $a \cdot r = b$ para alguna $r \in \mathbb{Z}$. Multiplicando por c a ambos lados, $a \cdot (r \cdot c) = b \cdot c$ y así $a \mid b \cdot c$.
(11) Si $a \mid b$, entonces para alguna $r \in \mathbb{Z}$ $a \cdot r = b$ y de aquí $|a| \cdot |r| = |b|$ y como $r \neq 0$, debido a que $b \neq 0$, por el ejercicio 2.1.5, se tiene que $|a| \leq |b|$. ∎

Nota 7.1.6. El inciso (3) del teorema 7.1.5 nos dice que el signo es irrelevante en la divisibilidad.

Proposición 7.1.7. *Si* $a, b \in \mathbb{Z}$ *con* $a \neq 0$ *y* $a \mid b$, *entonces el entero* c *tal que* $a \cdot c = b$ *es único.*

Demostración. Supongamos que $a \cdot c = a \cdot c' = b$. Entonces $a \cdot (c - c') = 0$ y ya que $\mathbb{Z}$ es un dominio entero y $a \neq 0$, se debe tener $c - c' = 0$, es decir, $c = c'$. ∎

Nota 7.1.8. En el caso en que $a \mid b$ y $a \neq 0$, el entero r tal que $a \cdot r = b$, que sabemos es único por la proposición 7.1.7, lo denotamos por $\frac{b}{a}$. Esto es, si $a \neq 0$

y $a \mid b$, $\frac{b}{a}$ ***denotará al único entero tal que*** $\boldsymbol{a \cdot \frac{b}{a} = b}$. ¿Por qué pedimos $a \neq 0$?, pues porque si $a = 0$ y $0 \mid b$, entonces $b = 0$ y cualquier entero r satisface $0 \cdot r = 0$ y por lo tanto $\frac{0}{0}$ no tiene sentido, aun cuando 0 divida a 0. Por otro lado, $a \cdot 0 = 0$ para todo entero a y si $a \neq 0$, entonces 0 es el único entero tal que $a \cdot 0 = 0$, así que $\frac{0}{a} = 0$, con lo que se tiene entonces que $\frac{0}{a} = \frac{0}{b}$ para cualesquiera enteros a y b distintos de cero.

Veamos a continuación un resultado al que se le conoce como algoritmo de la división. Sin embargo éste no es un algoritmo, sino más bien un teorema de existencia y es de gran importancia debido a las aplicaciones que tiene como lo veremos a lo largo de este capítulo. Antes de presentarlo necesitamos el siguiente

Lema 7.1.9. *Sean $r, r', b \in \mathbb{Z}$ tales que $b > 0$, $0 \leq r < b$ y $0 \leq r' < b$. Entonces $|r - r'| < b$.*

Demostración. Como $0 \leq r' < b$, entonces $-b < -r' \leq 0$ y sumando esta desigualdad con $0 \leq r < b$ obtenemos $-b < r - r' < b$ y por el teorema 6.3.16 inciso (4) esto último implica $|r - r'| < b$. ∎

Teorema 7.1.10. *(Algoritmo de la división) Dados los entero a y b con $b \neq 0$, existen enteros únicos q y r tales que*

$$a = b \cdot q + r \quad \textit{donde } 0 \leq r < |b|.$$

Demostración. Es suficiente considerar $a \geq 0$ y $b > 0$ ya que los casos restantes se pueden obtener de éste (véase el ejercicio 7.1.30). Queremos encontrar enteros q y r tales que $a = b \cdot q + r$, o lo que es lo mismo tal que $r = a - b \cdot q$ y $0 \leq r < b$, así que de existir es lógico que los busquemos en el conjunto $A = \{a - bx \in \mathbb{Z} \mid x \in \mathbb{Z} \text{ y } a - b \cdot x \geq 0\}$. Ahora, evidentemente $A \subseteq \mathbb{N}$ y $A \neq \varnothing$ ya que $y = a - b \cdot (-a) = a + b \cdot a \geq 0$ y $y \in A$. Por el principio del buen orden A tiene mínimo que denotaremos por r. Entonces $r = a - b \cdot q$ para alguna $q \in \mathbb{Z}$ y así $a = b \cdot q + r$. Veamos que r es la buscada, es decir, $0 \leq r < b$. Supongamos que $b \leq r$. Entonces $r = b + r'$ y como $b > 0$ se tiene que $0 \leq r' < r$. Además $r' = r - b = a - b \cdot q - b = a - b \cdot (q + 1)$ lo que significa que $r' \in A$, Luego por ser r el mínimo de A, debe se $r \leq r'$, lo que contradice que $r' < r$. Por lo tanto $a = b \cdot q + r$ con $0 \leq r < b$.

Unicidad. Supongamos que $a = b \cdot q + r = b \cdot q' + r'$ donde $0 \leq r, r' < b$. Entonces $b \cdot (q - q') = r' - r$ y por lo tanto $b \mid |r - r'|$. Pero por el lema 7.1.9, $0 \leq |r - r'| < b$,

así que la única posibilidad para que $b \mid |r - r'|$ es que $|r - r'| = 0$ y entonces también debe ser $q - q' = 0$ por ser $b \neq 0$. ∎

A los enteros q y r de éste último teorema los llamaremos ***cociente*** y ***residuo*** respectivamente.

Corolario 7.1.11. *Sean $a, b \in \mathbb{Z}$ con $b \neq 0$ y $a = b \cdot q + r$ con $0 \leq r < |b|$. Entonces $b \mid a$ si y sólo si $r = 0$. Esto es $b \mid a$ si y sólo si al aplicar el algoritmo de la división a a y b, el residuo es cero.*

Antes de ver una aplicación del algoritmo de la división necesitamos el siguiente

Lema 7.1.12. *Sean $a, b \in \mathbb{Z}$ tales que $a > 0$, $b > 1$ y $a = b \cdot q + r$ con $0 \leq r < b$. Entonces $a > q \geq 0$.*

Demostración.

$1^o/$ $q \geq 0$. Supongamos que $q < 0$: Multiplicando por b (recuérdese que $b > 0$) y al sumar r a ambos lados de la desigualdad obtenemos

$$a = b \cdot q + r < b \cdot 0 + r = r.$$

Luego existe $t > 0$ tal que $a + t = r$ (con lo cual $t < r$) y $a = b \cdot q + r = b \cdot q + a + t$. Cancelando a, se tiene $b \cdot q + t = 0$, lo que implica que $b \mid t$ y como ambos b y t son mayores que cero, entonces $b \leq t < r < b$, lo que es absurdo. Por lo tanto $q \geq 0$.

$2^o/$ Supongamos $a \leq q$. Entonces $a = b \cdot q + r \geq b \cdot q > q \geq a$, que es absurdo. Luego debe ser $q < a$. ∎

Teorema 7.1.13. *Sea $a \in \mathbb{Z}$ con $a > 1$. Entonces cada $n \in \mathbb{N} - \{0\}$ se puede expresar de manera única como*

$$n = r_k a^k + \cdots + r_1 a + r_0 a^0$$

donde $0 \leq r_i < a$ para $i = 0, \ldots, k$ y $r_k \neq 0$.

Demostración. Por inducción sobre n.

$1°/$ $n = 1$. $1 = 1 \cdot a^0$.

$2°/$ Supongamos que todo número entero m tal que $1 \leq m < n$ se puede expresar de esta manera.

Por el algoritmo de la división $n = a \cdot q + r_0$ donde $0 \leq r_0 < a$ y además por el lema 7.1.12, $n > q \geq 0$. Si $q = 0$, la expresión para n sería $n = r_0 \cdot a^0$. Si $q > 0$,

como $q < n$, por hipótesis de inducción $q = r_k \cdot a^{k-1} + \cdots + r_2 \cdot a + r_1 \cdot a$ con $0 \leq r_i < a$ para $i = 1, \ldots k$ y $r_k \neq 0$ y de aquí obtenemos que

$$n = aq + r_0 = a(r_k \cdot a^{k-1} + \cdots + r_1 \cdot a^0) + r_0 \cdot a^0,$$

con $0 \leq r_i < a$ para $i = 0, \ldots k$ y $r_k \neq 0$.

Unicidad. Nuevamente por inducción sobre n.

$1°/$ $n = 1$. Si $1 = r_k a^k + \cdots + r_1 a + r_0 a^0$, entonces debe ser $k = 0$ y $r_0 = 1$ ya que si fuera algún $r_i > 0$ con $i > 0$, entonces $r_i a^i \geq a > 1$.

$2°/$ Supongamos que $n = r_k a^k + \cdots + r_1 a + r_0 a^0 = s_t a^t + \cdots + s_1 a + s_0 a^0$, con $0 \leq r_i, s_i < a$ para todo $i = 0, \ldots, k$ y $j = 0, \ldots, t$. Entonces

$$n = \left(r_k a^{k-1} + \cdots + r_1\right) a + r_0 = \left(s_t a^{t-1} + \cdots + s_1\right) a + s_0 \text{ donde } 0 \leq r_0,\ s_0 < a$$

y por la unicidad en el algoritmo de la división,

$$q = r_k a^{k-1} + \cdots + r_1 = s_t a^{t-1} + \cdots + s_1 \ \ y \ \ r_0 = s_0.$$

Ahora, si $q = 0$, entonces $r_i = 0 = s_j$ para $1 \leq i \leq k$ y $1 \leq j \leq t$ y $r_0 = s_0$ y si $q > 0$, como $q < n$, por la hipótesis de inducción $k = t$ y $r_i = s_i$ para $i = 1, \ldots, k$. ∎

Nota 7.1.14. Dados n y $a > 1$, para obtener los valores de $r_0, \ldots, r_k$, se usa iteradamente el algoritmo de la división: $n = q \cdot a + r_0$ con $0 \leq r_0 < a$. Si $q < a$, esta es la expresión buscada, si no, $q = q_1 \cdot a + r_1$, con $0 \leq r_1 < a$ y $n = q_1 a^2 + r_1 a + r_0$ y así sucesivamente hasta obtener la expresión deseada.

Ejemplo 7.1.15. Sea $n = 273$ y $a = 5$.

$$273 = 54 \cdot 5 + 3 = (10 \cdot 5 + 4) \cdot 5 + 3 = 10 \cdot 5^2 + 4 \cdot 5 + 3 = 2 \cdot 5^3 + 4 \cdot 5 + 3.$$

Entonces $273 = 2 \cdot 5^3 + 0 \cdot 5^2 + 4 \cdot 5 + 3 \cdot 5^0$.

De acuerdo a este último teorema diremos que la representación de un número natural $n \geq 1$ en ***base a*** es $r_k r_{k-1} \cdots r_1 r_0$ si $n = r_k a^k + \cdots + a r_1 + r_0$, donde $0 \leq r_i < a$ para $i = 0, \ldots, k$ y $r_k \neq 0$ y lo denotamos $\boldsymbol{n = (r_k r_{k-1} \cdots r_1 r_0)_a}$. Observamos que los números naturales tal como los conocemos están dados en base 10, esto es dado un número natural n, $n = (n)_{10}$. Por último, por la unicidad, $(r_k \cdots r_1 r_0)_a = (s_t \cdots s_1 s_0)_a$ si y sólo si $k = t$ y $r_i = s_i$ para toda $i \in \{0, \ldots, k\}$.

Ejemplo 7.1.16. Para el número natural 4506 se tiene que

$$4506 = 4 \cdot 10^3 + 5 \cdot 10^2 + 0 \cdot 10 + 6 \cdot 10^0$$

y este mismo número en base 5 será 121011 ya que

$$4506 = 1 \cdot 5^5 + 2 \cdot 5^4 + 1 \cdot 5^3 + 0 \cdot 5^2 + 1 \cdot 5 + 1 \cdot 5^0$$

y entonces se tendrá que $4506 = (4506)_{10} = (121011)_5$.

Cuando la base a sea mayor que 10 debemos tener cuidado con la notación ya que al escribir un número en esta base en la sucesión pueden aparecer los números $10, 11, \ldots, a-1$, así que para evitar confusiones podríamos usar paréntesis cada vez que aparezca alguno de ellos o también asignarle un símbolo a cada uno de ellos, lo que es lo más recomendable cuando a no es grande. Por ejemplo si $a = 13$, la representación en base 13 de 2023 está determinado por

$$2023 = 11 \cdot 13^2 + 12 \cdot 13 + 8 \cdot 13^0$$

y entonces podríamos escribir $(2023)_{10} = ((11)(12)8)_{13}$ o también si usamos los símbolos α, β, γ para 11, 12, y 13 respectivamente en cuyo caso tenemos que $(2023)_{10} = (\alpha\beta 8)_\gamma$.

Las operaciones aritméticas, suma y producto, con los números expresados en una base distinta de 10 se realiza de manera similar a las conocidas en base 10. Por ejemplo, en base 3, la suma de $(1022)_3$ y $(211)_3$ sería

$$\begin{array}{cccccc} & 1 & 0 & 2 & 2 \\ + & & 2 & 1 & 1 \\ \hline & 2 & 0 & 1 & 0 \end{array}$$

y así $(1022)_3 + (211)_3 = (2010)_3$.

Y el producto

$$\begin{array}{cccccccc} & & & 1 & 0 & 2 & 2 \\ & & \times & & 2 & 1 & 1 \\ \hline & & & 1 & 0 & 2 & 2 \\ & & 1 & 0 & 2 & 2 & \\ & 2 & 1 & 2 & 1 & & \\ \hline 1 & 0 & 0 & 1 & 1 & 1 & 2 \end{array}$$

así $(1022)_3 \cdot (211)_3 = (1001112)_3$

De la misma manera a la usual (base 10) podemos decir cuándo dos números dados en base a, uno es menor que otro: $(r_k \cdots r_1 r_0)_a < (s_t \cdots s_1 s_0)_a$ si y sólo si $k < t$ o si $k = t$, existe $m \leq k$ tal que $r_m < s_m$ y $r_j = s_j$ para $j = m+1, \ldots, k$.

§ 7.2. Máximo común divisor y mínimo común múltiplo

Iniciaremos esta sección introduciendo el conjunto de divisores comunes de dos enteros (que después generalizaremos a un número finito de enteros) y veremos que, cuando uno de ellos es distinto de cero, este conjunto tiene máximo el cual tiene propiedades muy interesantes.
Para cada $a \in \mathbb{Z}$, denotamos por $D(a)$ al conjunto de sus divisores, esto es,

$$D(a) = \{x \in \mathbb{Z} \mid \quad x \mid a\}.$$

Veamos algunas propiedades de estos conjuntos.

(1) $D(0) = \mathbb{Z}$. Como ya hemos visto (teorema 7.1.5 inciso (4)) cualquier entero divide a cero.
(2) $\pm 1, \pm a \in D(a)$.
(3) Si $a \neq 0$, entonces $D(a)$ es finito.
Por el teorema 7.1.5 inciso (11), si $a \neq 0$ y $x \mid a$, entonces $|x| \leq |a|$ y por lo tanto x tiene un número finito de posibilidades.

Consideramos ahora el conjunto $D(a) \cap D(b)$ de divisores comunes de los enteros a y b. Como $1 \in D(a)$ para todo $a \in \mathbb{Z}$, $D(a) \cap D(b) \neq \varnothing$ para cualesquiera a y b. Si $a \neq 0$ o $b \neq 0$, entonces $D(a) \cap D(b)$ es finito y por lo tanto tiene máximo (corolario 6.3.10) y las propiedades que lo determinan son las siguientes:

§ §7.2.1. Máximo común divisor.

Definición 7.2.1*. Dados dos enteros a y b, no ambos cero, su* **máximo común divisor** *es el entero d que satisface*

(i) $d \mid a$ y $d \mid b$ (d es un divisor común de a y b)
(ii) Si $d' \mid a$ y $d' \mid b$, entonces $d' \leq d$ (d es el máximo de los divisores comúnes)

Nota 7.2.2. Como consecuencia de la definición tenemos que deber ser $d \geq 1$ ya que $1 \in D(a) \cap D(b)$ para cualquier pareja de enteros a y b.

Al máximo común divisor de a y b lo denotamos por $\boldsymbol{(a, b)}$.

Ejemplo 7.2.3. Sean $a = 30$ y $b = 42$.

$$D(a) = \{\pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 10, \pm 15, \pm 30\} \text{ y } D(b) = \{\pm 1, \pm 2, \pm 3, \pm 6, \pm 7, \pm 14, \pm 21, \pm 42\}.$$

Entonces $D(a) \cap D(b) = \{\pm 1, \pm 2, \pm 3, \pm 5, \pm 6\}$. Por lo tanto el máximo común divisor de 30 y 42 es 6, esto es, $(30, 42) = 6$.

Nota 7.2.4. **m.c.d.** significará máximo común divisor.

Más adelante veremos que la propiedad (3) en la definición de m.c.d. se puede sustituir por otra más fuerte.
Las siguientes son algunas propiedades inmediatas del m.c.d.

Proposición 7.2.5. *San $a, b \in \mathbb{Z}$ con $a \neq 0$ o $b \neq 0$. Entonces*

(1) $(a, b) = (b, a)$
(2) $(a, b) = (|a|, |b|)$
(3) $(a, b) = |a|$ *si y sólo si* $a \mid b$. *En particular* $(a, 0) = |a|$ *para* $a \neq 0$.

La demostración de estas propiedades son muy sencillas y las dejamos como ejercicio. (ejercicio 7.2.1)
Debido a que $(a, b) = (|a|, |b|)$, en nuestro estudio del m.c.d. basta considerar $a \geq 0$ y $b \geq 0$. El m.c.d. tiene propiedades muy interesantes entre las que destacan dos definiciones alternativas para éste.

Definición 7.2.6. *Sean $a, b, c \in \mathbb{Z}$. c es combinación lineal de a y b si existen enteros x y y tales que $c = ax + by$.*

Ejemplo 7.2.7.
(1) 93 es combinación lineal de 3 y 39 ya que $93 = 3 \cdot 5 + 39 \cdot 2$.
(2) 11 es combinación lineal de 4 y 7 puesto que $11 = 4 \cdot 8 - 3 \cdot 7$. Podemos decir que 11 también es combinación lineal de 8 y -3.

Considerando ahora el conjunto A de todas las combinaciones lineales de a y b, es decir, $\{ax + by \mid x, y \in \mathbb{Z}\}$. Este conjunto A es infinito si $a \neq 0$ o $b \neq 0$. Además $A \cap (\mathbb{N} - \{0\}) \neq \varnothing$ (verifíquelo) y por lo tanto tiene mínimo, esto último por el axioma de buen orden. Evidentemente este elemento mínimo que es la mínima combinación lineal positiva de a y b es mayor que cero y demostraremos que es precisamente el máximo común divisor de a y b.

Lema 7.2.8. *Sean $a, b \in \mathbb{Z}$ con $a \neq 0$ o $b \neq 0$ y sea d la mínima combinación lineal positiva de a y b. Entonces $d \mid a$ y $d \mid b$.*

Demostración. Como d es la mínima combinación lineal positiva, entonces $d = ax + by$ con $x, y \in \mathbb{Z}$ y $d > 0$. Para demostrar que $d \mid a$ aplicaremos el algoritmo de la división a d y a y mostraremos que el residuo es cero.
Sea $a = dq + r$ donde $0 \leq r < d$. Entonces $r = a - dq = a - (ax + by)q = a(1 - xq) + b(-yq)$ y de aquí se tiene que r es una combinación lineal de a y b y debido a que $0 \leq r < d$ y es la mínima combinación lineal de a y b, la única posibilidad para r es que $r = 0$ y por lo tanto $d \mid a$. Análogamente $d \mid b$. ∎

La ventaja de tener definiciones alternativas para el m.c.d. de dos enteros, como se irá viendo a lo largo de este capítulo, es que nos permite usar cualquiera de ellas según no sea más conveniente.

Teorema 7.2.9. *Sean $a, b, d \in \mathbb{Z}$ con $a \neq 0$ o $b \neq 0$. Son equivalentes*

(1) $d = (a, b)$
(2) *d es la mínima combinación lineal positiva de a y b.*
(3) *d satisface*
  (*i*) $d \geq 1$
  (*ii*) $d \mid a$ *y* $d \mid b$
  (*iii*) *Si* $d' \mid a$ *y* $d' \mid b$ *entonces* $d' \mid d$.

Demostración. (1) $\Longrightarrow$ (2) Sean $d = (a, b)$ y $d' = ax + by$ la mínima combinación lineal positiva de a y b. Por el lema 7.2.8 $d' \mid a$ y $d' \mid b$ y por lo tanto $d' \leq d$. Por otro lado, $d \mid a$ y $d \mid b$ implican $d \mid ax + by = d'$. Como $d' > 0$, entonces $d \leq d'$. Luego $d = d'$.
(2) $\Longrightarrow$ (3) Sea $d = ax + by$ la mínima combinación lineal positiva de a y b. Entonces

(*i*) $d \geq 1$
(*ii*) $d \mid a$ y $d \mid b$ por el lema 7.2.8
(*iii*) Si $d' \mid a$ y $d' \mid b$ entonces $d' \mid ax + by = d$.

(3) $\Longrightarrow$ (1) Supongamos que $d \in \mathbb{Z}$ satisface (*i*), (*ii*) y (*iii*). Entonces

(*i*) $d \mid a$ y $d \mid b$ por hipótesis
(*ii*) Si $d' \mid a$ y $d' \mid b$ entonces por (3) $d' \mid d$ y por ser $d > 0$, $d' \leq d$.

Por lo tanto $d = (a, b)$. ∎

Definición 7.2.10. *Sean $a, b \in \mathbb{Z}$ con $a \neq 0$ y $b \neq 0$. Diremos que a y b son* **primos relativos** *o* **primos entre sí** *o* **coprimos** *si* $(a, b) = 1$.

Corolario 7.2.11. *Los enteros a y b son primos relativos sí y sólo si* 1 *es combinación lineal de a y b.*

Corolario 7.2.12. *Si* $d = (a, b)$, *entonces* $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Se deja la demostración de estos dos últimos corolarios como ejercicio (véase los ejercicios 7.2.9 y 7.2.10 (1)).
Otras propiedades del m.c.d. están dadas en el siguiente resultado.

Teorema 7.2.13. *Sean $a, b, c \in \mathbb{Z}$ tales que $c \neq 0$ y $a \neq 0$ o $b \neq 0$. Entonces* $(ca, cb) = |c|(a, b)$.

Demostración. Recordemos que podemos suponer $c > 0$.
Sean $d = (ca, cb)$ y $d' = (a, b)$. Veremos que $d = cd'$ mostrando que cada uno de ellos divide al otro.

$1°/$ $cd' \mid d$. Como $d' \mid a$ y $d' \mid b$, entonces $cd' \mid ca$ y $cd' \mid cb$ y por lo tanto $cd' \mid d$.
$2°/$ Por el teorema 7.2.9, existen $x, y \in \mathbb{Z}$ tale que $d' = ax + by$. Multiplicando esta igualdad por c obtenemos $cd' = cax + cby$ y entonces $d \mid cd'$. ∎

Corolario 7.2.14. *Sean $a, b, c \in \mathbb{Z}$ tales que $c \neq 0$ y $a \neq 0$ o $b \neq 0$, $c \mid a$ y $c \mid b$. Entonces* $\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{(a,b)}{|c|}$.

Demostración. Primero, como $c \mid a$ y $c \mid b$, entonces $c \mid (a, b)$ y así $\frac{a}{c}$, $\frac{b}{c}$ y $\frac{(a,b)}{|c|}$ tiene sentido. Aplicando el teorema 7.2.13, tenemos que

$$(a, b) = \left(c\frac{a}{c}, c\frac{b}{c}\right) = |c| \left(\frac{a}{c}, \frac{b}{c}\right)$$

y de aquí se obtiene el resultado. ∎

Teorema 7.2.15. *Sean $a, b, c \in \mathbb{Z} - \{0\}$ tales que $(a, c) = (b, c) = 1$. Entonces* $(ab, c) = 1$.

Demostración. Por el corolario 7.2.11, $1 = ax + cy$ y $1 = bx' + cy'$, con $x, y, x', y' \in \mathbb{Z}$. Multiplicando estas igualdades se tiene

$$1 = ab(xx') + c(axy' + byx' + cyy')$$

y nuevamente por el corolario 7.2.11, $(ab, c) = 1$. ∎

Teorema 7.2.16. *Sean $a, b, c \in \mathbb{Z} - \{0\}$. Si $a \mid bc$ y $(a, b) = 1$, entonces $a \mid c$.*

Demostración. Como $(a, b) = 1$, existen $x, y \in \mathbb{Z}$ tales que $1 = ax + by$ y de aquí $c = cax + cby$. Ya que $a \mid a$ y $a \mid bc$, entonces $a \mid a(cx) + (bc)y = c$. ∎

Teorema 7.2.17. *Sean $a, b, c \in \mathbb{Z}$ con $a \neq 0$ o $b \neq 0$. Si $a \mid c$, $b \mid c$ y $(a, b) = 1$, entonces $ab \mid c$.*

Demostración. $a \mid c$ implica que $c = ar$ con $r \in \mathbb{Z}$. Por otro lado, $b \mid c = ar$ y ya que $(a, b) = 1$, por el teorema 7.2.16, $b \mid r$. Sea $r = bs$ con $s \in \mathbb{Z}$. Entonces $c = ar = abs$ y así $ab \mid c$. ∎

Hasta el momento hemos visto que para obtener el m.c.d. de dos enteros a y b, debemos encontrar primero $D(a)$ y $D(b)$ (aunque en realidad bastaría con uno de ellos ¿por qué?) y de ahí $D(a) \cap D(b)$. Este procedimiento puede ser muy largo, sobre todo en los casos en que a y b son muy grandes. Sin embargo este proceso puede reducirse considerablemente mediante un algoritmo, conocido como el algoritmo de Euclides, que se basa precisamente en en el algoritmo de la división.

Algoritmo de Euclides

Podemos suponer $a > 0$ y $b > 0$ puesto que en el caso de que alguno sea cero, por ejemplo a, $(a, b) = (0, b) = b$. Comenzamos aplicando el algoritmo de la división a los enteros a y b y a partir de ahí se obtiene una sucesión de igualdades, cada una de ellas como resultado de aplicar el algoritmo de la división a una pareja de enteros que aparecen en la igualdad inmediata anterior.

$$\begin{array}{rcll} a & = & bq_0 + r_0 & 0 < r_0 < b \\ b & = & r_0q_1 + r_1 & 0 < r_1 < r_0 \\ & \vdots & & \\ r_{i-1} & = & r_iq_{i+1} + r_{i+1} & 0 < r_{i+1} < r_i \\ & \vdots & & \end{array}$$

Como se muestra en las igualdades, mientras el residuo $r_i > 0$, se obtiene una nueva igualdad. Pero debido a que $r_0 > r_1 > \cdots > r_i > \cdots$ y cada $r_i \geq 0$, en algún momento se tendrá que para alguna n, $r_n = 0$ y por lo tanto ahí termina la sucesión.

Supongamos entonces que se tiene

$$\begin{array}{rcll} a & = & bq_0 + r_0 & 0 < r_0 < b \\ b & = & r_0q_1 + r_0 & 0 < r_1 < q_0 \\ & \vdots & & \\ r_{n-3} & = & r_{n-2}q_{n-1} + r_{n-1} & 0 < r_{n-1} < r_{n-2} \\ r_{n-2} & = & r_{n-1}q_n + r_n & r_n = 0 \end{array} \tag{1}$$

Lo que probaremos es que el último residuo distinto de cero, en este caso r_{n-1}, es precisamente el m.c.d. de a y b. Antes de probar esto necesitamos el siguiente:

Lema 7. 2.18. *Sean $r, s, q, t \in \mathbb{Z}$ tales que $s = tq + r$ y $t \neq 0$. Entonces $(s, t) = (r, t)$.*

Demostración. Demostraremos que $(s,t) \mid (r,t)$ y $(r,t) \mid (s,t)$ y como ambos son positivos se tendrá entonces $(s,t) = (r,t)$.
Como $(s,t) \mid s$ y $(s,t) \mid t$, entonces $(s,t) \mid s - tq = r$ y por lo tanto $(s,t) \mid (r,t)$.
Análogamente $(r,t) \mid r$ y $(r,t) \mid t$ implica que $(r,t) \mid tq + r = s$ y de aquí $(r,t) \mid (s,t)$. ∎

Teorema 7.2.19. *Sean $a, b \in \mathbb{Z}$ con $a > 0$ y $b > 0$. El último residuo distinto de cero al aplicar el algoritmo de Euclides a a y b es el m.c.d. de a y b.*

Demostración. Aplicando iteradamente el lema 7.2.18 al conjunto de igualdades (1), arriba, tenemos

$$r_{n-1} = (0, r_{n-1}) = (r_{n-1}, r_{n-2}) = (r_{n-2}, r_{n-3}) = \cdots = (r_1, r_0) = (b, r_0) = (a, b).$$ ∎

Así pues el algoritmo de Euclides nos permite encontrar el m.c.d. de dos enteros *a* y *b*. Pero no solamente eso, sino que además a través de él podemos expresar éste m.c.d. como combinación lineal de *a* y *b*. Veamos un ejemplo.

Ejemplo 7.2.20. Sean $a = 1984$ y $b = 34131$. Aplicando el algoritmo de Euclides a *a* y *b* obtenemos

$$\begin{aligned} 34131 &= 1984 \cdot 17 + 403 \\ 1984 &= 403 \cdot 4 + 372 \\ 403 &= 372 \cdot 1 + 31 \\ 372 &= 31 \cdot 12 + 0 \end{aligned}$$

Entonces, por el teorema 7.2.17, $(34131, 1984) = 31$. Ahora expresemos este m.c.d. como combinación lineal de *a* y *b*
Empezamos a despejar los residuos de abajo hacia arriba en la sucesión de igualdades:

$$\begin{aligned} 31 &= 403 \cdot 1 - 372 \cdot 1 \\ &= 403 \cdot 1 - (1984 \cdot 1 - 403 \cdot 4) \cdot 1 \\ &= 403 \cdot 5 - 1984 \cdot 1 \\ &= (34131 - 1984 \cdot 17) \cdot 5 - 1984 \cdot 1 \\ &= 34131 \cdot 5 - 1984 \cdot 85 - 1984 \cdot 1 \\ &= 34131 \cdot 5 - 1984 \cdot 86 \end{aligned}$$

Generalizamos ahora el concepto de m.c.d. a un numero finito de enteros.

Definición 7.2.21. *Sean $a_1, \ldots, a_m \in \mathbb{Z}$, donde al menos un $a_i \neq 0$. Un entero d es el máximo común divisor de $a_1 \ldots, a_m$ si satisface*

(*i*) $d \geq 1$
(*ii*) $d \mid a_i$ *para toda* $i = 1, \ldots, m$
(*iii*) *Si* $d' \mid a_i$ *para toda* $i = 1, \ldots, m$, *entonces* $d' \mid d$

Denotamos al m.c.d. por $\boldsymbol{d = (a_1, \ldots, a_m)}$.
Comparando esta última definición con la dada para el caso $m = 2$, hemos pedido en el inciso (*iii*) que $d' \mid d$ en lugar de $d' \leq d$. No hay ningún problema en esto ya que, como se hizo en el caso de dos enteros, son equivalentes.

§ §7.2.2. Mínimo común múltiplo.

Introducimos el concepto de mínimo común múltiplo de manera similar al de m.c.d.
Dado cualquier entero a, definimos $\boldsymbol{M(a)} = \{x \in \mathbb{Z} \mid a \mid x\}$ y llamamos a cada elemento de este conjunto un múltiplo de a. No es difícil ver que $M(a) = \{ay \mid y \in \mathbb{Z}\}$.
Algunas propiedades de estos conjuntos son

(1) $M(0) = \{0\}$.
(2) $0, \pm a \in M(a)$.
(3) $M(a) = M(-a)$.
(4) Si $y \in M(a)$, entonces $y \cdot z \in M(a)$ para todo $z \in \mathbb{Z}$.
(5) Si $a \neq 0$, entonces $M(a)$ es infinito.
(6) Para cualesquiera $a, b \in \mathbb{Z} - \{0\}$, $a \cdot b \in M(a) \cap M(b)$.
(7) Si $a \neq 0$ y $b \neq 0$, entonces $M(a) \cap M(b)$ es infinito.
(8) Si $a \neq 0$ y $b \neq 0$, entonces $M(a) \cap M(b)$ tiene un mínimo positivo.

Estas propiedades son consecuencia de propiedades sobre divisibilidad vistas en la sección 7, así que dejamos la demostración como ejercicio (véase ejercicio 7.2.3).
Las propiedades que determinan al mínimo positivo del inciso (8) son

Definición 7.2.22. *Dados* $a, b \in \mathbb{Z}$ *con* $a \neq 0$ *y* $b \neq 0$, *su* **mínimo común múltiplo** *es el entero* m *que satisface*

(*i*) $m > 0$
(*ii*) $a \mid m$ *y* $b \mid m$
(*iii*) *Si* $a \mid m'$ *y* $b \mid m'$ *entonces* $m \leq |m'|$

Denotamos por **[*a*, *b*]** al mínimo común múltiplo (**m.c.m.**) de a y b.

Ejemplo 7.2.23. Encontremos el m.c.m. de $a = 6$ y $b = 10$.
$M(a) = \{0, \pm 6, \pm 12, \pm 18, \pm 24, \pm 30, \pm 36, \pm 42, \pm 48, \pm 54, \pm 60, \pm 66, \ldots\}$

$M(b) = \{0, \pm 10, \pm 20, \pm 30, \pm 40, \pm 50, \pm 60, \pm 70, \ldots\}$
$M(a) \cap M(b) = \{0, \pm 30, \pm 60, \pm 90, \ldots\}$
Entonces $[6, 10] = 30$.

Proposición 7.2.24. *Sean $a, b \in \mathbb{Z}$ con $a \neq 0$ y $b \neq 0$. Entonces*

(1) $[a, b] = [b, a]$
(2) $[a, b] = [|a|, |b|]$
(3) $[a, b] = |a|$ *si y sólo si* $b \mid a$.

Demostración. (1) y (2) son inmediatas, así que sólo demostraremos (3). Por (2) basta suponer $a > 0$ y $b > 0$.

$\Longrightarrow$) Supongamos $[a, b] = a$. Por definición $b \mid [a, b] = a$.
$\Longleftarrow$) Si $b \mid a$, entonces a es múltiplo de a y b y de aquí $[a, b] \leq a$. Por otro lado, por definición, $a \mid [a, b]$ y entonces $a \leq [a, b]$. Por lo tanto $[a, b] = a$. ∎

Similarmente a como sucedió con el m.c.d., en la definición de m.c.m. se puede sustituir el inciso (*iii*) por una propiedad más fuerte.

Teorema 7.2.25. *Sean $a, b \in \mathbb{Z}$ con $a \neq 0$ y $b \neq 0$. Son equivalentes*

(1) $m = [a, b]$
(2) *m satisface*
  (i') $m > 0$
  (ii') $a \mid m$ *y* $b \mid m$
  (iii') *Si* $a \mid m'$ *y* $b \mid m'$, *entonces* $m \mid m'$.

Demostración. (1) $\Longrightarrow$ (2). Sea $m = [a, b]$. Por la definición de $[a, b]$, se satisfacen (i') y (ii'). Ahora sea $m' \in \mathbb{Z}$ tal que $a \mid m'$ y $b \mid m'$ y sea $m' = mq + r$, con $0 \leq r < m$. Como $a \mid m'$ y $b \mid m'$, entonces $a \mid r$ y $b \mid r$, luego por (*iii*) de la definición de m.c.m., si $r > 0$, debe ser $[a, b] = m \leq r$ lo cual es imposible. Por lo tanto $r = 0$ y entonces $m \mid m'$.
(2) $\Longrightarrow$ (1) Es inmediato ya que $m \mid m'$ implica $m \leq |m'|$. ∎

Teorema 7.2.26. *Sean $a, b, c \in \mathbb{Z}$. Entonces* $[ca, cb] = |c|[a, b]$.

Demostración. Podemos suponer $c > 0$. Sea $m = [ca, cb]$ y $m' = [a, b]$. Mostraremos que $m \mid c \cdot m'$ y $c \cdot m' \mid m$.

1°/ Como $a \mid m'$ y $b \mid m'$, entonces $ca \mid cm'$ y $cb \mid cm'$ y de aquí $m \mid c \cdot m'$.

2°/ Ya que $ca \mid m$ y $cb \mid m$, se tiene que existen $r, s \in \mathbb{Z}$ tales que $car = m = cbs$ y por lo tanto $ar = bs$ (recuérdese que $c \neq 0$). De aquí $a \mid bs$ y por supuesto también $b \mid bs$, por lo que $m' \mid bs$ y así $c \cdot m' \mid c \cdot bs = m$.

Ahora, como $m > 0$ y $c \cdot m' > 0$, entonces $m = c \cdot m'$ ∎

El siguiente resultado muestra la relación que existe entre el m.c.d. y el m.c.m. de dos enteros.

Teorema 7.2.27. *Sean $a, b \in \mathbb{Z} - \{0\}$. Entonces $[a, b] \cdot (a, b) = |a \cdot b|$.*

Demostración. Empezamos demostrando el resultado cuando $(a, b) = 1$ y de éste y el teorema 7.2.26 obtendremos el caso general.
Supongamos que $(a, b) = 1$. Debemos demostrar que $[a, b] = |a \cdot b|$. Podemos suponer $a > 0$ y $b > 0$. Como $a \cdot b$ es múltiplo común de a y b se tiene que $[a, b] \mid a \cdot b$. Por otro lado, $a \mid [a, b]$ y $b \mid [a, b]$ y puesto que $(a, b) = 1$, por el teorema 7.2.17, $a \cdot b \mid [a, b]$. Entonces $[a, b] = a \cdot b$.
Ahora sea $d = (a, b)$. Entonces $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ y por el teorema 7.2.26 y el primer caso, $(a, b)[a, b] = d\left[d\frac{a}{d}, d\frac{b}{d}\right] = d^2\left[\frac{a}{d}, \frac{b}{d}\right] = d^2\frac{a}{d} \cdot \frac{b}{d} = ab$. ∎

Así como se generalizó el m.c.d. de dos enteros a un número finito, haremos lo mismo para el m.c.m.:

Definición 7.2.28. *Sean $a_1, \ldots, a_n \in \mathbb{Z} - \{0\}$. El mínimo común múltiplo de $a_1, \ldots, a_n$ es el entero m que satisface:*

(*i*) $m \geq 1$
(*ii*) $a_i \mid m$ *para toda* $i = 1, \ldots, n$
(*iii*) *Si* $a_i \mid m'$ *para toda* $i = 1, \ldots, n$, *entonces* $m \leq |m'|$.

Al mínimo común múltiplo de $a_1, \ldots, a_n$ lo denotaremos por $\mathbf{[a_1, \ldots, a_n]}$.

Nota 7.2.29. La existencia del m.c.m. de $a_1, \ldots, a_n$ está asegurada aplicando el axioma del buen orden al conjunto $M(a_1) \cap \cdots \cap M(a_n) \cap (\mathbb{N} - \{0\})$ que sabemos es no vacío ya que $|a_1 \cdot \ldots \cdot a_n|$ pertenece a él.

§ 7.3. Ecuaciones diofantinas

Una aplicación de lo que se vio en la sección 2 sobre m.c.d está en la manera de encontrar en $\mathbb{Z}$ una solución, si la hay, de una ecuación del tipo $ax + by = c$, donde $a, b, c \in \mathbb{Z}$. Este tipo de ecuaciones forman parte de las así llamadas ***ecuaciones diofantinas***, debiéndose este nombre a Diophantos (siglo III D.C.)

que propuso una gran cantidad de problemas en cuyo planteamiento matemático aparecen ecuaciones con coeficientes enteros, no sólo del tipo de ecuación de la que hablamos sino de varias más como por ejemplo $x^2 + y^2 + z^2 + w^2 = n$ donde n es un número natural, que por cierto se ha demostrado que siempre tiene solución para toda n. Por supuesto dependiendo de cómo es la ecuación será el método para encontrar una solución (si la hay) de ellas. En esta sección sólo estudiamos las ecuaciones del tipo mencionado al inicio de ésta.

Definición 7.3.1. *Sean $a, b, c \in \mathbb{Z}$. Una pareja de enteros x_0, y_0 es una solución de la ecuación $ax + by = c$ si $ax_0 + by_0 = c$.*

No todas las ecuaciones $ax + by = c$ tiene solución en $\mathbb{Z}$. Por ejemplo $2x + 6y = 3$ no tiene solución en $\mathbb{Z}$ puesto que sin importar los valores enteros de x y y; el lado izquierdo de la igualdad será siempre par y 3 no lo es. Así pues, nuestra tarea consistirá, por un lado encontrar un criterio para saber cuándo una ecuación de este tipo tiene solución y por otro, en caso de que la tenga, cómo encontrar no sólo una sino todas las soluciones.
Empezamos estudiando ecuaciones del tipo $ax + by = 0$, esto es, cuando $c = 0$ y a las que se les llama ***homogéneas***, para luego pasar a la ecuación general, en donde en algún momento se hará uso del caso de una ecuación homogénea.
Consideremos la ecuación $ax + by = 0$ con $a, b \in \mathbb{Z}$. Evidentemente tiene al menos una solución que es $x = 0$ y $y = 0$ y a la que llamaremos solución trivial. Así pues la parte interesante será investigar si la ecuación tiene solución distinta de la trivial y cuáles son todas. La respuesta está dada en el siguiente

Teorema 7.3.2. *Sean $a, b \in \mathbb{Z}$ tales que $a \neq 0$ y $b \neq 0$. Las soluciones de la ecuación $ax + by = 0$ están dadas por $x = \frac{b}{d} \cdot t$, $y = \frac{-a}{d} \cdot t$ donde t es un entero arbitrario y $d = (a, b)$.*

Demostración. Es claro que para cualquier entero t, la pareja de enteros $x = \frac{b}{d} \cdot t$, $y = \frac{-a}{d} \cdot t$ es solución de la ecuación, esto es,

$$a\left(\frac{b}{d} \cdot t\right) + b\left(\frac{-a}{d} \cdot t\right) = \frac{ab}{d} \cdot t - \frac{ab}{d} \cdot t = 0.$$

Por otro lado, si (x_0, y_0) es una solución de la ecuación, entonces $ax_0 + by_0 = 0$. De $d\left(\frac{a}{d}x_0 + \frac{b}{d}y_0\right) = 0$ y $d \neq 0$, obtenemos $\frac{a}{d}x_0 + \frac{b}{d}y_0 = 0$, es decir, $\frac{a}{d}x_0 = -\frac{b}{d}y_0$. Entonces debido a que $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, por el teorema 7.2.16 $\frac{a}{d} \mid y_0$ y así $y_0 = \frac{a}{d}r$ para algún entero r. Análogamente $\frac{b}{d} \mid x_0$, por lo que $x_0 = \frac{b}{d}t$ para algún entero

t. Ahora, teniendo en cuenta que (x_0, y_0) es solución de la ecuación se tiene que $0 = ax_0 + by_0 = a\left(\frac{b}{d}t\right) + b\left(\frac{a}{d}r\right) = \frac{ab}{d}(t + r)$, luego, por ser $\frac{ab}{d} \neq 0$, $t + r = 0$, es decir $r = -t$. Por lo tanto $x_0 = \frac{b}{d}t$ y $y_0 = \frac{-a}{d}t$. ∎

Nota 7.3.3. En el teorema 7.3.2, hemos pedido que $a \neq 0$ y $b \neq 0$, hecho que se usó en la demostración. Sin embargo, si alguno de ellos es cero, digamos b, igualmente el conjunto de soluciones queda descrito de la misma manera; $x = \frac{b}{d}t = 0$ y $y = \frac{-a}{|a|}t = \pm t$, donde $t \in \mathbb{Z}$ y $(a, b) = |a|$.

Pasando ahora al caso general, ya hemos visto que no toda ecuación

$$ax + by = c \quad (c \neq 0)$$

tiene solución en los enteros. En el párrafo inmediato posterior a la definición 7.3.1 se da un ejemplo de esto, en donde observamos que $2 = (2, 6) \nmid 3$. En general si existe una solución, entonces se debe cumplir que $(a, b) \mid c$, luego este hecho es una condición necesaria para que la ecuación tenga solución. En el siguiente teorema veremos que esta condición resulta ser también suficiente y aún más, en la demostración se indicará cómo encontrar una solución particular y de ahí el teorema 7.3.5 nos dice cómo encontrar todas las soluciones.

Teorema 7.3.4. *Sean $a, b \in \mathbb{Z}$ tales que $a \neq 0$ o $b \neq 0$. La ecuación $ax + by = c$ tiene solución en $\mathbb{Z}$ si y sólo si $(a, b) \mid c$.*

Demostración.

- $\Longrightarrow$) Supongamos que la ecuación tiene solución (x_0, y_0). Entonces $ax_0 + by_0 = c$ y por lo tanto $(a, b) \mid c$.
- $\Longleftarrow$) Sea $d = (a, b)$ y supongamos que $d \mid c$. Entonces $d \cdot c' = c$ para alguna $c' \in \mathbb{Z}$. d es combinación lineal de a y b (teorema 7.2.9), esto es, existen enteros r y s tales que $ar + bs = d$. Multiplicando por c' a ambos lados de la igualdad obtenemos $a \cdot rc' + b \cdot sc' = d \cdot c' = c$ y por lo tanto $x = rc'$ y $y = sc'$ será solución de la ecuación. ∎

Este último teorema nos permite encontrar una solución particular de la ecuación $ax + by = c$, pero con la ayuda del teorema 7.3.2 obtendremos todas las soluciones a través de las soluciones de la ecuación $ax + by = 0$, a la que llamamos ***ecuación homogénea asociada***.

Teorema 7.3.5. *Sean $a, b, c \in \mathbb{Z}$ tales que $a \neq 0$ y $b \neq 0$ y sea (x_0, y_0) una solución particular de la ecuación $ax + by = c$. Entonces todas las soluciones de*

la ecuación están dadas por

$$x = x_0 + \tfrac{b}{d}t, y = y_0 - \tfrac{a}{d}t \quad \textit{donde } d = (a,b) \textit{ y } t \in \mathbb{Z}.$$

Demostración. Primero para cualquier $t \in \mathbb{Z}$, la pareja de enteros $x = x_0 + \frac{b}{d}t$ y $y = y_0 - \frac{a}{d}t$ es solución de la ecuación, pues

$$a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right) = ax_0 + by_0 + \frac{ab}{d}t - \frac{ab}{d}t = ax_0 + by_0 = c.$$

Ahora, supongamos que (x_1, y_1) es solución de la ecuación. Luego

$$ax_1 + by_1 = c = ax_0 + by_0,$$

y de aquí $a(x_1 - x_0) + b(y_1 - y_0) = 0$, por lo que $(x_1 - x_0, y_1 - y_0)$ es un solución de $ax + by = 0$. Pero por el teorema 7.3.2, debe ser $x_1 - x_0 = \frac{b}{d}t$ y $y_1 - y_0 = -\frac{a}{d}t$ para alguna $t \in \mathbb{Z}$. Entonces $x_1 = x_0 + \frac{b}{d}t$ y $y_1 = y_0 - \frac{a}{d}t$ para alguna $t \in \mathbb{Z}$. ∎

Ejemplo 7.3.6. Encontraremos todas las soluciones (si las tiene) de

$$72x + 20y = 28.$$

Verificamos primero que la ecuación tiene solución viendo que efectivamente $4 = (72, 20) \mid 28$. Como ya hemos visto, basta encontrar una solución particular para de ahí obtener todas y para esto, como se hizo en la demostración del teorema 7.3.2, expresamos 4 como combinación lineal de 72 y 20 apoyándonos en el algoritmo de Euclides.

$$\begin{aligned} 72 &= 20 \cdot 3 + 12 \\ 20 &= 12 \cdot 1 + 8 \\ 12 &= 8 \cdot 1 + 4 \\ 8 &= 4 \cdot 2 + 0 \end{aligned}$$

Entonces

$$\begin{aligned} 4 &= 12 - (8 \cdot 1) \\ &= 12 - (20 - 12 \cdot 1) \cdot 1 \\ &= 12 \cdot 2 - 20 \cdot 1 \\ &= (72 - 20 \cdot 3) \cdot 2 - 20 \cdot 1 \\ &= 72 \cdot 2 - 20 \cdot 7 \end{aligned}$$

Así pues, $4 = 72 \cdot 2 + 20 \cdot (-7)$ y multiplicando por 7 a ambos lados de la igualdad obtenemos $72 \cdot 14 + 20 \cdot (-49) = 28$.

De aquí se tiene que $x_0 = 14$ y $y_0 = -49$ es una solución particular de la ecuación. Luego todas las soluciones están dadas por $x = 14 + \frac{20}{4}t = 14 + 5t$, $y = -49 - \frac{72}{4}t = -49 - 18t$ y $t \in \mathbb{Z}$.

§ 7.4. Números primos

Cada entero x distinto de 1 y -1 tiene al menos cuatro divisores que son ± 1 y $\pm x$. Existen algunos enteros cuyos únicos divisores son estos, por ejemplo, los divisores de $2, 3$ y 5 son $\{\pm 1, \pm 2\}$, $\{\pm 1, \pm 3\}$ y $\{\pm 1, \pm 5\}$ respectivamente. En esta sección veremos que hay una infinidad de enteros mayores que 1 con esta propiedad y que juegan un papel relevante en el estudio de los números enteros (Teoría de números). A este tipo de enteros los llamaremos números primos y a lo largo de esta sección se mostrará su importancia.

Definición 7.4.1. *Un entero $p > 1$ se llama* **primo** *si su único divisor mayor que 1 es p. A los enteros que no son primos los llamaremos* **compuestos**.

Dicho de otra manera, un entero $p > 1$ es primo si y sólo si $p = a \cdot b$, con $a, b \in \mathbb{Z}$ y $a \geq 1$ implica $a = 1$ o $a = p$.

Ejemplo 7.4.2. $11, 23$ y 37 son números primos y $4, 27$ y 45 son números compuestos.

Proposición 7.4.3. *Sea p primo y a cualquier entero. Entonces*

$$(a, p) = \begin{cases} 1 & si \;\; p \nmid a \\ p & si \;\; p \mid a \end{cases}$$

Demostración. Sea $d = (a, p)$. Entonces $d \mid p$, y por ser p primo, $d = 1$ o $d = p$. Luego $d = 1$ cuando $p \nmid a$ y $d = p$ cuando $p \mid a$. ∎

Teorema 7.4.4. *Sea p primo. Si $p \mid a \cdot b$, entonces $p \mid a$ o $p \mid b$.*

Demostración. Supongamos que $p \mid a \cdot b$ y que $p \nmid a$. Entonces por la proposición 7.4.3 $(a, p) = 1$ Luego por el teorema 7.2.16 $p \mid b$. ∎

En realidad la propiedad de los primos descrita en este último teorema los caracteriza:

Teorema 7.4.5. *Sea $p \in \mathbb{Z}$ con $p > 1$. p es primo si y sólo si cada vez que $p \mid a \cdot b$, entonces $p \mid a$ o $p \mid b$.*

Demostración.

$\Longrightarrow$) Es precisamente el teorema 7.4.4
$\Longleftarrow$) Supongamos que p tiene la propiedad: $p \mid a \cdot b$ implica $p \mid a$ o $p \mid b$. Mostraremos que los únicos divisores positivos de p son 1 y p. Sea $a \in \mathbb{Z}$, $a \geq 1$ tal que $a \mid p$. Entonces existe $b \in \mathbb{Z}$ tal que $p = a \cdot b$ (obsérvese que también $b \mid p$). Luego, por hipótesis, $p \mid a$ o $p \mid b$. Si $p \mid a$, como a y p son positivos, por (12) del teorema 7.1.5, debe ser $a = p$. Si $p \mid b$, el mismo argumento muestra que $b = p$ y entonces $a = 1$.∎

En el ejercicio 7.4.50 se pide demostrar una generalización del teorema 7.4.5: Si p es primo y $p \mid a_1 \cdot a_2 \cdot \ldots \cdot a_n$, entonces $p \mid a_i$ para alguna $i = 1, 2, \ldots, n$. Una aplicación de este resultado se da en el teorema 7.4.7.
El conjunto de los número primos genera a los números enteros, en el siguiente sentido.

Teorema 7.4.6. *Cada número entero $n > 1$ se expresa como un producto de primos, no necesariamente distintos y puede aparecer un único primo una sola vez.*

Demostración. Por inducción sobre n

1°/ $n = 2$. Como 2 es primo, la descomposición es $2 = 2$.
2°/ Sea $n > 2$ y supongamos cierto el teorema para toda m tal que $1 < m < n$.

Hay dos posibilidades para n: n es primo o n es compuesto. Si n es primo aquí terminamos, así que supongamos que n es compuesto, esto es, $n = a \cdot b$ donde $1 < a, b < n$. Por hipótesis de inducción, $a = p_1 \cdot \ldots p_r$ y $b = q_1 \cdot \ldots \cdot q_s$, con p_i, q_j primos para $i = 1, \ldots, r$ y $j = 1, \ldots, s$. Entonces

$$n = p_1 \cdot \ldots p_r \cdot q_1 \cdot \ldots q_s. \blacksquare$$

Salvo el orden de los factores, la descomposición en primos es única, esto significa que cada primo y el número de veces que aparece en la descomposición está determinado, de manera única, por n:

Teorema 7.4.7. *(Teorema de descomposición única) La descomposición de un número entero $n > 1$, como producto de números primos, es única salvo por el orden de los factores.*

Demostración. Sean $n > 1$ y $n = p_1 \cdot \ldots p_k$ con $k \geq 1$ y p_i primo para $i = 1, \ldots, k$. Demostraremos el resultado por inducción sobre k, el número de factores.

1°/ $k = 1$. Entonces $n = p_1$ con p_1 primo y supongamos que $p_1 = q_1 \cdot \ldots q_r$ donde q_j es primo para $j = 1, \ldots, r$. Como p_1 es primo y $p_1 \mid q_1 \cdot \ldots q_r$, por el ejercicio

7.4.50, $p_1 \mid q_i$ para alguna $i = 1, \ldots, r$ y sin pérdida de generalidad podemos suponer $p_1 \mid q_1$. Como q_1 es primo y $p_1 > 1$, entonces $p_1 = q_1$. Si fuera $r > 1$, tendríamos que $q_2 \cdot \ldots q_s = 1$ lo que es un absurdo, ya que cada $q_i > 1$.
2°/ Supongamos ahora $k > 1$ y que el teorema es cierto para $k-1$ y supongamos que $n = p_1 \cdot \ldots p_k = q_1 \cdot \ldots q_r$ donde q_j es primo para $j = 1, \ldots, r$. Con el mismo argumento que el caso $k = 1$, podemos suponer que $p_k \mid q_r$ y por lo tanto $p_k = q_r$, por lo que podemos cancelar p_k en la igualdad para obtener $p_1 \cdot \ldots p_{k-1} = q_1 \cdot \ldots q_{r-1}$ y esto por la hipótesis de inducción implica que

$$k - 1 = r - 1 \; y \; p_i = q_{j_i} \; para \; i = 1, \ldots, k-1$$

$$y \; \{j_1, \ldots, j_{k-1}\} = \{1, \ldots, k-1 = r-1\}. \; \blacksquare$$

Ya hemos mencionado que en la descomposición de un número $n > 1$ como producto de primos, un primo puede aparecer más de una vez, así que si el primo p aparece m veces, en lugar de escribir m veces el primo p, podemos sustituirlo por p^m y de esta manera n se expresará como $n = p_1^{m_1} \cdot \ldots \cdot p_k^{m_k}$, donde $p_1, \ldots, p_k$ son todos primos distintos y $m_i \geq 1$ para $i = 1, \ldots, k$. La unicidad quedaría expresada como sigue:
Si $p_1^{m_1} \cdot \ldots \cdot p_k^{m_k} = q_1^{t_1} \cdot \ldots \cdot q_r^{t_r}$ donde p_i y q_j son primos $m_i \geq 1$, $t_j \geq 1$ para $i = 1, \ldots, k$ y $j = 1, \ldots, r$, $p_i \neq p_s$ si $i \neq s$ y $q_j \neq q_\ell$ si $j \neq \ell$, entonces $k = r$, $p_i = q_{j_i}$ y $m_i = t_{j_i}$ para $i = 1, \ldots, k$ y $\{j_1, \ldots, j_k\} = \{1, \ldots, k\}$.

Corolario 7.4.8. *Dados $a \in \mathbb{Z}$, $a \neq 1, -1$ existe un primo p tal que $p \mid a$.*

Demostración. Sea $a \in \mathbb{Z}$, $a \neq 1$ y $a \neq -1$ y consideremos $\mid a \mid$, el valor absoluto de a. Si $\mid a \mid = 0$, entonces $a = 0$ y cualquier primo lo divide. Supongamos entonces que $a \neq 0$, entonces $\mid a \mid > 1$ Por el teorema 7.4.6, $\mid a \mid = p_1 \cdots p_r$ donde $r \geq 1$ y p_i es primo para $i = 1, \ldots, r$. Entonces cualquier primo que aparece en esta descomposición divide a $\mid a \mid$ y por lo tanto a a. $\blacksquare$

Como mencionamos al principio de esta sección, hay una infinidad de números primos:

Teorema 7.4.9. *El conjunto de números primos es infinito.*

Demostración. Supongamos que sólo hay un número finito de primos y sean estos $p_1, \ldots, p_n$. Sea $a = p_1 \cdot \ldots \cdot p_n + 1$. Por el corolario 7.4.8 existe un primo que divide a a. Entonces este primo debe ser p_i para alguna $i = 1, \ldots, n$. Luego $p_i \mid p_1 \cdot \ldots \cdot p_n + 1$ y $p_i \mid p_1 \cdot \ldots \cdot p_n$ implica $p_i \mid 1$ lo que es un absurdo. $\blacksquare$

Si denotamos los números primos $p_1, \ldots, p_n, \ldots$ de tal manera que si $i < j$, entonces $p_i < p_j$, obtenemos la sucesión ascendente de números primos:

$$p_1 = 2 < p_2 = 3 < p_3 = 5 < p_4 = 7 < \cdots \tag{2}$$

Con esta notación para los números primos, en la descomposición de un entero $a > 1$ como producto de primos podríamos hacer aparecer a todos los primos, considerando que si un primo p_i no divide a a, entonces p_i aparecerá con exponente cero. Entonces la expresión de a como producto de primos sería $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n} \cdot \ldots = \prod_{i=1}^{\infty} p_i^{\alpha_i}$ donde $\alpha_i \geq 0$ para toda $i = 1, 2, 3, \ldots$ y $\alpha_j = 0$ para toda j salvo un número finito. Es más, podemos incluir a 1, en cuyo caso $\alpha_i = 0$ para toda $i = 1, 2, 3, \ldots$. De esta manera cada entero mayor que cero tiene asociado una sucesión de números naturales $(\alpha_1, \alpha_2, \ldots, \alpha_n, \ldots)$ donde todos los elementos que aparecen en esta sucesión son cero salvo para un número finito. El orden es importante debido a que el i-ésimo número natural que aparece en la sucesión denota el exponente del i-ésimo número primo de la sucesión ascendente de números primos dada en (2), así que, dados $a = \prod_{i=1}^{\infty} p_i^{\alpha_i}$ y $b = \prod_{i=1}^{\infty} p_i^{\beta_i}$, por el teorema 7.4.7, $a = b$ si y sólo si $\alpha_i = \beta_i$ para toda $i = 1, 2, 3 \ldots$. Ahora dada una sucesión de números naturales $(\alpha_1, \alpha_2, \ldots, \alpha_n, \ldots)$ donde todos son cero salvo un número finito, ésta determina un único número entero mayor que cero, que es $\prod_{i=1}^{\infty} p_i^{\alpha_i}$.

Ejemplo 7.4.10. $1012 = 2^2 \cdot 11^1 \cdot 23^1$. Entonces $1012 = \prod_{i=1}^{\infty} p_i^{\alpha_i}$, donde $\alpha_1 = 2$, $\alpha_5 = 1$, $\alpha_9 = 1$ y $\alpha_i = 0$ para toda $i \neq 1, 5, 9$. La sucesión determinada por 1012 es $(2, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, \ldots)$.

Ejemplo 7.4.11. La sucesión $(0, 2, 0, 1, 0, 0, 0, 1, 0, 0, \ldots)$ determina al número entero $3^2 \cdot 7 \cdot 19 = 1197$.

Dados $a = \prod_{i=1}^{\infty} p_i^{\alpha_i}$ y $b = \prod_{i=1}^{\infty} p_i^{\beta_i}$, podemos determinar cuándo a divide a b en términos de sus sucesiones asociadas:

Proposición 7.4.12. *$a \mid b$ si y sólo si $\alpha_i \leq \beta_i$ para todo $i = 1, 2, 3, \ldots$.*

Demostración.

$\Longrightarrow$) Supongamos que $a \mid b$. Para $j = 1, 2, 3, \ldots$, $p_j^{\alpha_j} \mid a$ y por el teorema 7.1.5(6) $p_j^{\alpha_j} \mid b$. Ahora, como $\left(p_j^{\alpha_j}, \prod_{\substack{i=1 \\ i \neq j}}^{\infty} p_i^{\beta_i} \right) = 1$, entonces por el teorema 7.2.16 $p_j^{\alpha_j} \mid p_j^{\beta_j}$. Por lo tanto $p_j^{\alpha_j} \cdot x = p_j^{\alpha_j}$ para algún $x \in \mathbb{Z}$ y $x \mid p_j^{\alpha_j}$, lo que implica $x \mid p_j^s$ para algún $s \in \mathbb{N}$ (ejercicio 7.4.14) . Esto es, $p_j^{\alpha_j} p_j^s = p_j^{\beta_j}$ y por el teorema 7.4.7 $\alpha_j + s = \beta_j$. Luego $\alpha_j \leq \beta_j$ $j = 1, 2, 3, \ldots$.

$\Longleftarrow$) Supongamos que para todo $j = 1, 2, 3, \ldots$, $\alpha_j \leq \beta_j$. Entonces $p_j^{\alpha_j} \mid p_j^{\beta_j}$ para todo $j = 1, 2, 3, \ldots$. Si $\alpha_{j_1}, \ldots, \alpha_{j_m}$ son todos los exponentes mayores que cero, aplicando repetidamente el teorema 7.2.17, obtenemos

$$p_{j_1}^{\alpha_{j_1}} \cdot \ldots \cdot p_{j_m}^{\alpha_{j_m}} \mid p_{j_1}^{\beta_{j_1}} \cdot \ldots \cdot p_{j_m}^{\beta_{j_m}}$$

y por lo tanto $p_{j_1}^{\alpha_{j_1}} \cdot \ldots \cdot p_{j_m}^{\alpha_{j_m}} \mid b$, es decir, $a \mid b$. ∎

Sean $a = \prod_{i=1}^{\infty} p_i^{\alpha_i}$ y $b = \prod_{i=1}^{\infty} p_i^{\beta_i}$, los exponentes del m.c.d. y el m.c.m. pueden expresarse en términos de α_i y β_i:

Proposición 7.4.13. *Sean* $a = \prod_{i=1}^{\infty} p_i^{\alpha_i}$ *y* $b = \prod_{i=1}^{\infty} p_i^{\beta_i}$. *Entonces*

(1) $(a, b) = \prod_{i=1}^{\infty} p_i^{\gamma_i}$ *donde* $\gamma_i = \min\{\alpha_i, \beta_i\}$ *para todo* $i = 1, 2, 3, \ldots$.

(2) $[a, b] = \prod_{i=1}^{\infty} p_i^{\delta_i}$ *donde* $\delta_i = \max\{\alpha_i, \beta_i\}$ *para todo* $i = 1, 2, 3, \ldots$.

La demostración queda como ejercicio (véase ejercicio 7.4.42)
El siguiente resultado es una buena aplicación de la proposición 7.4.13.

Proposición 7.4.14. *Sean* $a, b, c \in \mathbb{Z} - \{0\}$. *Entonces* $([a, b], c) = [(a, c), (b, c)]$.

Demostración. Sean $a = \prod_{i=1}^{\infty} p_i^{\alpha_i}$, $b = \prod_{i=1}^{\infty} p_i^{\beta_i}$ y $c = \prod_{i=1}^{\infty} p_i^{\gamma_i}$. Entonces, por la proposición 7.4.13, $([a, b], c) = \prod_{i=1}^{\infty} p_i^{\delta_i}$ donde $\delta_i = \min\{\max\{\alpha_i, \beta_i\}, \gamma_i\}$ y $[(a, c), (b, c)] = \prod_{i=1}^{\infty} p_i^{\rho_i}$ donde $\rho_i = \max\{\min\{\alpha_i, \gamma_i\}, \min\{\beta_i, \gamma_i\}\}$.

Para demostrar que $([a,b],c) = [(a,c),(b,c)]$ basta ver que $\delta_i = \rho_i$ para toda $i = 1,2,3,\ldots$, que es $\min\{\max\{\alpha_i,\beta_i\},\gamma_i\} = \max\{\min\{\alpha_i,\gamma_i\},\min\{\beta_i,\gamma_i\}\}$ para toda $i = 1,2,3,\ldots$.
Como α_i y β_i juegan un papel simétrico, es suficiente suponer $\alpha_i \leq \beta_i$. Existen tres casos:

(1) $\gamma_i \leq \alpha_i \leq \beta_i$
$\min\{\max\{\alpha_i,\beta_i\},\gamma_i\} = \min\{\beta_i,\gamma_i\} = \gamma_i$
$\max\{\min\{\alpha_i,\gamma_i\},\min\{\beta_i,\gamma_i\}\} = \max\{\gamma_i,\gamma_i\} = \gamma_i$
(2) $\alpha_i \leq \gamma_i \leq \beta_i$
$\min\{\max\{\alpha_i,\beta_i\},\gamma_i\} = \min\{\beta_i,\gamma_i\} = \gamma_i$
$\max\{\min\{\alpha_i,\gamma_i\},\min\{\beta_i,\gamma_i\}\} = \max\{\alpha_i,\gamma_i\} = \gamma_i$
(3) $\alpha_i \leq \beta_i \leq \gamma_i$
$\min\{\max\{\alpha_i,\beta_i\},\gamma_i\} = \min\{\beta_i,\gamma_i\} = \beta_i$
$\max\{\min\{\alpha_i,\gamma_i\},\min\{\beta_i,\gamma_i\}\} = \max\{\alpha_i,\beta_i\} = \beta_i$. ∎

Esta última proposición se usará en la demostración del teorema 7.6.10.

§ 7.5. Congruencias

La definición de congruencia se da a través de la divisibilidad. Este concepto es muy importante en la teoría de números, entre otras cosas, nos permite describir propiedades cuyas demostraciones resultan más sencillas y un ejemplo de esto es el teorema de Fermat: Si p es un número primo y $(a,p) = 1$, entonces $p \mid a^{p-1} - 1$. Es importante destacar que con el uso de congruencias podemos dar muchos ejemplos de campos (véase 7.7.14), los cuales serán muy distintos de los que conocemos: $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$. Es más cada uno de estos campos será finito.

Definición 7.5.1. *Sean $m,a,b \in \mathbb{Z}$ con $m > 0$. Diremos que* ***a* es congruente con *b* módulo *m*** *si $m \mid a - b$ y en este caso lo denotaremos por* $\boldsymbol{a \equiv b}$ **(mód *m*)**. *En caso contrario, es decir, si $m \nmid a - b$, diremos que a es incongruente con b y lo denotamos $a \not\equiv b$* (mód m).

Ejemplo 7.5.2. $21 \equiv 13$ (mód 4) ya que $4 \mid 21 - 13 = 8$. Por otra parte, $29 \not\equiv 34$ (mód 7) ya que $7 \nmid 29 - 34 = -5$.

La relación que hemos definido en $\mathbb{Z}$ a través de la congruencia módulo m es de equivalencia y gracias a este hecho podremos construir los campos de los que hablamos en la introducción de esta sección.

Teorema 7.5.3. *Congruencia módulo m es una relación de equivalencia en* $\mathbb{Z}$.

Demostración. Es consecuencia de las propiedades de divisibilidad ya vistas.

(*i*) $a \equiv a \pmod{m}$ para todo a puesto que $m \mid a - a = 0$.
(*ii*) $a \equiv b \pmod{m}$ implica $m \mid a - b$. Luego $m \mid -(a - b) = b - a$ y por lo tanto $b \equiv a \pmod{m}$.
(*iii*) Como $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$ implica $m \mid a - b$ y $m \mid b - c$. Luego $m \mid (a - b) + (b - c) = a - c$ y entonces $a \equiv c \pmod{m}$. ∎

En el siguiente teorema se muestra cómo la congruencia módulo m se comporta como la igualdad, en el sentido de que se pueden sumar, restar o multiplicar. Cuando consideramos $a \equiv b \pmod{m}$, supondremos que $a, b, m \in \mathbb{Z}$, $m > 0$.

Teorema 7.5.4. *Si* $a \equiv b \pmod{m}$ *y* $c \equiv d \pmod{m}$, *entonces*

(1) $a + c \equiv b + d \pmod{m}$
(2) $a \cdot c \equiv b \cdot d \pmod{m}$.

Demostración. $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$ implican $m \mid a - b$ y $m \mid c - d$ respectivamente. Entonces

(1) $m \mid (a - b) + (c - d) = (a + c) - (b + d)$ y por lo tanto $a + c \equiv b + d \pmod{m}$.
(2) $m \mid (a - b) \cdot (c - d) = a \cdot c - a \cdot d - b \cdot c + b \cdot d$. Pero

$$a \cdot c - a \cdot d - b \cdot c + b \cdot d = (a \cdot c - b \cdot d) - (a - b) \cdot d - (c - d) \cdot b$$

y como $m \mid -(a-b) \cdot d - (c-d) \cdot b$ porque $m \mid -(a-b) \cdot d$ y $m \mid (c-d) \cdot b$, entonces $m \mid a \cdot c - b \cdot d$ y así $a \cdot c \equiv b \cdot d \pmod{m}$. ∎

Corolario 7.5.5. *Si* $a \equiv b \pmod{m}$ *y* $t \in \mathbb{Z}$, *entonces*

(1) $a + t \equiv b + t \pmod{m}$
(2) $a \cdot t \equiv b \cdot t \pmod{m}$
(3) $a^n \equiv b^n \pmod{m}$, *para toda* $n \in \mathbb{N}$.

Demostración. Para (1) y (2) los resultados se obtienen al considerar $a \equiv b \pmod{m}$ y $t \equiv t \pmod{m}$ y aplicar el teorema 7.5.4 y (3) se demuestra por inducción sobre n y usando el teorema 7.5.4 inciso (2). ∎

El siguiente es un buen ejemplo de la aplicación de las propiedades de congruencias:

Ejemplo 7.5.6. Supongamos que deseamos saber si un entero x es divisible por 3. Sin realizar la división podemos responder esta pregunta: si $(x)_{10} = a_k a_{k-1} \cdots a_0$

(donde $0 \leq a_i \leq 9$ para $i = 0, \ldots, k$), entonces

$$x = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0.$$

Como

$$10 \equiv 1 \ (\text{mód } 3) \qquad \text{(por definición)},$$

también

$$10^i \equiv 1 \ (\text{mód } 3) \qquad \text{(corolario7.5.5 (2))},$$

y

$$a_i 10^i \equiv a_i \ (\text{mód } 3) \qquad \text{(corolario7..5.4 (3))}$$

y entonces por el teorema 7.5.4

$$x = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0 \equiv a_k + a_{k-1} + \cdots + a_1 + a_0 \ (\text{mód } 3).$$

Por lo tanto

$$x \equiv 0 \ (\text{mód } 3) \quad \textit{si y sólo si} \quad a_k + a_{k-1} + \cdots + a_1 + a_0 \equiv 0 \ (\text{mód } 3).$$

Resumiendo, para saber si un entero x es divisible por 3 basta verificar que 3 divide a la suma de los dígitos que aparecen en él. Por ejemplo, si $x = 3728957$, entonces $3 + 7 + 2 + 8 + 9 + 5 + 7 = 41$, así que $3 \mid x$ si y sólo si $3 \mid 41$. Pero también $3 \mid 41$ si y sólo si $3 \mid 4 + 1 = 5$ y como esto último no es cierto entonces $3 \nmid 3728957$. En cambio para $x = 25987251$,

$$2 + 5 + 9 + 8 + 7 + 2 + 5 + 1 = 39$$

que es divisible por 3. Entonces $3 \mid 25987251$.

A partir de algunas congruencias se pueden establecer otras módulo otro entero $m' > 0$.

Teorema 7.5.7. *Sean $a, b, t, m \in \mathbb{Z}$, con $m, t > 0$.*

(1) *Si $a \equiv b$ (mód m), entonces $a \cdot t \equiv b \cdot t$ (mód $m \cdot t$).*
(2) *Si $a \equiv b$ (mód m) y $t \mid m$, entonces $a \equiv b$ (mód t).*
(3) *Si $a \equiv b$ (mód m) y $d = (a, b, m)$, entonces $\frac{a}{d} \equiv \frac{b}{d}$ (mód $\frac{m}{d}$).*
(4) *Si $t \cdot a \equiv t \cdot b$ (mód m), entonces $a \equiv b$ (mód $\frac{m}{d}$), donde $d = (t, m)$.*
(5) *Sean $m_1, \ldots, m_k$ enteros mayores que cero. $a \equiv b$ (mód m_i) para todo $i = 1, \ldots, k$ si y sólo si $a \equiv b$ (mód $[m_1, \ldots, m_k]$)*

Demostración. (1) y (2) son consecuencia de (9) y (6) respectivamente del teorema 7.1.5.

(3) Si $m \cdot q = a - b$ donde $q \in \mathbb{Z}$, entonces $d\left(\frac{m}{d}\right) q = d\left(\frac{a}{d} - \frac{b}{d}\right)$. Luego $\frac{m}{d} \cdot q = \frac{a}{d} - \frac{b}{d}$ y por lo tanto $\frac{a}{d} \equiv \frac{b}{d}$ (mód $\frac{m}{d}$).
(4) $t \cdot a \equiv t \cdot b$ (mód m) implica que $m \cdot q = t(a - b)$ para alguna $q \in \mathbb{Z}$. Entonces $\frac{m}{d} \cdot q = \frac{t}{d}(a - b)$, y debido a que $\left(\frac{m}{d}, \frac{t}{d}\right) = 1$ por el corolario 7.2.12, se tiene que $\frac{m}{d} \mid a - b$. Luego $a \equiv b$ (mód $\frac{m}{d}$).
(5) $\Longleftarrow$) Supongamos $a \equiv b$ (mód $[m_1, \ldots, m_k]$). Por ser $[m_1, \ldots, m_k]$ el m.c.m. de $m_1, \ldots, m_k$, entonces $m_i \mid [m_1, \ldots, m_k]$ para $i = 1, \ldots, k$, y por el inciso (2), $a \equiv b$ (mód m_i) para toda $i = 1, \ldots, k$.
$\Longrightarrow$) Supongamos $a \equiv b$ (mód m_i) para toda $i = 1, \ldots, k$. Luego $m_i \mid a - b$ para toda $i = 1, \ldots, k$. Entonces, por la definición de m.c.m. $[m_1, \ldots, m_k] \mid a - b$. ∎

La afirmación inversa del inciso (2) del corolario 7.5.5 en general no es cierta, por ejemplo $9 \cdot 5 \equiv 9 \cdot 4$ (mód 3) pero $5 \not\equiv 4$ (mód 3). Sin embargo, si $t \cdot a \equiv t \cdot b$ (mód m) y $(t, m) = 1$, entonces $a \equiv b$ (mód m) (inciso (4)).

Definición 7.5.8. *Sea $m \in \mathbb{Z}$, $m > 0$. El conjunto $\{a_1, \ldots, a_r\} \subseteq \mathbb{Z}$ es un* **conjunto completo de representantes módulo *m*** *si*

(*i*) $a_i \not\equiv a_j$ (mód m) *para cualquier* $i, j = 1, \ldots, r$ *con* $i \neq j$.
(*ii*) *Dado* $a \in \mathbb{Z}$, $a \equiv a_i$ (mód m) *para alguna* $i = 1, \ldots, r$.

Ejemplo 7.5.9. Sea $m \in \mathbb{Z}$, $m > 0$. $\{0, 1, \ldots, m - 1\}$ es un conjunto completo de representantes módulo m:

(*i*) Si $i \equiv j$ (mód m) con $i, j \in \{0, 1, \ldots, m - 1\}$ entonces $m \mid i - j$ y como $|i - j| \leq m - 1$ por el lema 7.1.9, entonces debe ser $i = j$.
(*ii*) Sea $a \in \mathbb{Z}$. Por el algoritmo de la división $a = m \cdot q + k$, donde $0 \leq k < m$. Pasando a congruencia módulo m obtenemos $a \equiv m \cdot q + k \equiv k$ (mód m), donde $k \in \{0, 1, \ldots, m - 1\}$

Teorema 7.5.10. *Si $\{a_1, \ldots, a_r\}$ y $\{b_1, \ldots, b_s\}$ son dos conjuntos completos de representantes módulo m, entonces $r = s$.*

Demostración. Por ser $\{b_1, \ldots, b_s\}$ un conjunto completo de representantes módulo m, para cada $i = 1, \ldots, r$ existe j_i, $1 \leq j_i \leq s$, tal que $a_i \equiv b_{j_i}$ (mód m) y como las a_i son incongruentes entre sí módulo m, entonces también las b_{j_i} y por lo tanto $r \leq s$. La otra desigualdad, $s \leq r$, se obtiene usando el mismo argumento. ∎

Corolario 7.5.11. *Sea $m \in \mathbb{Z}$, $m > 0$. Cada conjunto completo de representantes módulo m tiene exactamente m elementos.*

Demostración. Se sigue del ejemplo 7.5.9 y el teorema 7.5.10. ∎

En el caso en que el módulo es un primo se obtienen algunas propiedades muy interesantes.

Teorema 7.5.12. *Sean $a_1, \ldots, a_k \in \mathbb{Z}$ y p primo. Entonces*

$$(a_1 + \cdots + a_k)^p \equiv a_1^p + \cdots + a_k^p \pmod{p}$$

Demostración. Por inducción sobre k.

1°/ $k = 1$. Es claro ya que $a_1^p \equiv a_1^p \pmod{p}$.

2°/ $k = 2$. Demostraremos este caso puesto que lo utilizaremos en el paso inductivo.

Por el teorema del binomio, $(a_1 + a_2)^p = \sum_{i=0}^{p} C_p^i a_1^{p-i} a_2^i$, donde $C_p^0 = C_p^p = 1$ y para $i = 1, \ldots, p-1$, $C_p^i = \frac{p!}{i!(p-i)!} \in \mathbb{Z}$. Esto es $i!(p-i)! \mid p! = p \cdot (p-1)!$ y como $(i!(p-i)!, p) = 1$ ya que el factor $i!(p-i)!$ no es divisible por p, entonces $i!(p-i)! \mid (p-1)!$ para cada $i = 1, \ldots, p-1$. Luego $C_p^i = p \cdot \frac{(p-1)!}{i!(p-i)!}$ para $i = 1, \ldots, p-1$ y así $C_p^i \equiv 0 \pmod{p}$ para $i = 1, \ldots, p-1$ y por lo tanto

$$(a_1 + a_2)^p \equiv a_1^p + a_2^p \pmod{p}$$

3°/ Sea $k \geq 3$ y suponemos cierto el teorema para $k-1$. Entonces

$$\begin{aligned} ((a_1 + \cdots + a_{k-1}) + a_k)^p &\equiv (a_1 + \cdots + a_{k-1})^p + a_k^p \pmod{p} \\ &\equiv a_1^p + \cdots + a_{k-1}^p + a_k^p \pmod{p}. \end{aligned}$$ ∎

Nota 7.5.13. Si p es primo, entonces $(-1)^p \equiv -1 \pmod{p}$. Cuando p es impar esto es claro y cuando $p = 2$, $(-1)^2 \equiv 1 \equiv -1 \pmod{2}$.

El siguiente resultado es consecuencia del último teorema.

Teorema 7.5.14. *Sea p primo. Entonces $a^p \equiv a \pmod{p}$ para todo entero a.*

Demostración. Para $a = 0$ o $a = 1$, la congruencia es clara, así que supongamos $a > 1$. Entonces $a = \underbrace{1 + \cdots + 1}_{a \text{ veces}}$ y por el teorema 7.5.12,

$$a^p = (1 + \cdots + 1)^p \equiv 1^p + \cdots + 1^p = a \pmod{p}.$$

Ahora si $a < 0$, $a = -\underbrace{(1 + \cdots + 1)}_{|a| \text{ veces}}$ y teniendo en cuenta $(-1)^p \equiv -1 \pmod{p}$, entonces $a^p = (-1)^p (1 + \cdots + 1)^p \equiv -(1 + \cdots + 1) = a \pmod{p}$. ∎

Una pequeña variación de teorema 7.5.14 es el conocido teorema de Fermat.

Teorema 7.5.15. *(teorema de Fermat) Si p es primo y $(a, p) = 1$, entonces*

$$a^{p-1} \equiv 1(\text{ mód } p).$$

Demostración. Del teorema 7.5.14 $a^p - a = a\left(a^{p-1} - 1\right) \equiv 0$ (mód p) y esto implica que $p \mid a \cdot (a^{p-1} - 1)$. Pero como $(a, p) = 1$, entonces $p \mid a^{p-1} - 1$, es decir, $a^{p-1} \equiv 1$ (mód p). ∎

§ 7.6. Congruencias lineales y sistemas de congruencias

En la sección 7 estudiamos la ecuación diofantina $ax + by = c$ y dimos un criterio para saber cuándo una ecuación de este tipo tiene solución en $\mathbb{Z}$ y no sólo eso, justo que en el caso de que tenga solución, se exhibió un método para encontrar todas las soluciones.

Definición 7.6.1. *Una congruencia del tipo* $\boldsymbol{ax \equiv b \pmod{m}}$ *se llama* **congruencia lineal** *y $x_0 \in \mathbb{Z}$ será solución de ella si satisface la congruencia, es decir, $ax_0 \equiv b$ (mód m).*

Consideremos la congruencia lineal $ax \equiv b$ (mód m). Si $x_0 \in \mathbb{Z}$ es una solución de la congruencia, entonces $ax_0 \equiv b$ (mód m) y por lo tanto $ax_0 - my_0 = b$ para alguna $y_0 \in \mathbb{Z}$, lo que significa que (x_0, y_0) es una solución de la ecuación diofantina $ax - my = b$. Inversamente, si (x_0, y_0) es una solución de $ax - my = b$ entonces $ax_0 \equiv b$ (mód m). Resumiendo, $ax \equiv b$ (mód m) tiene solución si y sólo si $ax - my = b$ tiene solución. Pero esta última ecuación, por el teorema 7.3.4 tiene solución si y sólo si $(a, m) \mid b$. Entonces

Teorema 7.6.2. *La congruencia lineal $ax \equiv b$ (mód m) tiene solución en $\mathbb{Z}$ si y sólo si $(a, m) \mid b$.*

Proposición 7.6.3. *Si $a \equiv a'$ (mód m) y $b \equiv b'$ (mód m), entonces las congruencias $ax \equiv b$ (mód m) y $a'x \equiv b'$ (mód m) tienen las mismas soluciones.*

Demostración. Si $x_0 \in \mathbb{Z}$ es solución de $ax \equiv b$ (mód m), entonces se cumple que $ax_0 \equiv b$ (mód m). Luego por las propiedades de la congruencia tenemos que

$$a'x_0 \equiv ax_0 \equiv b \equiv b' \text{ (mód } m)$$

Análogamente si x_0 es solución de $a'x \equiv b'$ (mód m). ∎

Lema 7.6.4. *Si x_0 es un solución de $ax \equiv b \pmod m$ y $x_0 \equiv x_1 \pmod m$, entonces x_1 también es una solución de la congruencia.*

Demostración. $x_0 \equiv x_1 \pmod m$ implica que $x_0 - x_1 = m \cdot r$ para alguna $r \in \mathbb{Z}$. Entonces $a(x_0 - x_1) = a \cdot m \cdot r \equiv 0 \pmod m$. Luego $ax_0 \equiv ax_1 \pmod m$. Pero $ax_0 \equiv b \pmod m$ y por lo tanto $ax_1 \equiv b \pmod m$. ∎

Según este último lema, x_0 es una solución de $ax \equiv b \pmod m$ si y sólo si $x_0 + m \cdot k$ es solución para toda $k \in \mathbb{Z}$.

Teorema 7.6.5. *Sea x_0 una solución de $ax \equiv b \pmod m$ y sea $d = (a, m)$. Entonces*

$$x_0, \quad x_0 + \frac{m}{d}, \ \ldots \ , \quad x_0 + \frac{m}{d} \cdot (d-1)$$

son también soluciones de la congruencia que satisfacen $x_0 + \frac{m}{d} \cdot i \not\equiv x_0 + \frac{m}{d} \cdot j \pmod m$ si $i \neq j, 0 \leq i, j \leq d-1$ y si x_0' es cualquier solución de la congruencia, entonces
$x_0' \equiv x_0 + \frac{m}{d} \cdot j \pmod m$ para alguna $j = 0, \ldots, d-1$.

Demostración. $a\left(x_0 + \frac{m}{d} i\right) \equiv ax_0 + a\frac{m}{d} i \equiv b + \frac{a}{d} mi \equiv b \pmod m$. Si

$$x_0 + \frac{m}{d} \cdot i \equiv x_0 + \frac{m}{d} \cdot j \pmod m,$$

entonces $\frac{m}{d} \cdot i \equiv \frac{m}{d} \cdot j \pmod m$ y por el teorema 7.5.7(4), dividiendo en la congruencia por $\frac{m}{d} = \left(\frac{m}{d}, m\right)$ obtenemos $i \equiv j \pmod d$ y como $0 \leq i, j \leq d-1$, debe ser $i = j$. Ahora, si x_0' es cualquier solución, entonces $ax_0' \equiv b \equiv ax_0 \pmod m$ por lo que $x_0' \equiv x_0 \pmod{\frac{m}{d}}$. Luego, para alguna $k \in \mathbb{Z}$ y expresando este k como $k = dq + j, 0 \leq j < d$, se tiene $x_0' = x_0 + \frac{m}{d} k = x_0 + \frac{m}{d}(dq + j) = x_0 + mq + \frac{m}{d} j \equiv x_0 + \frac{m}{d} j \pmod m$. ∎

Entonces el conjunto de soluciones de una congruencia lineal la podemos describir a través de un conjunto finito de soluciones y en este sentido diremos que la congruencia tiene d soluciones incongruentes módulo m.

Corolario 7.6.6. *Si la ecuación $ax \equiv b \pmod m$ tiene solución, entonces tiene exactamente (a, m) soluciones incongruentes entre sí módulo m.*

Ejemplo 7.6.7. La congruencia $8x \equiv 6 \pmod{14}$ tiene exactamente

$$2 = (8, 14)$$

soluciones incongruentes entre sí módulo 14. Para encontrar todas ellas, debemos dar una solución particular y para esto debemos encontrar una solución de $8x - 14y = 6$ para lo cual se puede aplicar el método dado en la sección 7.3. Después de hacer esto llegamos a que $x = 6$ y $y = 3$) es solución. Entonces sólo hay dos soluciones incongruentes entre sí módulo 14 y son $x_0 = 6$ y $x_1 = 6 + 7 \cdot 1 = 13$.

Una persona ha dejado como herencia a 7 familiares cierto número x de automóviles con la condición de que no fueran vendidos. Al tratar de repartirla por partes iguales resultó que sobraban dos autos y como ninguno aceptó (!oh condición humana¡) que hubiese algunos que recibieran más que otros, mientras discutían una posible solución, uno de ellos renunció (se sacó la lotería), lo que redujo el número a 6. Sin embargo, al hacer nuevamente el reparto resultó que sobraban 3 autos. Después de un tiempo sin lograr ponerse de acuerdo uno de los herederos murió, quedando 5 para la repartición. Afortunadamente para ellos, al hacer el reparto no sobró ningún auto. ¿Cuáles son las posibilidades para x? Sabemos que en el primer intento de repartición sobraron 2 autos, así que $7 \mid x - 2$, en el segundo sobraron 3, por lo que $6 \mid x - 3$ y en el último no sobró ninguno, es decir, $5 \mid x$. Conclusión: x debe satisfacer cada una de las siguientes congruencias lineales

$$\begin{aligned} x &\equiv 2 \pmod 7 \\ x &\equiv 3 \pmod 6 \\ x &\equiv 0 \pmod 5 \end{aligned}$$

Estudiaremos el problema en general.
Consideramos el sistema de congruencias lineales

$$\left\{\begin{array}{rcl} x & \equiv & a_1 \pmod{m_1} \\ x & \equiv & a_2 \pmod{m_2} \\ & \vdots & \\ x & \equiv & a_k \pmod{m_k} \end{array}\right. \tag{3}$$

Definición 7.6.8*. Un entero x_0 es una* ***solución del sistema de congruencias*** *(3) si x_0 es solución da cada una de ellas, es decir, $x_0 \equiv a_i \pmod{m_i}$ para toda $i = 1, \ldots, k$.*

No todo sistema de congruencias tiene solución como se muestra en el siguiente ejemplo.

Ejemplo 7.6.9. Considere el siguiente sistema de congruencias lineales

$$\begin{aligned} x &\equiv 3 \text{ (mód } 6) \\ x &\equiv 1 \text{ (mód } 9) \end{aligned}$$

Si este sistema tuviera solución x_0, entonces $x_0 \equiv 3$ (mód 6) y $x_0 \equiv 1$ (mód 9), esto es, $6 \mid x_0 - 3$ y $9 \mid x_0 - 1$, pero esto implica que $3 = (6, 9) \mid x_0 - 3$ y $3 \mid x_0 - 1$ y por lo tanto se debe tener que $3 \mid (x_0 - 1) - (x_0 - 3) = 2$ lo que es imposible, así que el sistema no puede tener solución.

Analizando el último ejemplo observamos que una condición necesaria para que el sistema (3) tenga solución es que $(m_i, m_j) \mid a_i - a_j$ para cualesquiera $i, j = 1, \ldots, k$. Demostraremos que esta condición también es suficiente.
Recordemos que $[m_1, \ldots, m_k]$ denota el m. c. m. de $m_1, \ldots, m_k$.

Teorema 7.6.10. *El sistema de congruencias lineales (3) tiene solución si y sólo si para cualesquiera* $i, j = 1, \ldots, k$, $(m_i, m_j) \mid a_i - a_j$. *En este caso la solución es única módulo* $[m_1, \ldots, m_k]$.

Demostración. Si el sistema tiene solución x_0, entonces para cualesquiera $i, j = 1, \ldots k$, se tiene que $m_i \mid x_0 - a_i$ y $m_j \mid x_0 - a_j$, luego $(m_i, m_j) \mid x_0 - a_i$ y $(m_i, m_j) \mid x_0 - a_j$ y por lo tanto $(m_i, m_j) \mid a_i - a_j$.
Supongamos ahora que $(m_i, m_j) \mid a_i - a_j$ para cualesquiera $i, j = 1, \ldots, k$.
La idea de la demostración será exhibir un mecanismo para pasar de las k congruencias lineales a un sistema de $k - 1$ congruencias lineales sin perder la hipótesis de que el m.c.d. de cualesquiera dos de los módulos divide a la diferencia correspondiente y tal que el conjunto de soluciones de ambos sistemas es el mismo. De esta manera podremos ir disminuyendo el número de congruencias lineales hasta llegar a una sola congruencia cuyas soluciones serán precisamente todas las soluciones del sistema original.
Consideramos las dos primeras congruencias

$$x \equiv a_1 \text{ (mód } m_1) \ \ y \ \ x \equiv a_2 \text{ (mód } m_2).$$

Deberemos sustituir estas dos congruencias por una sola de tal manera que las soluciones de esta última sean exactamente las soluciones simultaneas de las dos congruencias iniciales. Es claro que si buscamos las soluciones comunes, del conjunto de soluciones de la primera congruencia debemos buscar aquellas que también sean solución de la segunda. Como los enteros de la forma $x = a_1 + m_1 y$ para cualquier entero y son todas las soluciones de $x \equiv a_1$ (mód m_1) encontremos

los enteros y para los cuales $a_1 + m_1 y$ es solución de $x \equiv a_2$ (mód m_2), esto es, $a_1 + m_1 y \equiv a_2$ (mód m_2). Debemos resolver entonces la congruencia lineal

$$m_1 y \equiv a_2 - a_1 \ (\text{mód } m_2).$$

Por hipótesis $(m_1, m_2) \mid a_1 - a_2$, así que la congruencia tiene solución y todas las soluciones están dada por $y = x_0 + \frac{m_2}{(m_1, m_2)} z$ para cualquier entero z y x_0 solución particular.
Por lo tanto las soluciones comunes son los enteros

$$x = a_1 + m_1 y = a_1 + m_1 \left(x_0 + \frac{m_2}{(m_1, m_2)} z \right) = a_1 + m_1 x_0 + \frac{m_1 \cdot m_2}{(m_1, m_2)} z = a_1 + m_1 x_0 + [m_1, m_2] z,$$

o lo que es lo mismo $x \equiv a_1 + m_1 x_0 \pmod{[m_1, m_2]}$.
Consideramos ahora el nuevo sistema de $(k-1)$ congruencias lineales

$$(4) \qquad \begin{cases} x \equiv a_1 + m_1 x_0 & (\text{mód } [m_1, m_2]) \\ x \equiv a_3 & (\text{mód } m_3) \\ \quad \vdots & \\ x \equiv a_k & (\text{mód } m_k) \end{cases}$$

Queda claro que este nuevo sistema y el original tienen el mismo conjunto de soluciones, así que para terminar con esta demostración sólo debemos verificar que las hipótesis prevalecen en este nuevo sistema y para esto es suficiente ver que $\big([m_1, m_2], m_j\big) \mid a_1 + m_1 x_0 - a_j$ para toda $j = 3, \ldots, k$ puesto que las otras posibilidades permanecen sin cambio, que es, $(m_i, m_j) \mid a_i - a_j$ para cualesquiera $i, j = 3, \ldots, k$. Ahora, por la proposición 7.4.14

$$\big([m_1, m_2], m_j\big) = \big[(m_1, m_j), (m_2, m_j)\big],$$

así que basta demostrar que tanto (m_1, m_j) como (m_2, m_j) dividen a

$$a_1 + m_1 x_0 - a_j,$$

pues de esto se tendrá entonces que $\big[(m_1, m_j), (m_2, m_j)\big] \mid a_1 + m_1 x_0 - a_j$. Y dado que $(m_1, m_j) \mid a_1 - a_j$ y $(m_1, m_j) \mid m_1 x_0$, entonces $(m_1, m_j) \mid a_1 - a_j + m_1 x_0$. En el otro caso, debido a que $a_1 + m_1 x_0$ es solución de $x \equiv a_2$ (mód m_2), se tiene que $m_2 \mid a_1 + m_1 x_0 - a_2$ y por lo tanto $(m_2, m_j) \mid a_1 + m_1 x_0 - a_2$. Además por hipótesis $(m_2, m_j) \mid a_2 - a_j$, luego $(m_2, m_j) \mid a_1 + m_1 x_0 - a_2 + a_2 - a_j = a_1 + m_1 x_0 - a_j$.

Continuando de esta manera, el sistema (4) de $k-1$ congruencias puede ser sustituido por un sistema de $k-2$ congruencias

$$\begin{cases} x \equiv a \pmod{[m_1, m_2, m_3]} \\ x \equiv a_4 \pmod{m_4} \\ \quad \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

sin que el conjunto de soluciones cambie y en el que permanece la hipótesis. Finalmente con este procedimiento llegamos a una sola congruencia

$$x \equiv b \ ([m_1, \ldots, m_k])$$

cuyas soluciones serán precisamente las soluciones del sistema original y por lo que también se concluye que es única módulo $([m_1, \ldots, m_k])$. ■

En realidad el teorema 7.6.10 es una generalización de un resultado conocido como el *teorema chino del residuo* el cual, aunque es un corolario del teorema 7.6.10, lo presentamos como teorema:

Teorema 7.6.11. ***Teorema chino del residuo***. *Sean $m_1, \ldots, m_k$ enteros tales que $(m_i, m_j) = 1$ si $i \neq j$. El sistema de congruencias*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

siempre tiene solución y es única módulo $m_1 \cdot \ldots \cdot m_k$.

Demostración. Como para cualesquiera m_i, m_j; distintos $(m_i, m_j) = 1$, se satisfacen entonces las hipótesis del teorema 7.6.10, luego el sistema tiene solución la cual es única módulo $[m_1, \ldots, m_k] = m_1 \cdot \ldots \cdot m_k$. ■

Ejemplo 7.6.12. Consideramos el sistema de congruencias lineales

$$\begin{cases} x \equiv 10 \pmod{12} \\ x \equiv 7 \pmod{15} \\ x \equiv 4 \pmod{18} \end{cases}$$

El sistema tiene solución puesto que

$$(12, 15) = 3 \mid 10 - 7 = 3, \quad (12, 18) = 6 \mid 10 - 4 = 6 \quad y \quad (15, 18) = 3 \mid 7 - 4 = 3.$$

Las soluciones de $x \equiv 10 \pmod{12}$ están dada por $x = 10 + 12y$ para toda $y \in \mathbb{Z}$. Veamos ahora para qué y, x también es solución de la segunda congruencia: $10 + 12y \equiv 7 \pmod{15}$, es decir $12y \equiv 7 - 10 = -3 \pmod{15}$. $y = 1$ es solución de esta congruencia y por lo tanto, por el teorema 7.6.5 las soluciones son $y = 1 + \frac{15}{3}z$ para toda $z \in \mathbb{Z}$. Entonces

$$x = 10 + 12y = 10 + 12(1 + 5z) = 10 + 12 + 60z$$

o lo que es lo mismo $x \equiv 22 \pmod{60}$ son todas las soluciones simultáneas de las dos primeras congruencias, con lo que el nuevo sistema a resolver es

$$\begin{cases} x \equiv 22 \pmod{60} \\ x \equiv 4 \pmod{18} \end{cases}$$

Nuevamente las soluciones de la primera congruencia son $x = 22 + 60y$ para todo $y \in \mathbb{Z}$. Ahora

$$22 + 60y \equiv 4 \pmod{18}$$

es equivalente a

$$60y \equiv 4 - 22 = -18 \equiv 0 \pmod{18}.$$

Así que como $y = 0$ es un solución de $60y \equiv 0 \pmod{18}$, entonces las soluciones de este son $y = 0 + \frac{18}{(60,18)}z = \frac{18}{6}z = 3z$. Entonces

$$x = 22 + 60y = 22 + 60(3z) = 22 + 180z$$

son todas las soluciones comunes, esto es, $x \equiv 22 \pmod{180}$. Es decir todas las soluciones del sistema son todas las x tales que $x \equiv 22 \pmod{180}$.

§ 7.7. El anillo $\mathbb{Z}_m$

En el teorema 7.5.3 se demostró que la congruencia módulo m es un relación de equivalencia en $\mathbb{Z}$. En esta sección trabajaremos con la partición asociada (conjunto de clases de equivalencia) a esta relación (proposición 1.6.18) a la que daremos estructura de anillo donde las operaciones estarán definidas a través de las operaciones de $\mathbb{Z}$. Entonces para cada entero $m > 0$ estaremos construyendo un anillo. Estos anillos son muy diferentes al anillo de los enteros. Para empezar todos serán finitos y no sólo para una gran cantidad de ellos estos anillos serán dominios enteros (que hasta el momento no teníamos ejemplos de éstos), que resultan ser campos con lo cual también tendremos ejemplos de campos finitos que por supuesto son muy distintos a los campos que también estudiaremos en este libro: $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$.

Denotaremos por $\mathbb{Z}_m$ al conjunto de todas las clases de equivalencia módulo m y entenderemos por $\overline{a}$ la clase de equivalencia a la cual pertenece a y recordamos que **$\overline{a} = \overline{b}$ si y sólo si $a \equiv b$ (mód m)**. Empezamos dándole estructura de anillo a $\mathbb{Z}_m$, pero antes veamos que $\mathbb{Z}_m$ es finito.

Proposición 7.7.1. *Para cada entero $m > 0$, $\mathbb{Z}_m$ es finito.*

Demostración. En el ejemplo 7.5.9 demostramos que $\{0, 1, \ldots, m-1\}$ es un conjunto completo de representantes. No es difícil ver entonces que

$$\overline{0}, \overline{1}, \ldots, \overline{m-1}$$

son todas las clases de equivalencia distintas módulo m. Esto es

$$\mathbb{Z}_m = \left\{\overline{0}, \overline{1}, \ldots, \overline{m-1}\right\}. \blacksquare$$

Nota 7.7.2. Hay que tener en cuenta que cada clase de equivalencia está dada a través de un representante de ella. Hemos escogido $0, 1, \ldots, m-1$ por comodidad, pero podríamos haber escogido cualquier otro elemento en cada clase de equivalencia, por ejemplo, $m \in \overline{0}$ y por lo tanto $\overline{m} = \overline{0}$ o $3m + 1 \in \overline{1}$ y entonces $\overline{3m+1} = \overline{1}$. Esto hay que tenerlo en cuenta en la definición de suma y producto en $\mathbb{Z}_m$.

Definición 7.7.3. *Sea $\overline{a}, \overline{b} \in \mathbb{Z}_m$. La suma y producto de $\overline{a}$ y $\overline{b}$ son respectivamente:*

$$\overline{a} + \overline{b} = \overline{a+b} \text{ y } \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

Es claro que estamos definiendo la suma y el producto en $\mathbb{Z}_m$ a través de cualquier representante en las clases de equivalencia, así que lo primero que debemos ver es que no depende de estas elecciones.

Proposición 7.7.4. *Si $\overline{a} = \overline{a}'$ y $\overline{b} = \overline{b}'$ en $\mathbb{Z}_m$, entonces $\overline{a+b} = \overline{a'+b'}$ y $\overline{a \cdot b} = \overline{a' \cdot b'}$.*

Demostración. Si $\overline{a} = \overline{a'}$ y $\overline{b} = \overline{b'}$ en $\mathbb{Z}_m$, entonces $a \equiv a' (\text{mód } m)$ y $b \equiv b' (\text{mód } m)$. luego por el teorema 7.5.4 incisos (1) y (2) se tiene respectivamente que $a + b \equiv a' + b' (\text{mód } m)$ y que $a \cdot b \equiv a' \cdot b' (\text{mód } m)$. Por lo tanto $\overline{a+b} = \overline{a'+b'}$ y $\overline{a \cdot b} = \overline{a' \cdot b'}$. $\blacksquare$

Teorema 7.7.5. *$(\mathbb{Z}_m, +, \cdot)$ es un anillo conmutativo.*

Demostración. Como la suma y producto se dio a través de de la suma y producto de $\mathbb{Z}$, las propiedades de $\mathbb{Z}_m$ se heredan de las correspondientes en $\mathbb{Z}$. Sean $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$.

(1) La suma es asociativa

$$\left(\overline{a}+\overline{b}\right)+\overline{c}=\left(\overline{a+b}\right)+\overline{c}=\overline{(a+b)+c}=\overline{a+(b+c)}=\overline{a}+\left(\overline{b+c}\right)=\overline{a}+\left(\overline{b}+\overline{c}\right).$$

(2) La suma es conmutativa
$\overline{a}+\overline{b}=\overline{a+b}=\overline{b+a}=\overline{b}+\overline{a}$.

(3) $\overline{a}+\overline{0}=\overline{a+0}=\overline{a}$; así que $\overline{0}$ es el neutro aditivo.

(4) $\overline{-a}$ es el inverso de $\overline{a}$: $\overline{a}+\overline{-a}=\overline{a+(-a)}=\overline{0}$.

(5) El producto es asociativo

$$\left(\overline{a}\cdot\overline{b}\right)\cdot\overline{c}=\left(\overline{a\cdot b}\right)\cdot\overline{c}=\overline{(a\cdot b)\cdot c}=\overline{a\cdot(b\cdot c)}=\overline{a}\cdot\left(\overline{b\cdot c}\right)=\overline{a}\cdot\left(\overline{b}\cdot\overline{c}\right).$$

(6) El producto es conmutativo $\overline{a}\cdot\overline{b}=\overline{a\cdot b}=\overline{b\cdot a}=\overline{b}\cdot\overline{a}$.

(7) $\overline{a}\cdot\overline{1}=\overline{a\cdot 1}=\overline{a}$, así que $\overline{1}$ es el neutro multiplicativo.

(8) El producto distribuye a la suma
$\overline{a}\cdot\left(\overline{b}+\overline{c}\right)=\overline{a}\cdot\left(\overline{b+c}\right)=\overline{a\cdot(b+c)}=\overline{a\cdot b+a\cdot c}=\overline{a\cdot b}+\overline{a\cdot c}=\overline{a}\cdot\overline{b}+\overline{a}\cdot\overline{c}$.

■

En vista de que $\mathbb{Z}_m$ es finito podemos construir sus tablas de sumar y multiplicar.

Ejemplo 7.7.6. Construyamos la tabla de la suma y el producto de $\mathbb{Z}_5$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

En algunos casos, como podemos apreciar en la tabla, hemos sustituido el resultado de la suma y el producto por un representante entre 0 y 4. Por ejemplo

$$\overline{2}+\overline{3}=\overline{5}=\overline{0},\quad \overline{4}+\overline{3}=\overline{7}=\overline{2},\quad \overline{3}\cdot\overline{3}=\overline{9}=\overline{4},\quad \overline{3}\cdot\overline{2}=\overline{6}=\overline{1}.$$

Observación 7.7.7. El hecho de que cada renglón (columna) en la tabla de la suma aparece $\overline{0}$ se debe a que cada elemento tiene inverso aditivo. En el caso del producto puede verse que cada elemento distinto de $\overline{0}$ tiene inverso multiplicativo, esto es, en cada renglón (columna) salvo la correspondiente a $\overline{0}$, aparece el $\overline{1}$. Esto significa que en $\mathbb{Z}_5$ cada elemento distinto de $\overline{0}$ tiene inverso multiplicativo.

Ejemplo 7.7.8. Las tablas de suma y producto en $\mathbb{Z}_6$ son

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

A diferencia de la tabla del producto para $\mathbb{Z}_5$ en la cual los renglones (columnas) correspondientes a elementos distintos de $\overline{0}$, no aparece $\overline{0}$, en la tabla del producto en $\mathbb{Z}_6$ sí aparece $\overline{0}$. Por ejemplo puede observarse que en el renglón (columna) correspondiente a $\overline{3}$, sólo aparecen $\overline{0}$ o $\overline{3}$, esto es porque $\overline{3}\cdot\overline{2}=\overline{6}=\overline{0}$ y $\overline{4}\cdot\overline{3}=\overline{12}=\overline{0}$, lo que significa que $\mathbb{Z}_6$ no es un dominio entero. Además el único elemento de $\mathbb{Z}_6$ que tiene inverso multiplicativo es $\overline{5}$. Conclusión: $\mathbb{Z}_5$ y $\mathbb{Z}_6$ como anillos son muy diferentes, el primero es un campo (ver definición 7.7.14 pág 283) y el segundo ni siquiera es dominio entero y no es difícil sospechar cual es la razón: 6 es un número compuesto.

Teorema 7.7.9. *$\mathbb{Z}_m$ es dominio entero si y sólo si m es primo.*

Demostración.

$\Longrightarrow$) Supongamos que $\mathbb{Z}_m$ es un dominio entero y supongamos también que m no es primo. Entonces $m=a\cdot b$ donde $1<a,b<m$ y por lo tanto $\overline{a}\cdot\overline{b}=\overline{m}=\overline{0}$. Pero como $\mathbb{Z}_m$ es un dominio, entonces $\overline{a}=\overline{0}$ o $\overline{b}=\overline{0}$, lo que significa que $m\mid a$ o $m\mid b$ lo cual es imposible. Luego m es primo.

$\Longleftarrow$) Supongamos que m es primo y supongamos que $\overline{a} \cdot \overline{b} = \overline{0}$ en $\mathbb{Z}_m$. Entonces $m \mid a \cdot b$ y por ser m primo, $m \mid a$ o $m \mid b$ y por lo tanto $\overline{a} = \overline{0}$ o $\overline{b} = \overline{0}$. Luego $\mathbb{Z}_m$ es dominio. ∎

En general, podemos investigar cuándo un elemento en $\mathbb{Z}_m$ (para cualquier m) tiene inverso multiplicativo. Esto es, queremos encontrar una condición necesaria y suficiente para que la ecuación $\overline{a}x = \overline{1}$ tenga solución en $\mathbb{Z}_m$ (donde $\overline{a}, \overline{1} \in \mathbb{Z}_m$), significando esto último la existencia de un elemento $\overline{b} \in \mathbb{Z}_m$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$. Teniendo en cuenta que la ecuación $\overline{a}x = \overline{1}$ en $\mathbb{Z}_m$ es equivalente a la congruencia $ax \equiv 1$ (mód m), que por el teorema 7.6.2 sabemos cuándo tiene solución, podemos entonces dar la versión de este teorema en $\mathbb{Z}_m$.

Teorema 7.7.10. *Sean $\overline{a}, \overline{b} \in \mathbb{Z}_m$, La ecuación $\overline{a}x = \overline{b}$ en $\mathbb{Z}_m$ tiene solución si y sólo si $(a, m) \mid b$ y en este caso tiene exactamente (a, m) soluciones distintas.*

Demostración. Basta ver que $\overline{a}x = \overline{b}$ en $\mathbb{Z}_m$ es equivalente a $ax \equiv b$ (mód m) y por lo tanto tiene solución si y sólo si $(a, m) \mid b$ (teorema 7.6.2.). ∎

Nota 7.7.11. Es importante mencionar que las soluciones y el número de éstas de una ecuación $\overline{a}x = \overline{b}$ en $\mathbb{Z}_m$ no depende de los representantes, es decir, si $\overline{a} = \overline{a}'$ y $\overline{b} = \overline{b}'$, entonces las ecuaciones $\overline{a}x = \overline{b}$ y $\overline{a}'x = \overline{b}'$ tienen exactamente las mismas soluciones (proposición 7.6.3)

Corolario 7.7.12. *Sea $\overline{a} \in \mathbb{Z}_m$. La ecuación $\overline{a}x = \overline{1}$ tiene solución si y sólo si $(a, m) = 1$.*

Otra diferencia que puede observarse entre los distintos $\mathbb{Z}_m$ es que cuando m es primo una ecuación $\overline{a}x = \overline{b}$ para $\overline{a} \neq \overline{0}$ tiene exactamente una solución, mientras que para los m que no son primos, si la ecuación $\overline{a}x = \overline{b}$ tiene solución puede ser que tenga más de una.

Ejemplo 7.7.13. La ecuación $\overline{3}x = \overline{2}$ no tiene solución en $\mathbb{Z}_6$ ya que $(3, 6) = 3 \nmid 2$ y la ecuación $\overline{3}x = \overline{3}$ en $\mathbb{Z}_6$ tiene 3 soluciones distintas que son $\overline{1}, \overline{3}$ y $\overline{5}$.

De toda la discusión anterior concluimos que cuando m es primo, cada elemento distinto de $\overline{0}$ en $\mathbb{Z}_m$ tiene inverso multiplicativo.

Definición 7.7.14. *Sea K un conjunto y $+, \cdot$ dos operaciones definidas en K. Diremos que $(K, +, \cdot)$ es un* **campo** *si es un anillo conmutativo y además cada elemento distinto de cero tiene inverso multiplicativo.*

Teorema 7.7.15. *$(\mathbb{Z}_m, +, \cdot)$ es un campo si y sólo si m es primo.*

Demostración.

$\Longleftarrow$) Ya hemos visto que para cualquier m $(\mathbb{Z}_m, +, \cdot)$ es anillo conmutativo y si $\overline{a} \neq \overline{0}$ en $\mathbb{Z}_m$, entonces $(a, m) = 1$ (por ser m primo) y por lo tanto $\overline{a}x = \overline{1}$ tiene solución por el corolario 7.7.12.

$\Longrightarrow$) Si $(\mathbb{Z}_m, +, \cdot)$ es campo, en particular es dominio entero ya que si $\overline{a} \cdot \overline{b} = \overline{0}$ y $\overline{a} \neq \overline{0}$, entonces $\overline{a}$ tiene inverso multiplicativo $\overline{a}^{-1}$. Luego

$$\overline{b} = (\overline{a}^{-1} \cdot \overline{a}) \cdot \overline{b} = \overline{a}^{-1} \cdot (\overline{a} \cdot \overline{b}) = \overline{a}^{-1} \cdot \overline{0} = \overline{0}.$$

Por último, por el teorema 7.7.9 m es primo. ∎

Para finalizar, tenemos una buena cantidad de ejemplos de campos, uno por cada primo p. Además todos ellos son finitos (que por cierto no son los únicos). Más adelante estudiaremos otros campos (infinitos) que son los campos de los números racionales, los números reales y los números complejos. Por otra parte también tenemos muchos ejemplos de anillos que no son dominios enteros, a saber los $\mathbb{Z}_m$ cuando m es compuesto.

§§ Ejercicios sección 7.1.

7.1.1. [1] Sean $a, b, c \in \mathbb{Z}$. Demuestre

(1) $1 \mid a$ y $-1 \mid a$.
(2) $a \mid a$. En particular $0 \mid 0$.
(3) Si $a \mid b$, entonces $-a \mid b$, $a \mid -b$ y $-a \mid -b$.
(4) $a \mid 0$.
(5) Si $0 \mid a$, entonces $a = 0$ (el único elemento que es divisible por cero es cero).
(6) Si $a \mid b$, entonces $a \cdot b \mid b \cdot c$.
(7) Si $a \mid b$ y $a \mid c$, entonces $a \mid b \cdot x + c \cdot y$ para cualesquiera $x, y \in \mathbb{Z}$.
(8) Si $a \mid b$ y $b \mid a$, entonces $a = b$ o $a = -b$ (esto es $|a| = |b|$).

7.1.2. Diga si los siguientes enunciados son verdaderos o falsos, justificando su respuesta.

(1) $6 \mid 42$
(2) $4 \mid 50$
(3) $16 \mid 0$
(4) $0 \mid 15$

[1] Parte del teorema 7.1.5 pág. 246.

(5) $14 \mid 997157$
(6) $17 \mid 998189$

7.1.3. Sean $a, b, c, d \in \mathbb{Z}$. Determine si los siguientes enunciados son verdaderos o falsos. Si son verdaderos, probar el resultado, y si son falsos, dar un contraejemplo.

(1) Si $a \mid b$ y $c \mid d$, entonces $a + c \mid b + d$.
(2) Si $a \mid b$ y $a \mid c$, entonces $a \mid b - c$.
(3) Si $a \nmid b$, entonces $b \nmid a$.
(4) Si $a \nmid b$ y $b \nmid c$, entonces $a \nmid c$.
(5) Si $a < b$ entonces $a \mid b$.
(6) $a \mid b$ ó $b \mid a$.
(7) Si $ac \mid bc$, entonces $a \mid b$.
(8) Si $a \mid b + c$, entonces $a \mid b$ y $a \mid c$.
(9) Si $a^2 \mid b^3$, entonces $a \mid b$.
(10) Si $a \nmid b$ y $a \nmid c$, entonces $a \nmid b + c$.
(11) Si $a \mid b$ y $b \mid a$, entonces $a = b$.

7.1.4. Sean $a, b \in \mathbb{Z}^+$. Si $b \mid a$ y $b \mid (a + 2)$, muestre que $b = 1$ o $b = 2$.

7.1.5. Sean $a, b_1, \ldots, b_n \in \mathbb{Z}$. Demuestre que si $a \mid b_i$ para $i = 1, \ldots, n$, entonces para cualesquiera $x_1, \ldots, x_n \in \mathbb{Z}$; $a \mid b_1 x_1 + \cdots + b_n x_n$.

7.1.6. Encuentre enteros a, b y c tales que $a \mid bc$ pero $a \nmid b$ y $a \nmid c$.

7.1.7. Demuestre que: $a \mid b \iff |a| \mid b \iff a \mid |b| \iff |a| \mid |b|$.

7.1.8. Sean $a, b, c, d \in \mathbb{Z}$. Demuestre que:

(1) Si $a \mid 1$, entonces $a = \pm 1$.
(2) $a \mid n$ para todo $n \in \mathbb{Z}$ si y sólo si $a = \pm 1$.
(3) $n \mid a$ para todo $n \in \mathbb{Z}$ si y sólo si $a = 0$.
(4) Si $a \nmid bc$ entonces $a \nmid b$ y $a \nmid c$.
(5) $a \mid a^n$ para todo $n \in \mathbb{N}$.
(6) Si $ac \mid bc$ y $c \neq 0$, entonces $a \mid b$.
(7) Si $a \mid b$ y $c \mid d$, entonces $ac \mid bd$.

7.1.9. Sean $a, b, c, d \in \mathbb{Z}$ con $a \neq 0$. Demuestre que

(1) Si $c \mid a$, entonces $c \neq 0$.

(2) Si $c \neq 0$, $a \mid b$ y $c \mid d$, entonces $\frac{bd}{ac} = \frac{b}{a} \cdot \frac{d}{c}$.[2]

(3) Si $a \mid b$ y $a \mid c$, entonces $\frac{b+c}{a} = \frac{b}{a} + \frac{c}{a}$.

(4) Si $d \neq 0$, $a \mid b$, $c \mid d$ y $ad \mid bc$, entonces $\frac{bc}{ad} = \frac{\frac{b}{a}}{\frac{d}{c}}$.

(5) Si $m \leq n$, entonces $a^m \mid a^n$ y $\frac{a^n}{a^m} = a^{n-m}$.

7.1.10. Completar la demostración de existencia en el algoritmo de la división. Se tienen cuatro casos:

(1) $a \geq 0$ y $b > 0$; (2) $a \geq 0$ y $b < 0$;
(3) $a < 0$ y $b > 0$; (4) $a < 0$ y $b < 0$.

El caso (1) se demuestra en el teorema 7.1.10. Pruebe los casos restantes. (Sugerencia:
Para (2) considerar que $-b > 0$ y aplicar el caso (1) a a y $-b$.
Para (3) aplicar el caso (1) a $-a > 0$ y $b > 0$; luego notar que

$$b(-q') + (-r') = b(-(q' + 1)) + (b - r').$$

Finalmente el caso (4) es análogo al caso (3); note además que si $0 \leq r' < -b$, entonces $0 \leq -b - r' < -b$.)

Se dice que un número entero n es ***par*** si $n = 2k$ para algún entero k y n es ***impar*** si $n = 2k + 1$ para algún entero k.

7.1.11. Demuestre que:

(1) Todo entero es par o impar, pero no ambos.
(2) La suma de dos números pares es también un número par.
(3) La suma de un número par con un impar es impar.
(4) Si el cuadrado de un entero es par, entonces éste es par.
(5) Si el cuadrado de un entero es impar, entonces éste es impar.
(6) El producto de dos números impares es un número impar.
(7) Si el producto de dos números es impar, entonces ambos son impares.
(8) El producto de dos números es un número par si y sólo si al menos uno de éstos es un número par.

7.1.12. Usando el algoritmo de la división pruebe que

[2] Véase nota 7.1.8 para la notación $\frac{b}{a}$.

(1) Todo entero es de la forma, $4k$, $4k+1$, $4k+2$ o $4k+3$, para algún entero k.
(2) Todo entero impar es de la forma $4k+1$ o $4k+3$ donde $k \in \mathbb{Z}$.
(3) Todo entero impar es de la forma $6k+1$, $6k+3$ o $6k+5$ donde $k \in \mathbb{Z}$.

7.1.13. Use inducción (sobre n) para probar que si $a \mid b_1, \ldots, a \mid b_n$ y $r_1, \ldots, r_n$ son enteros arbitrarios, entonces $a \mid r_1 b_1 + \cdots + r_n b_n$.

7.1.14. Sea $n \in \mathbb{N}$, donde $n \geq 2$. Demuestre que si $a_1 \mid b_1$, $\ldots$, $a_n \mid b_n$, entonces $(a_1 a_2 \cdots a_n) \mid (b_1 b_2 \cdots b_n)$.

7.1.15. Sean $a, b \in \mathbb{Z}$ tales que $17 \mid 2a + 3b$. Pruebe que $17 \mid 9a + 5b$.

7.1.16. Si $a, b, c \in \mathbb{Z}$ y $31 \mid (5a + 7b + 11c)$, demuestre que

(1) $31 \mid (21a + 17b + 9c)$ y
(2) $31 \mid (6a + 27b + 7c)$.

7.1.17. Demuestre que para todo $n \in \mathbb{Z}$ se cumple:

(1) $2 \mid n^2 - n$
(2) $6 \mid n^3 - n$
(3) $30 \mid n^5 - n$

7.1.18. Demuestre que para todo $n \in \mathbb{Z}$ se cumple:

(1) $4 \nmid n^2 + 2$;
(2) $4 \nmid n^2 - 3$.

7.1.19. Si $a, b \in \mathbb{Z}$ y ambos son impares, demuestre que $2 \mid (a^2 + b^2)$ pero que $4 \nmid (a^2 + b^2)$.

7.1.20. Pruebe que para todo $n \in \mathbb{N}$ se cumple:

(1) $15 \mid 2^{4n} - 1$
(2) $9 \mid 2^{4n} + 3n - 1$
(3) $25 \mid 2^{4n} + 10n - 1$
(4) $2 \mid 3^{2^n} + 1$ pero $4 \nmid 3^{2^n} + 1$
(5) $64 \mid 3^{2n+2} - 8n - 9$

7.1.21. Probar que

(1) El producto de tres enteros consecutivos es divisible entre 6; de cuatro enteros consecutivos entre 24.
(2) Si $a \in \mathbb{Z}$, entonces para todo $k \in \mathbb{N}$ se cumple que $k! \mid (a+1)(a+2)\cdots(a+k)$.

7.1.22. Demuestre que $8^n \mid (4n)!$ y $16^n \mid (6n)!$, para todo $n \in \mathbb{N}$.

7.1.23. Demuestre que $2^n \mid (n+1)(n+2)\cdots(2n)$, para todo $n \in \mathbb{N}$.

7.1.24.

(1) Sean $a, b \in \mathbb{Z}$. Pruebe que $a^2 - b^2 \neq 1$.
(2) Probar que el producto de cualesquiera cuatro enteros consecutivos positivos no puede ser un cuadrado perfecto.

7.1.25. Sea n es un entero impar. Demuestre que

(1) $8 \mid n^2 - 1$;
(2) Si $3 \nmid n$, entonces $6 \mid n^2 - 1$

7.1.26. Sean n un natural y a y b enteros cualesquiera. Demuestre que

(1) $a - b \mid a^n - b^n$.
(2) Si n es impar, entonces $a + b \mid a^n + b^n$.
(3) Si $d \mid n$, entonces $a^d - b^d \mid a^n - b^n$.

7.1.27. Sea $n, k \in \mathbb{Z}^+$ con k impar. Pruebe que

$$(1 + 2 + \cdots + n) \mid \left(1^k + 2^k + \cdots + n^k\right).$$

7.1.28. Sean $k, n \in \mathbb{N}$.

(1) Demuestre que $(n-1)^2 \mid (n^k - 1)$ si y sólo si $(n-1) \mid k$. (Sugerencia: $n^k = [(n-1)+1]^k$).
(2) Sea $a \in \mathbb{Z}$ con $n \neq a$. Demuestre que $(n-a)^2 \mid (n^k - a^k)$ si y sólo si $(n-a) \mid ka^{k-1}$

7.1.29. Demuestre que

(1) Cualquier entero de la forma $6k + 5$ es también de la forma $3m + 2$, pero no al revés.
(2) El cuadrado de cualquier entero es de la forma $3k$ o $3k + 1$.
(3) El cuadrado de cualquier número impar se puede expresar como un número de la forma $8n + 1$.
(4) El cubo de cualquier entero es de la forma $9k$, $9k + 1$ o $9k - 1$.
(5) La cuarta potencia de cualquier entero es de la forma $5k$ o $5k + 1$.
(6) La cuarta potencia de cualquier número impar se puede expresar como un número de la forma $16n + 1$.

7.1.30. Demostrar el algoritmo de la división para los casos restantes: $a < 0$ y $b > 0$; $a > 0$ y $b < 0$; $a < 0$ y $b < 0$. (Sugerencia: En cada caso multiplique adecuadamente por -1 para poder aplicar el algoritmo de Euclides a la

pareja de enteros positivos resultantes. Por ejemplo, en ele primer caso considere $a > 0$ y $-b > 0$.)

7.1.31. Usando el algoritmo de la división, encontrar el cociente y el residuo en la división de b por a, donde a y b son los siguientes:

(1) $a = 0$, $b = -3$
(2) $a = 47$, $b = -6$.
(3) $a = 12$, $b = 59$
(4) $a = 59$, $b = 12$
(5) $a = -59$, $b = 12$
(6) $a = 59$, $b = -12$
(7) $a = 23$, $b = 7$
(8) $a = 434$, $b = 31$
(9) $a = -115$, $b = 12$
(10) $a = 37$, $b = 1$
(11) $a = 8611$, $b = -37$
(12) $a = -8611$, $b = -37$
(13) $a = -37$, $b = 8611$
(14) $a = c^3 + 2c^2 + 2c + 2$, $b = c + 1$ $(c > 0)$

7.1.32. Utilice el corolario 7.1.10 para determinar cuáles de los siguientes enunciados son verdaderos o falsos.

(1) $6 \mid 42$
(2) $4 \mid 50$
(3) $16 \mid 0$
(4) $14 \mid 997157$
(5) $17 \mid 998189$

7.1.33. Encuentra todos los enteros positivos n tales que $(n + 1) \mid (n^2 + 1)$

7.1.34. Encuentra todos los enteros positivos n tales que $(n^2 + 1) \mid (n^6 + 216)$

7.1.35. Supóngase $a, b, n \in \mathbb{Z}$, $a \neq b$, y $|a - b| < |n|$. Pruebe que $n \nmid a$ y $n \nmid b$.

7.1.36. Definimos en $\mathbb{Z}$ la siguiente relación: Dados $a, b \in \mathbb{Z}$;

$$a \sim b \text{ si y sólo si } a \mid b.$$

¿La relación "$\sim$" es de equivalencia en $\mathbb{Z}$?

7.1.37.

(1) Sean $a, b, c \in \mathbb{Z}$ tales que $a \neq 0$ o $b \neq 0$. Demuestre que, si $c \mid a$ y $c \mid b$, entonces $c \neq 0$.
(2) Sean $a, b, c, d \in \mathbb{Z}$ tale que $a \neq 0$, $c \neq 0$, $a \mid b$ y $c \mid d$; demostrar que, si $d \neq 0$ y $ad \mid bc$, entonces $\frac{bc}{ad} = \frac{\frac{b}{a}}{\frac{d}{c}}$.

7.1.38. Sea $a = 2^n \cdot t$, donde t es impar. Demuestre que $2^{n+1} \nmid a$.

7. 1.39. Decimos que $c \in \mathbb{Z}^+ \cup \{0\}$ es un ***cuadrado***, si existe $m \in \mathbb{Z}$ tal que $c = m^2$. Demuestre que si c es un cuadrado, entonces existe $k \in \mathbb{Z}^+ \cup \{0\}$ tal que $c \in \{4k, 4k + 1\}$.

7.1.40. Demuestre los siguientes criterios de divisibilidad:

(1) Un número es divisible por 2 si y sólo si su último dígito es par.
(2) Un número es divisible por 3 si y sólo si la suma de sus dígitos el múltiplo de 3.
(3) Un número es divisible por 4 si y sólo si sus últimos dos dígitos son 00 o forman un número divisible por 4.
(4) Un número es divisible por 5 si y sólo si su último dígito es 0 ó 5.
(5) Un número es divisible por 8 si y sólo si sus últimos tres dígitos son 000 o forman un número divisible por 8.
(6) Un número es divisible por 9 si y sólo si la suma de sus dígitos el múltiplo de 9.
(7) Un número es divisible por 10 si y sólo si su último dígito es 0.

7.1.41. En cada uno de los siguientes casos exprese n en base a.

(1) $n = 328$, $a = 8$;
(2) $n = 723$, $a = 7$;
(3) $n = 1207$, $a = 11$;
(4) $n = 2770$, $a = 2$;
(5) $n = 541$, $a = 3$;
(6) $n = 224$, $a = 7$.

7.1.42. Sea $n = (r_k \cdots r_1 r_0)_a$. Demuestre que $n \leq a^{k+1} - 1$.

7.1.43.

(1) Ordénese los números binarios $(1011)_2$, $(110)_2$, $(11011)_2$, $(10110)_2$ y $(101010)_2$ de mayor a menor.

(2) Ordénese los números hexadecimales $(1076)_{16}$, $(3056)_{16}$, $(3CAB)_{16}$, $(5ABC)_{16}$ y $(CACB)_{16}$ de mayor a menor.

7.1.44. Realice las siguientes operaciones:

(1) $(1076)_8 + (2076)_8$;
(2) $(89\beta)_{12} + (5\alpha 6)_{12}$;
(3) $(2000)_7 - (1336)_7$;
(4) $(10121)_3 \times (1201)_3$;
(5) $(\gamma\beta\alpha)_{16} \times (\alpha\beta\gamma)_{16}$.

7.1.45. Completa las operaciones.

$$\begin{array}{cccccc} & \square & 3 & \square & \square & 4 \\ & & & \square & 3 & 7 \\ + & & \square & 4 & 1 & 3 \\ \hline & 2 & 0 & 8 & 7 & \square \end{array} \qquad \begin{array}{cccc} & A & 7 & 4_{12} \\ - & \square & 9 & \square_{12} \\ \hline & 6 & \square & 5_{12} \end{array}$$

$$\begin{array}{ccccc} & & \square & 2 & \square \\ \times & & & \square & 7 \\ \hline & 4 & 3 & 9 & 6 \\ \square & \square & 8 & 4 & \\ \hline \square & \square & \square & \square & \square \end{array} \qquad \begin{array}{cccccc} & & 2 & \square & 3 & 4_6 \\ & \times & & 3 & 2 & \square_6 \\ \hline & & 1 & 4 & 3 & 0 & 2 \\ & & \square & 1 & 1 & 2 & \\ 1 & \square & 1 & \square & 0 & & \\ \hline \square & \square & \square & \square & \square & \square & 2_6 \end{array}$$

7.1.46. Encuentre el valor de la base a en cada uno de los siguientes casos.

(1) $(54)_a = (64)_{10}$
(2) $(1001)_a = (9)_{10}$
(3) $(1001)_a = (126)_{10}$
(4) $(144)_a = (110001)_2$
(5) $(1234)_a = (1\delta\delta\alpha)_{16}$

7.1.47.

(1) Sea b una base tal que $(120)_a + (211)_a = (331)_a$. Encuentre los posibles valores de a.
(2) Resolver la ecuación $(229)_a - (99)_a = (140)_a$.

7.1.48. ¿Qué puede decir acerca del número de unos que aparecen en la representación binaria de un entero par? ¿Y si es impar? (justifique su respuesta)

7.1.49. Si un número en base 2 se escribe con 8 cifras, ¿Cuántas podría tener en base 12?

7.1.50. El siguiente ejercicio presenta un versión alternativa del algoritmo de la división.

(1) Sean a y b enteros no nulos. Demuestre que existen dos enteros q y r, únicos, tales que

$$a = bq + r, \quad -\frac{|b|}{2} < r \leq \frac{|b|}{2}$$

(2) Encuéntrense los números q y r garantizados por el algoritmo de la división del inciso (1) donde $a = 47$ y $b = -6$.

7.1.51. Demuestre que existen dos enteros q y r, únicos, tales que

$$a = bq + r, \quad 2b \leq r < 3b.$$

§§ Ejercicios sección 7.2.

7.2.1. Demuestre la proposición 7.2.5

7.2.2. Sean $a, b, c, d \in \mathbb{Z}$. Determine si los siguientes enunciados son verdaderos o falsos. Si son verdaderos, probar el resultado, y si son falsos, dar un contraejemplo.

(1) Si a es par y b es impar, entonces $(a, b) = \left(\frac{a}{2}, b\right)$.
(2) Si $a \nmid b$, entonces $(a, b) = 1$.
(3) Si $(a, b) = 1$ y $(b, c) = 1$, entonces $(a, c) = 1$.
(4) Si $d = ax + by$, para ciertos enteros x, y, entonces $d = (a, b)$.
(5) $c \mid a$ y $c \mid b$ si y sólo si $c \mid (a, b)$.
(6) $(a, a + k) \mid k$ para todo entero k no cero.
(7) Si $(a, b) = (a, c)$, entonces $[a, b] = [a, c]$.
(8) $(a, b) \mid [a, b]$.
(9) Si $d = (a, b)$, entonces $\left(\frac{a}{d}, b\right) = 1$.
(10) $(a, b, c)[a, b, c] = |abc|$.
(11) Si $(a, b, c) = 1$ entonces $(a, b) = 1$ o $(b, c) = 1$ o $(a, c) = 1$.

7.2.3. Sean $a, b \in \mathbb{Z}$. Demuestre que:

(1) $M(0) = \{0\}$.
(2) $0, \pm a \in M(a)$.
(3) $M(a) = M(-a)$.

(4) Si $y \in M(a)$, entonces $y \cdot z \in M(a)$ para todo $z \in \mathbb{Z}$.
(5) Si $a \neq 0$, entonces $M(a)$ es infinito.
(6) Para cualesquiera $a, b \in \mathbb{Z}$, $0, a \cdot b \in M(a) \cap M(b)$.
(7) Si $a \neq 0$ y $b \neq 0$, entonces $M(a) \cap M(b)$ es infinito.
(8) Si $a \neq 0$ y $b \neq 0$, entonces $M(a) \cap M(b)$ tiene un mínimo positivo.

7.2.4.
(1) Encuentre $[a, b]$ para los siguiente calores de a y b
(1) $a = 108$, $b = 28$; (2) $a = 56$, $b = 31$;
(3) $a = -14$, $b = -28$; (4) $a = 17$, $b = 23$.
(2) Para cada uno de los incisos anteriores encuentre $[a, b]$.

7.2.5. Sean $a, b, c, d \in \mathbb{Z}$. Demuestre que si $a \mid b$ y $c \mid d$, entonces $(a, c) \mid (b, d)$ y $[a, c] \mid [b, d]$.

7.2.6. Sean a, b, c enteros positivos. Demuestre que

(1) Si $(a, b) = [a, b]$, entonces $a = b$.
(2) Si $(a, b) = (a, c)$ y $[a, b] = [a, c]$, entonces $b = c$.
(3) Si $[a, b] + (a, b) = a + b$, entonces $a \mid b$ o $b \mid a$.

7.2.7. Considere las siguientes parejas de números enteros.

(1) 15 y 21
(2) 527 y 765
(3) 361 y 1178
(4) 132 y -473
(5) 1024 y 1000
(6) -2024 y 1024
(7) -2076 y -1076
(8) 2076 y 1776
(9) 1976 y 1776
(10) 3076 y 1776
(11) 1816 y -1789
(12) -666 y -12309
(13) $2n + 1$ y $4n$
(14) $4n^2 + 2n - 40$ y $2n + 7$

(*a*) Usando el algoritmo de Euclides, determine para cada pareja de enteros su máximo común divisor y expréselo como una combinación lineal de éstos.
(*b*) Encuentre para cada pareja su mínimo común múltiplo.

7.2.8. Demuestre que si $d > 0$, $d \mid a$, $d \mid b$ y $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, entonces $d = (a, b)$.

7.2.9. Sean $a, b \in \mathbb{Z}$. Demostrar que $(a, b) = 1$ si y sólo si existen $x, y \in \mathbb{Z}$ tales que $1 = ax + by$.

7.2.10. Sean $a, b \in \mathbb{Z}$.

(1) Demuestre que, si $d = (a, b)$ entonces $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

(2) Si $d = (a, b)$, ¿es cierto que $\left(\frac{a}{d}, b\right) = 1$?

7.2.11. Demuestre que para cualquier entero a, $(a, a + 1) = 1$.

7.2.12.

(1) Sean $a, b_1, b_2, \ldots, b_n \in \mathbb{Z}$ con $(a, b_1) = (a, b_2) = \ldots = (a, b_n) = 1$. Demuestre que

$$(a, b_1 b_2 \cdots b_n) = 1.$$

(2) Sean $a_1, a_2, \ldots, a_n, c \in \mathbb{Z}$ con $(a_i, a_j) = 1$ para todo $i \neq j$. Muestre que si $a_i \mid c$ para toda i, entonces $a_1 a_2 \cdots a_n \mid c$.

7.2.13. Demostrar que $(a, b, c) = ((a, b), c)$.

7.2.14. Sean $a, b, c, d \in \mathbb{Z}$. Demuestre que

(1) $(a, b) = 1$ si y sólo si $(a + b, ab) = 1$.
(2) Si $(b, c) = 1$ y $d \mid b$ entonces $(d, c) = 1$.
(3) Si $(a, b) = 1$ y $c \mid a + b$, entonces $(a, c) = 1$ y $(b, c) = 1$.
(4) Si $(b, c) = 1$, $d \mid b$ y $d \mid a \cdot c$, entonces $d \mid a$.

7.2.15. Sean $a, b, d \in \mathbb{Z} - \{0\}$ con d impar. Demuestre que si $d \mid (a+b)$ y $d \mid (a-b)$, entonces $d \mid (a, b)$.

7.2.16. Sean $m, n \in \mathbb{Z}$. Si $d \mid mn$ y $(m, n) = 1$, demuestre que d se puede escribir como $d = rs$ donde $r \mid m$, $s \mid n$ y $(r, s) = 1$.

7.2.17. Sean $a, m, n \in \mathbb{Z}^+$. Si $(m, n) = 1$, demuestre que $(a, mn) = (a, m)(a, n)$.

7.2.18. Sean $a, b, c \in \mathbb{Z}$. Si $(a, c) = 1$, demuestre que $(ab, c) = (b, c)$.

7.2.19. Sean $a, b, m, n \in \mathbb{Z}$. Si $(m, n) = 1$, demuestre que

$$(ma + nb, mn) = (a, n)(b, m).$$

7.2.20. Sean $a, b \in \mathbb{Z}$, con $d = (a, b)$, y sean enteros x, y tales que $ax + by = d$. Demuestre que $(x, y) = 1$.

7.2.21. Pruébese que:

(1) Si m es combinación lineal de a y b, entonces para todo $r \in \mathbb{Z}$ se tienen que rm también es combinación lineal de a y b.
(2) Si d es combinación lineal de a y b y b es combinación lineal de a y c, entonces d es combinación lineal de a y c.

7.2.22. Calcule:

(1) $(a, a+1)$;
(2) $[a, a+1]$;
(3) $(a, a+2)$;
(4) $(a+b, a^2-b^2)$;
(5) (a^2-b^2, a^3-b^3);
(6) (a^2-b^2, a^4-b^4).

7.2.23. Sean $a, b, m, \in \mathbb{Z}$ con $m, n \geq 0$. Muestre que

(1) $(a, b) = 1$ si y sólo si $(a^m, b) = 1$.
(2) $(a, b) = 1$ si y sólo si $(a^m, b^n) = 1$.

7.2.24.

(1) Demuestre que $(n! + 1, (n+1)! + 1) = 1$. (*Sugerencia: Utilice el algoritmo de Euclides*.)
(2) Encuentre $(n, n+1)$ y $[n, n+1]$ si $n \in \mathbb{Z}$.
(3) Sean $a, b \in \mathbb{Z}$ tales que $(a, 4) = 2$ y $(b, 4) = 2$. Demuestre que $(a+b, 4) = 4$.

7.2.25. Sean $a, b \in \mathbb{Z}^+$ con $a > b$. Pruebe

(1) $(a+b, a-b) \geq (a, b)$.
(2) Si $(a, b) = 1$, entonces $(a+b, a-b) = 1$ o 2.

7. 2.26. Sean a, b, c, d enteros positivos fijos. Si $(ad - bc) \mid a$ y $(ad - bc) \mid c$, demuestre que $(an + b, cn + d) = 1$ para cualquier $n \in \mathbb{N}$.

7.2.27. Sean $a, b \in \mathbb{Z} - \{0\}$ con $(a, b) = 1$. Demuestre que

(1) $(a + 2b, 2a + b) = 1$ o 3;
(2) $(a^2 + b^2, a + b) = 1$ o 2;
(3) $(a^2 - 3ab + b^2, a + b) = 1$ o 5

7.2.28. Si $(a, 4) = 2$ y $(b, 4) = 2$, pruebe que $(a + b, 4) = 4$.

7.2.29. Sea n un entero positivo. Demuestre que $(n! + 1, (n+1)! + 1) = 1$.

7.2.30. Sea n un entero positivo. Pruebe que si a, b son enteros positivos, entonces
(1) $(n^a - 1, n^b - 1) = n^{(a,b)} - 1$;
(2) $(n^a + 1, n^b + 1) \mid n^{(a,b)} + 1$.

7.2.31. Sean a, b enteros, y sea n un entero positivo.
(1) Si $a \neq b$, demuestre que

$$\left(\frac{a^n - b^n}{a - b}, a + b\right) = (n(a, b)^{n-1}, a - b)$$

(2) Si $a + b \neq 0$, demuestre que

$$\left(\frac{a^n + b^n}{a + b}, a + b\right) = (n(a, b)^{n-1}, a + b)$$

7.2.32. Probar que si $n < m$, entonces $a^{2^n} + 1$ es un divisor de $a^{2^m} - 1$. Demuestre que si a, m, n son enteros positivos con $m \neq n$, entonces

$$\left(a^{2^n} + 1, a^{2^m} + 1\right) = \begin{cases} 1 & \text{si } a \text{ es par} \\ 2 & \text{si } a \text{ es impar} \end{cases}$$

7.2.33 Eficiencia del algoritmo de Euclides. De acuerdo al algoritmo de Euclides, suponiendo que $a \geq b > 0$, se tiene que

$$\begin{array}{rcll} a & = & bq_0 + r_0 & 0 < r_0 < b \\ b & = & r_0 q_1 + r_1 & 0 < r_1 < r_0 \\ r_0 & = & r_1 q_2 + r_2 & 0 < r_2 < r_1 \\ & \vdots & & \\ r_{i-2} & = & r_{i-1} q_i + r_i & 0 < r_i < r_{i-1} \\ r_{i-1} & = & r_i q_{i+1} + r_{i+1} & r_{i+1} = 0 \end{array}$$

donde $r_i = (a, b)$. Demuestre que
(1) $a > 2r_0$, $b > 2r_1$ y para $k \geq 1$, $r_k > 2r_{k+2}$.
(2) $b > 2^{\frac{i}{2}}$.
(3) El algoritmo de Euclides para calcular (a, b) termina a lo más en $2\log_2(b)$ pasos, donde cada paso es una división con residuo.

7.2.34. Sean $a_1, \ldots, a_n \in \mathbb{Z} - \{0\}$ y $d = (a_1, \ldots, a_n)$. Probar que
(1) d es la mínima combinación lineal positiva de $a_1, \ldots, a_n$.
(2) $(ca_1, \ldots, ca_n) = |c| \cdot (a_1, \ldots, a_n)$.
(3) $[ca_1, \ldots, ca_n] = |c| \cdot [a_1, \ldots, a_n]$.

7.2.35. Sean $a_1, \ldots, a_n \in \mathbb{Z}$. Demostrar

(1) $d = (a_1, \ldots, a_n)$ si y sólo si d satisface
  (*i*) $d > 0$
  (*ii*) $d \mid a_i$ para toda $i = 1, \ldots, n$
  (*iii*) Si $d' \mid a_i$ para toda $i = 1, \ldots, n$, entonces $d' \leq d$.
(2) $m = [a_1, \ldots, a_n]$ si y sólo si m satisface
  (*i*) $m > 0$
  (*ii*) $a_i \mid m$ para toda $i = 1, \ldots, n$
  (*iii*) Si $a_i \mid m'$ para toda $i = 1, \ldots, n$, entonces $m \leq |m'|$.

7.2.36.

(1) Pruebe que $(a_1, a_2, \ldots, a_n) = ((a_1, a_2, \ldots, a_{n-1}), a_n)$.
(2) Sean $a = 165$, $b = 42$, $c = 147$. Encuentre (a, b, c) y escríbalo como combinación lineal de a, b y c.

7.2.37. Pruebe que $[a_1, a_2, \ldots, a_n] = [[a_1, a_2, \ldots, a_{n-1}], a_n]$.

7.2.38. Sea n un entero positivo. Encuentre $(n, n+1, n+2)$ y $[n, n+1, n+2]$.

7.2.39. El siguiente ejercicio presenta un nuevo algoritmo para calcular el máximo común divisor de dos números enteros positivos análogo al algoritmo Euclidiano. Este nuevo algoritmo está basado en el ejercicio 41 de la sección 7.1. Sean a y b enteros con $a \geq b > 0$. Entonces existen enteros q_1 y r_1 tales que

$$a = bq_1 + r_1, \quad -\frac{|b|}{2} < r_1 \leq \frac{|b|}{2}$$

Si $r_1 \neq 0$, existen (por the absolute least remainder algorithm) enteros q_2 y r_2 tales que

$$a = r_1 q_2 + r_2, \quad -\frac{|r_1|}{2} < r_2 \leq \frac{|r_1|}{2}$$

Si $r_2 \neq 0$, existen (por the absolute least remainder algorithm) enteros q_3 y r tales que

$$a = r_2 q_3 + r_3, \quad -\frac{|r_2|}{2} < r_3 \leq \frac{|r_2|}{2}$$

Continuando este proceso.

(1) Muestre que $r_n = 0$ para algún n. Si $n > 1$, muestre que $(a, b) = |r_{n-1}|$.
(2) Use el nuevo algoritmo para encontrar $(204, 228)$ y $(233, 377)$.

7.2.40. Sean $a_1, \ldots, a_n \in \mathbb{Z}$. Demostrar

(1) $d = (a_1, \ldots, a_n)$ si y sólo si d satisface
  (i) $d > 0$
 (ii) $d \mid a_i$ para toda $i = 1, \ldots, n$
(iii) Si $d' \mid a_i$ para toda $i = 1, \ldots, n$, entonces $d' \leq d$.
(2) $M = [a_1, \ldots, a_n]$ si y sólo si m satisface
  (i) $m > 0$
 (ii) $a_i \mid m$ para toda $i = 1, \ldots, n$
(iii) Si $a_i \mid d'$ para toda $i = 1, \ldots, n$, entonces $m \leq |m'|$.

§§ Ejercicios sección 7.3.

7.3.1. Encuentre todas las soluciones enteras (si las hay) de las ecuaciones diofantinas siguientes:

(1) $243x + 198y = 9$
(2) $43x + 64y = 1$
(3) $6x + 10y = 1$
(4) $35x + 17y = 14$
(5) $14x + 21y = 10$
(6) $-121x + 88y = -572$
(7) $2520x + 1188y = 108$
(8) $2520x + 1188y = -108$
(9) $93x + 81y = 3$

7.3.2. Probar que todas las soluciones de $3x + 5y = 1$ pueden escribirse en la forma $x = 2 + 5t$, $y = -1 - 3t$; también en la forma$x = 2 - 5t$, $y = -1 + 3t$; también en la forma $x = -3 + 5t$, $y = 2 - 3t$. Probar que $x = a + bt$, $y = c + dt$ es una forma de la solución general si y sólo si a, c es una solución y ya sea $b = 5$, $d = -3$ o bien $b = -5$, $d = 3$.

7.3.3. Si $ax + by = c$ tiene solución en $\mathbb{Z}$, probar que tiene una solución x_0, y_0 con $0 \leq x_0 < |b|$.

7.3.4. Dar otra demostración de que $ax + by = c$ tiene solución en $\mathbb{Z}$ si $(a, b) \mid c$ aplicando inducción sobre máx$\{a, b\}$. (Sugerencia: Si $0 < a < b$ entonces $ax+by = c$ es soluble si y sólo si $a(x - y) + (b - a)y = c$ es soluble)

7.3.5. Sean m y n enteros. Encuentre todas las soluciones enteras de las siguientes ecuaciones diofantinas.

(1) $(6n + 1)x + 3ny = 12$

(2) $(4n + 1)x + 2ny = n$
(3) $nx + (n + 1)y = m$.
(4) $nx + (n + 2)y = m$, donde n es impar.
(5) $nx + (n + 3)y = m$, donde $3 \nmid n$.
(6) $nx + (n + k)y = m$, donde k es un entero tal que $(k, n) = 1$.

7. 3.6. Determine los valores de c con $10 < c < 20$, para los que la ecuación diofantina $8x + 990y = c$ no tiene solución. Determine las soluciones para los valores restantes.

7.3.7. Sean $a, b, c, d \in \mathbb{Z}$.

(1) Muestre que si $ax + by = b + c$ tiene solución en $\mathbb{Z}$ si y sólo si $ax + by = c$ también tiene solución en $\mathbb{Z}$.
(2) Muestre que si $ax + by = c$ tiene solución en $\mathbb{Z}$ si y sólo si $(a, b) = (a, b, c)$.

7. 3.8. Sean $a, b \in \mathbb{Z}$; y suponga que toda solución en $\mathbb{Z}$ de la ecuación $ax + by = 1$ es de la forma

$$\begin{cases} x = 5 - 4t \\ y = 1 - 3t \end{cases}$$

donde $t \in \mathbb{Z}$. Determine los valores de a y b.

Definición. Decimos que la solución x_0, y_0 de la ecuación diofantina

$$ax + by = c$$

es positiva si x_0 y y_0 son enteros positivos.

7. 3.9. Encuentre todas las soluciones enteras POSITIVAS de las siguiente ecuaciones diofantina.

(1) $5x + 3y = 52$
(2) $40x + 63y = 521$
(3) $123x + 57y = 531$
(4) $12x + 501y = 1$
(5) $12x + 501y = 274$
(6) $97x + 98y = 1000$

7.3.10. Sea N el número de soluciones enteras positivas de la ecuación diofantina $ax + by = c$.

(1) Demuestre que

$$-\left\lfloor \frac{-(a,b)c}{ab} \right\rfloor - 1 \leq N \leq -\left\lfloor \frac{-(a,b)c}{ab} \right\rfloor .$$

(2) Si $(a,b) = 1$ y $ab \nmid c$, pruebe que

$$N = \left\lfloor \frac{c}{ab} \right\rfloor \qquad \text{o} \qquad N = \left\lfloor \frac{c}{ab} \right\rfloor + 1.$$

Demuestre que si $a \mid c$, entonces $N = \left\lfloor \frac{c}{ab} \right\rfloor$. (Recuérdese que $\lfloor x \rfloor$ denota la parte entera de x)

7.3.11. Determine los valores de c con $10 < c < 20$, para los que la ecuación diofantina $8x + 990y = c$ no tiene solución. Determine las soluciones para los valores restantes.

7.3.12. Expresar el número 100 como la suma de dos enteros, uno de los cuales es divisible por 7 y el otro por 11.

7.3.13. Sean $a, b, c, d \in \mathbb{Z}$. Demuestre que

(1) $ax + by = b + c$ tiene solución en $\mathbb{Z}$ si y sólo si $ax + by = c$ también tiene solución en $\mathbb{Z}$.
(2) $ax + by = c$ tiene solución en $\mathbb{Z}$ si y sólo si $(a,b) = (a,b,c)$.

7.3.14.

(1) Escriba a 24 como combinación lineal de 3 y 6 de cuatro formas distintas.
(2) Demuestre que 52 no es combinación lineal de 20 y 15.

7.3.15. Pruébese que:

(1) Si n es un número par, entonces n no es combinación lineal de 21 y 10.
(2) Si n es un número impar, entonces n no es combinación lineal de 98 y 102.
(3) Si $n = 3m + 1$, $m \in \mathbb{Z}$, entonces n no es combinación lineal de 45 y 1251.
(4) Si $n = 30m + 6$, $m \in \mathbb{Z}$, entonces n no es combinación lineal de 1020 y 210.

7. 3.16. Sean $a, b \in \mathbb{Z}$; y suponga que toda solución en $\mathbb{Z}$ de la ecuación $ax + by = 1$ es de la forma

$$\begin{cases} x = 5 - 4t \\ y = 1 - 3t \end{cases}$$

donde $t \in \mathbb{Z}$. Determine los valores de a y b.

7.3.17. Demuestre que si (x_0, y_0) es una solución de la ecuación diofantina $ax - by = 1$, entonces el área del triángulo cuyos vértices son $(0, 0)$, (b, a) y (x_0, y_0) es $\frac{1}{2}$.

7.3.18. Sean $(a, b) = 1$ y n un entero positivo. Demuestre que

(1) Si $n = ab - a - b$, entonces la ecuación $ax + by = n$ no tiene soluciones positivas.
(2) Si $n > ab - a - b$, entonces la ecuación $ax + by = n$ tiene soluciones positivas.

7.3.19. Una hombre paga 143 pesos por algunas sandías y algunos melones. Si cada sandía cuesta 17 pesos y cada melón 15 pesos, ¿cuántas sandías y melones compró en total?

7.3.20. Un teatro cobra 180 pesos por una entrada de adulto y 75 pesos por una de niño. El lunes pasado la recaudación fue de 9000 pesos. Suponiendo que los niños fueron minoría, ¿cuánta gente acudió al teatro?

7.3.21. Un hombre cobra un cheque por p pesos y c centavos en un banco. El cajero, por error, le da c pesos y p centavos. El hombre no se da cuenta hasta que gasta 23 centavos y además se da cuenta que en ese momento tiene $2p$ pesos y $2c$ centavos. ¿Cuál era el valor del cheque?

7.3.22. Resuelva este problema: una compañía compró cierto número de reliquias falsas a 1700 pesos cada una y vendió algunas de ellas a 4900 pesos cada una. Si la cantidad comprada originalmente es mayor que 5000 y menor que 10000 y la compañía obtuvo una ganancia de 24500. ¿Cuántas reliquias faltan por vender?

Definición. Decimos que la terna (a, b, c) de enteros es una terna pitagórica si se satisface que $a^2 + b^2 = c^2$. Llamamos a una terna pitagórica (a, b, c) primitiva si $(a, b, c) = 1$.

7.3.23.

(1) Demuestre que (a, b, c) es una terna pitagórica si y sólo si (ka, kb, kc), $k \in \mathbb{Z} - \{0\}$, es una terna pitagórica.
(2) Si la terna pitagórica (a, b, c) es primitiva, demuestre que
  (I) $(a, b) = (b, c) = (c, a) = 1$.
  (II) a y b tienen diferente paridad.
  (III) Si a es par, entonces b y c son impares.

(IV) Suponiendo que a es un número par, existen números enteros m, n con $m > n$, $(m, n) = 1$ y con distinta paridad tales que

$$a = 2mn, \quad b = m^2 - n^2, \quad c = m^2 + n^2.$$

7.3.24. Si la terna pitagórica (a, b, c) es primitiva, demuestre que

(1) a, b o c es múltiplo de 3.
(2) a o b es múltiplo de 4.
(3) Exactamente un elemento de $\{a, b, c\}$ es múltiplo de 5.

§§ Ejercicios sección 7.4.

7.4.1. Probar el teorema 7.4.6 (Cada número entero $n > 1$ se expresa como producto de primos, no necesariamente distintos y puede aparecer un único primo una sola vez) utilizando el principio del buen orden).

7. 4.2. Demuestre que si p es un número primo y $p \mid a_1 \cdots a_n$, entonces $p \mid a_i$ para alguna $i \in \{1, \ldots, n\}$.

7.4.3. Demuestre que si p es un primo y $1 \leq k < p$, entonces $p \mid C_p^k$.

7.4.4. Sea n un entero positivo. Pruebe que

(1) Si a y b son enteros positivos con $ab = n$, entonces $a^2 \leq n$ o $b^2 \leq n$.
(2) Si n es compuesto, entonces n tiene un divisor primo p que satisface que $p^2 \leq n$.

7.4.5. Demuestre que si $n > 2$, entonces existe un primo p tal que $n < p < n!$.

7.4.6. Sea $a \in \mathbb{Z}^+$. Demuestre que si $a \mid 42n + 37$ y $a \mid 7n + 4$, para algún entero n, entonces $a = 1$ ó $a = 13$.

7.4.7. Sea $p > 2$ un número primo tal que $p \mid (8a - b)$ y $p \mid (8c - d)$, donde $a, b, c, d \in \mathbb{Z}$. Demuestre que $p \mid (ad - bc)$.

7.4.8. Demuestre que

(1) 2 es el único número par que es primo.
(2) 2 y 3 son los únicos enteros consecutivos que son primos.
(3) 3, 5 y 7 son los únicos impares consecutivos que son primos.

7.4.9. Sea $n \in \mathbb{N}$. Demuestre que

(1) Si $n > 4$ y n es compuesto, entonces $n \mid (n - 1)!$.
(2) Si $n > 1$ y $n \mid (n - 1)! + 1$, entonces n es primo.

(3) n es primo si y sólo si $n \nmid (n-1)!$.

7.4.10. Demuestre que

(1) Si p y q son primos tales que $p - q = 3$, entonces $p = 5$.
(2) Si p y $p^2 + 8$ son primos, entonces $p^3 + 4$ también lo es. (Sugerencia: pruebe que $p = 3$)

7.4.11. Demuestre que si $n^2 - 2$ y $n^2 + 2$ son primos, entonces $3 \mid n$.

7. 4.12. Demuestre que si p y q son primos con $p \geq q \geq 5$, entonces $24 \mid p^2 - q^2$.

7.4.13. Demuestre que

(1) Si p es un primo con $p \geq 5$, entonces $p^2 + 2$ es compuesto.
(2) Si p es un primo impar con $p \neq 5$, entonces $p^2 + 1$ o $p^2 - 1$ es divisible por 5.
(3) Si p es primo con $p > 5$, entonces $p - 4$ no puede ser la cuarta potencia de un número entero.

7.4.14. [3] Demuestre que si p es un número primo y $x \mid p^\alpha$, entonces $x = p^\beta$ para algún $\beta \leq \alpha$.

7.4.15. Demostrar que

(1) Todo entero positivo n tienen una expresión única de la forma $n = 2^r m$, donde $r \geq 0$ y m es un entero positivo impar.
(2) Todo entero positivo n tienen una expresión única de la forma $n = 2^a 5^b m$, $a, b \geq 0$, m no es divisible por 2 o por 5.

7.4.16. Sea p un primo, y n y a enteros positivos. Decimos que p^a **divide exactamente** a n, denotado por $p^a \parallel n$, si $p^a \mid n$ pero $p^{a+1} \nmid n$. Muestre que

(1) Si $p^a \parallel m$ y $p^b \parallel n$, entonces $p^{a+b} \parallel mn$.
(2) Si $p^a \parallel m$, entonces $p^{ka} \parallel m^k$, donde k es un entero positivo.
(3) Si $a \neq b$, $m \neq n$, $p^a \parallel m$ y $p^b \parallel n$, entonces $p^{\text{mín}(a,b)} \parallel (m+n)$.
(4) Si $p > 2$, $a \leq b$, $p^n \parallel (m-1)$ y $p^{a+b} \parallel (m^k - 1)$, entonces $p^a \parallel k$.

7. 4.17. Dados los enteros positivos a y b tales que $a \mid b^2$, $b^2 \mid a^3$, $a^3 \mid b^4$, $b^4 \mid a^5 \ldots$, muestre que $a = b$.

7.4.18. Sea $n \in \mathbb{N}$. Demuestre que

(1) Si $2^n + 1$ es un número primo impar, entonces n es una potencia de 2.

[3] Parte del teorema 7.4.12 pág. 266.

(2) Si $2^n - 1$ es primo, entonces n también lo es.

7.4.19. Sean a y n enteros positivos.

(1) Demuestre que, si $a^n - 1$ es un número primo, entonces $a = 2$ y n es un número primo.
(2) Suponga que $a > 1$. Pruebe que, si $a^n + 1$ es un número primo, entonces a es par y n es una potencia de 2.

7.4.20.

(1) Pruebe que todo número primo de la forma $3n + 1$ es de la forma $6k + 1$.
(2) Sea n un entero positivo con $n \neq 1$. Demuestre que, si $n^2 + 1$ es un número primo, entonces $n^2 + 1$ es de la forma $4k + 1$ con $k \in \mathbb{Z}$.
(3) Demuestre que todo entero de la forma $3n + 2$ tiene un factor primo de esa forma.

7.4.21.

(1) Demuestre que el producto de tres enteros consecutivos no puede ser un cuadrado perfecto.
(2) Demuestre que el único primo p, para el cual $3p + 1$ es un cuadrado perfecto, es $p = 5$.
(3) Encuentre todos los primos p tales que $17p + 1$ es un cuadrado perfecto.

7.4.22. Encuéntrese el error en la siguiente "demostración", la cual afirma que no hay primos más grandes que 101.
Suponga que $n > 101$. Si n es par entonces no es primo, de modo que podemos suponer que n es impar. Así, los números $x = \frac{n+1}{2}$ e $y = \frac{n-1}{2}$, son enteros. Luego,

$$n = x^2 - y^2 = (x - y)(x + y)$$

y por lo tanto n no es primo. Así que no hay primos > 101.

7.4.23. Sea p_n el n-ésimo número primo.

(1) Calcule p_n para $n \leq 100$.
(2) Demuestre que $p_{n+1} \leq p \cdot \ldots \cdot p_n + 1$
(3) Usando inducción y el inciso anterior, demuestre que $p_n \leq 2^{2^{n-1}}$

7.4.24. Demuestre que

(1) Cualquier primo impar es de la forma $4k + 1$ o $4k + 3$, donde k es un entero.
(2) Todo entero de la forma $4m + 3$ tiene un factor primo de esa forma.
(3) Hay un número infinito de primos de la forma $4n + 3$.

7.4.25. Demuestre que hay un número infinito de primos de la forma $6n + 5$.

7.4.26. Demuestre que hay un número infinito de primos de la forma $4n + 1$. (Sugerencia: suponga que hay un número finito de primos de esta forma, y sean estos $q_1, \ldots, q_k$. Luego, considere $a = (q_1 \cdot \ldots \cdot q_k)^2 + 1$)

7.4.27. Pruebe o dé un contraejemplo de los siguientes enunciados.

(1) Todos los primos son de la forma $n! + 1$.
(2) Hay una infinidad de números compuestos.
(3) Hay un número infinito de primos que son de la forma $n^3 + 1$, donde n es un entero positivo.
(4) Si n es un número positivo, entonces $n^2 - n + 41$ es un número primo.

7.4.28. Pruebe que los siguientes números son compuestos.

(1) $n! + m$, $2 \leq m \leq n$
(2) $n^5 + n^4 + 1$, $n > 1$
(3) $n^4 + 4$, $n > 1$
(4) $n^4 + 4^n$, $n > 1$
(5) $8^n + 1$, $n \in \mathbb{N}$

7.4.29. Sean a, b, c, d enteros positivos tales que $ab = cd$. Pruebe que $a+b+c+d$ es compuesto.

7.4.30. Determine si los siguientes números enteros son primos o compuestos.

(1) 127	(2) 129	(3) 131	(4) 133
(5) 137	(6) 139	(7) 503	(8) 899
(9) 943	(10) 1511		

7.4.31. Expresar los siguientes números como productos de potencias de primos y encuentre la sucesión de exponentes asociada a cada descomposición.

(1) 51	(2) 87	(3) 361	(4) 367
(5) 8!	(6) 10!	(7) 12!	(8) 945
(9) 1001	(10) 6292	(11) 148500	(12) 7114800
(13) 7882875	(14) $10^6 - 1$	(15) $10^8 - 1$	(16) $2^{15} - 1$
(17) $2^{24} - 1$			

7.4.32. Sean a, b enteros, y sea n un entero positivo. Demuestre que si $(a, b) = 1$, con $a + b \neq 0$, y $p > 2$ es un primo, entonces

$$\left(\frac{a^p + b^p}{a + b}, a + b \right) = \begin{cases} 1 & \text{si } p \nmid (a + b) \\ p & \text{si } p \mid (a + b) \end{cases}$$

7.4.33. Encuentre todas las parejas de enteros a y b tales que
(1) $(a,b) = 12$ y $[a,b] = 360$;
(2) $(a,b) = 20$ y $[a,b] = 840$;
(3) $(a,b) = 18$ y $[a,b] = 3780$;
(4) $ab = 2^4 \cdot 3^4 \cdot 5^3 \cdot 7 \cdot 11^3 \cdot 13$ y $[a,b] = 2^2 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11^2 \cdot 13$.

7.4.34. Sea p un número primo. Si $(a,b) = p$ encuentre los posibles valores de:

(1) $\left(a^2, b\right)$; (2) $\left(a^2, b^2\right)$; (3) $\left(a^3, b\right)$; (4) $\left(a^3, b^2\right)$.

7.4.35. Sea p un número primo. Si $\left(a, p^2\right) = p$ y $\left(b, p^4\right) = p^2$ encuentre los posibles valores de:

(1) $\left(ab, p^5\right)$; (2) $\left(a+b, p^4\right)$; (3) $\left(a-b, p^5\right)$; (4) $\left(pa-b, p^5\right)$.

7.4.36. Sea p un número primo. Si $\left(a, p^2\right) = p$ y $\left(b, p^3\right) = p^2$ encuentre los posibles valores de $\left(a^2b^2, p^4\right)$ y $\left(a^2+b^2, p^4\right)$.

7.4.37. Sea p un número primo y r cualquier entero positivo. ¿Cuáles son los los posibles valores de $(p, p+r)$ y $[p+r, p]$?

7.4.38.
(1) Pruebe que un entero positivo $n > 1$ es un cuadrado perfecto si y sólo si en su descomposición en factores primos todos los exponentes son pares.
(2) Sean n, a y b enteros positivos tales que $ab = n^2$. Si $(a,b) = 1$, pruebe que existen enteros positivos c y d tales que $a = c^2$ y $b = d^2$.
(3) Sea $a_1 \cdot \ldots \cdot a_n = b^k$ con $(a_i, a_j) = 1$, para todo $i \neq j$. Demuestre que para todo $j = 1, \ldots, n$ existe un entero c_j tal que $a_j = c_j^k$.

7.4.39. Sean $a = \prod_{i=1}^{\infty} p_i^{\alpha_i}$, $b = \prod_{i=1}^{\infty} p_i^{\beta_i}$. Demuestre que $(a,b) = 1$ si y sólo si $\alpha_i > 0$ implica que $\beta_i = 0$ y $\beta_i > 0$ implica que $\beta_i = 0$, para todo $i = 1, 2, 3, \ldots$.

7.4.40. Un entero positivo es libre de cuadrados si éste no es divisible por el cuadrado de cualquier entero mayor que 1. Sea $a > 1$ y $a = \prod_{i=1}^{\infty} p_i^{\alpha_i}$. Pruebe que a es libre de cuadrados si y sólo si $\alpha_i \leq 1$, para todo $i = 1, 2, 3, \ldots$.

7.4.41.

(1) Sea $a \in \mathbb{Z}$ con $a > 1$ y sea $a = \prod_{i=1}^{\infty} p_i^{\alpha_i}$. Demuestre lo siguiente:

(I) Todo divisor positivo de a es de la forma $\prod_{i=1}^{\infty} p_i^{\beta_i}$ con $\alpha_i \geq \beta_i \geq 0$, para todo $i = 1, 2, 3, \ldots$.

(II) El número de divisores positivos de a es $\prod_{i=1}^{\infty}(\alpha_i + 1)$.

(2) Encuentre el número de divisores positivos de los números

(I) 148500;

(II) 7114800;

(III) 7882875.

7. 4.42. [4] Sean $a_1, a_2, \ldots, a_n \in \mathbb{Z}^+ - \{1\}$, donde, para cada $1 \leq j \leq n$, $a_j = \prod_{i=1}^{\infty} p_i^{\alpha_{ji}}$. Demuestre lo siguiente:

(1) $(a_1, a_2, \ldots, a_n) = \prod_{i=1}^{\infty} p_i^{\gamma_i}$, donde $\gamma_i = \text{mín}\{\alpha_{1i}, \alpha_{2i}, \ldots, \alpha_{ni}\}$, para toda $i = 1, 2, 3, \ldots$.

(2) $[a_1, a_2, \ldots, a_n] = \prod_{i=1}^{\infty} p_i^{\delta_i}$, donde $\delta_i = \text{máx}\{\alpha_{1i}, \alpha_{2i}, \ldots, \alpha_{ni}\}$, para toda $i = 1, 2, 3, \ldots$.

7.4.43. Demuestre que

(1) $(a, b)^2 \nmid [a, b]$ a menos que $(a, b) = 1$.

(2) $([a, b], c) = [(a, c), (b, c)]$, para todo $a, b, c \in \mathbb{Z}$ no nulos.

7.4.44. Encuentre cinco enteros $a_1, \ldots, a_5$ tales que:

(1) $(a_1, \ldots, a_5) = 1$ y

(2) si $i \neq j$, entonces $(a_i, a_j) \neq 1$.

7.4.45.

(1) Halle el cuadrado perfecto más pequeño que es divisible entre 7!.

(2) Encuentre el entero positivo más pequeño para el cual el producto $1260n$ es un cubo .

(3) Encuentre un número entero de forma que tenga exactamente 14 divisores positivos.

[4] Parte de la proposición 7.4.13.

(4) Encontrar el entero más pequeño divisible por 2 y 3 que es a la vez un cuadrado y una quinta potencia.
(5) Encuentre el menor entero positivo tal que tenga exactamente 12 divisores positivos.
(6) Halle dos números, uno con 21 divisores positivos y el otro con 10 divisores positivos cuyo máximo común divisor sea 18.
(7) Halle la suma de todos los divisores positivos de 360.
(8) Halle el producto de todos los divisores positivos de 360.

7.4.46. Sean p, q y r primos distintos. Para cada inciso, determine el máximo común divisor y el mínimo común múltiplo del los números en cuestión.

(1) $p^2q^3,\ pq^2r$
(2) $p^3qr^3,\ p^3q^4r^5$
(3) $2^3 \cdot 3^3 \cdot 5 \cdot 7,\ 2^2 \cdot 3^2 \cdot 5 \cdot 7^2$
(4) $2^2 \cdot 5^2 \cdot 7^3 \cdot 11^2,\ 3 \cdot 5 \cdot 11 \cdot 13 \cdot 17$
(5) $2^2 \cdot 5^7 \cdot 11^{13},\ 3^2 \cdot 7^5 \cdot 13^{11}$
(6) $3 \cdot 17 \cdot 19^2 \cdot 23,\ 5 \cdot 7^2 \cdot 11 \cdot 19 \cdot 29$
(7) 1001, 6292
(8) 422, 48
(9) 340, 260, 945
(10) 5076, 1076, 6292

7.4.47. Sean $a, b, c \in \mathbb{Z}$ no nulos.

(1) Si $[a,b,c] \cdot (a,b,c) = |abc|$, pruebe que $(a,b) = (b,c) = (a,c) = 1$.
(2) Demuestre que si x, y, z son enteros positivos, entonces

$$\begin{aligned} \text{máx}(x,y,z) &= x + y + z - \text{mín}(x,y) - \text{mín}(x,z) - \text{mín}(y,z) \\ &\quad + \text{mín}(x,y,z) \end{aligned}$$

(3) Use el inciso anterior para probar que $[a,b,c] \cdot (ab, bc, ca) = |abc|$.

7.4.48.

(1) Encuentre enteros a, b y c tales que $[a,b] = 1000$, $[b,c] = 2000$ y $[c,a] = 2000$.
(2) Sean a, b y c enteros. Muestre que

$$\frac{[a,b,c]^2}{[a,b] \cdot [b,c] \cdot [c,a]} = \frac{(a,b,c)^2}{(a,b) \cdot (b,c) \cdot (c,a)}.$$

7. 4.49. Determine si los siguientes enunciados son verdaderos o falsos. Si son verdaderos, probar el resultado, y si son falsos, dar un contraejemplo.

(1) Si $(a, b) = [a, c]$, entonces $[a, b] = [a, c]$.
(2) Si $(a, b) = (a, c)$, entonces $[a^2, b^2] = [a^2, c^2]$.
(3) Si $(a, b) = (a, c)$, entonces $(a, b) = (a, b, c)$.
(4) Si p es un primo y $(a, p^2) = p$, entonces $(a^2, p^2) = p^2$.
(5) Si p es un primo y $(a, p^2) = (b, p^2) = p$, entonces $(ab, p^4) = p^2$.
(6) Si p es un primo y $(a, p^2) = p$, entonces $(a + p, p^2) = p$.
(7) Si p es un primo, $p \mid a$ y $p \mid (a^2 + b^2)$, entonces $p \mid b$.
(8) Si p es un primo y $p \mid a^n$, $n > 1$, entonces $p \mid a$.
(9) Si $a^n \mid c^n$, entonces $a \mid c$.
(10) Si $a^m \mid c^n$, $m > n$, entonces $a \mid c$.
(11) Si $a^m \mid c^n$, $n > m$, entonces $a \mid c$.
(12) Si p es un primo y $p^4 \mid a^3$, entonces $p^2 \mid a$.
(13) Si p es un primo, $p \mid (a^2 + b^2)$ y $p \mid (b^2 + c^2)$, entonces $p \mid (a^2 - c^2)$.
(14) Si p es un primo, $p \mid (a^2 + b^2)$ y $p \mid (b^2 + c^2)$, entonces $p \mid (a^2 + c^2)$.
(15) Si $(a, b) = 1$, entonces $(a^2, ab, b^2) = 1$.
(16) $[a^2, b^2] = [a^2, ab, b^2]$.
(17) Si $b \mid (a^2 + 1)$, entonces $b \mid (a^4 + 1)$.
(18) Si $b \mid (a^2 - 1)$, entonces $b \mid (a^4 - 1)$.
(19) $(a, b, c) = ((a, b), (a, c))$.

7. 4.50. Sea $p \in \mathbb{Z}^+$ un número primo y $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. Demuestre que, si $p \mid a_1 \cdot a_2 \cdot \ldots \cdot a_n$, entonces $p \mid a_i$, para alguna $i \in \{1, 2, \ldots, n\}$.

7.4.51. Dados $a, b \in \mathbb{Z} - \{0\}$, demostrar que existe un conjunto de números primos $\{p_1, p_2, \ldots, p_r\}$ y enteros no negativos α_i, β_i con $1 \leq i \leq r$ tales que

$$
\begin{aligned}
a &= \pm p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}; \\
b &= \pm p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_r^{\beta_r}.
\end{aligned} \tag{5}
$$

7.4.52. Sean $a \in \mathbb{Z} - \{0\}$ tal que $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}$.

(1) ¿Qué condiciones deben satisfacer los exponentes α_i's, para que a sea un cuadrado? ¿Tal condición es suficiente?

(2) ¿Qué condiciones deben satisfacer los exponentes α_i's, para que a sea un cubo?[5]
(3) Si $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_r^{\beta_r}$, ¿qué condiciones deben satisfaces los exponentes α_i's y β_j's, para que $a \mid b$? y ¿para que $a^2 \mid b^2$?

7.4.53. Sean $a, b \in \mathbb{Z} - \{0\}$ y supóngase que ambos se expresan como en (5). Demostrar que $[a, b] = p_1^{\delta_1} \cdot p_2^{\delta_2} \cdot \ldots \cdot p_r^{\delta_r}$, donde $\delta_i = \text{máx}\{\alpha_i, \beta_i\}$ para toda $i = 1, \ldots, r$.

7.4.54. Sea $\{a_1, a_2, \ldots, a_n\} \subseteq \mathbb{Z} - \{0\}$ tales que $a_i = \pm p_1^{\alpha_{i1}} \cdot p_2^{\alpha_{i2}} \cdot \ldots \cdot p_k^{\alpha_{ik}}$, donde $\alpha_{ij} \in \mathbb{Z}^+ \cup \{0\}$, para toda $1 \leq i \leq n$ y $1 \leq j \leq k$. Demostrar que
(1) $(a_1, a_2, \ldots, a_n) = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \ldots \cdot p_k^{\gamma_k}$, donde $\gamma_j = \text{mín}\{\alpha_{1j}, \alpha_{2j}, \ldots, \alpha_{nj}\}$ para toda $1 \leq j \leq k$.
(2) $[a_1, a_2, \ldots, a_n] = p_1^{\delta_1} \cdot p_2^{\delta_2} \cdot \ldots \cdot p_k^{\delta_k}$, donde $\delta_j = \text{máx}\{\alpha_{1j}, \alpha_{2j}, \ldots, \alpha_{nj}\}$ para toda $1 \leq j \leq k$.
(*Sugerencia: Utilizar inducción sobre* $n \geq 2$.)

§§ Ejercicios sección 7.5.

7.5.1. Sean $a, b, c, d \in \mathbb{Z}$ y $m, n \in \mathbb{Z}^+$. Demuestre que
(1) Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$, entonces $ax + cy \equiv bx + dy \pmod{m}$ para todo $x, y \in \mathbb{Z}$;
(2) $a \equiv b \pmod{m}$ si y sólo si $a + c \equiv b + c \pmod{m}$;
(3) Si $a \equiv b \pmod{m}$, entonces $(a, m) = (b, m)$;
(4) $ca \equiv cb \pmod{m}$ si y sólo si $a \equiv b \left(\text{mód } \frac{m}{(c,m)}\right)$;
(5) Si $d > 0$ es tal que $d \mid a$, $d \mid b$ y $d \mid m$, entonces $\frac{a}{d} \equiv \frac{b}{d} \left(\text{mód } \frac{m}{d}\right)$;
(6) Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{n}$, entonces $a + c \equiv b + d \pmod{(m, n)}$;
(7) Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{n}$, entonces $ac \equiv bd \pmod{(m, n)}$.

7.5.2. Sea $m \in \mathbb{Z}^+$, y sean $a_k, b_k \in \mathbb{Z}$ con $k = 1, 2, \ldots, n$. Demuestre que si $a_k \equiv b_k \pmod{m}$, para todo $k = 1, 2, \ldots, n$, entonces
(1) $\sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} b_i \pmod{m}$;
(2) $\prod_{i=1}^{n} a_i \equiv \prod_{i=1}^{n} b_i \pmod{m}$.

7.5.3. Demuestre que si $0 \leq a < m$, $0 \leq b < m$, y $a \equiv b \pmod{m}$, entonces $a = b$.

[5] Esto es, $a = c^3$, para algún $c \in \mathbb{Z}$.

7.5.4. Diga si los siguientes enunciados son verdaderos o falsos, justificando su respuesta.

(1) $7 \equiv 5 \pmod 2$;
(2) $8 \equiv 12 \pmod 3$;
(3) $57 \equiv 208 \pmod 4$;
(4) $0 \equiv -5 \pmod 5$;
(5) $59 \equiv 31 \pmod 6$;
(6) $18 \not\equiv -2 \pmod 4$;
(7) $531 \not\equiv 1236 \pmod{7561}$;
(8) $12321 \not\equiv 111 \pmod 3$;
(9) Si $a \not\equiv b \pmod m$, entonces $m \nmid (a - b)$;
(10) Si $a \not\equiv b \pmod m$, entonces $b \not\equiv a \pmod m$;
(11) Si $a \not\equiv b \pmod m$ y $b \not\equiv c \pmod m$, entonces $a \not\equiv c \pmod m$;
(12) Si $a^n \equiv b^n \pmod m$, entonces $a \equiv b \pmod m$;
(13) Si $a \equiv b \pmod m$ y $a \equiv b \pmod n$, entonces $a \equiv b \pmod{m+n}$;
(14) Si $a \equiv b \pmod m$ y $a \equiv b \pmod n$, entonces $a \equiv b \pmod{mn}$;
(15) Si $ac \equiv bc \pmod m$, entonces $a \equiv b \pmod m$;
(16) Si $a + c \equiv b + d \pmod m$, entonces $a \equiv b \pmod m$ y $c \equiv d \pmod m$;
(17) Si $ac \equiv bc \pmod m$, entonces $a \equiv b \pmod m$;
(18) Si $ab \equiv 0 \pmod m$, entonces $a \equiv 0 \pmod m$ y $b \equiv 0 \pmod m$;
(19) Si $a \not\equiv 0 \pmod m$ y $b \not\equiv 0 \pmod m$, entonces $ab \not\equiv 0 \pmod m$;
(20) Si $(a, m) = (b, m)$, entonces $a \equiv b \pmod m$.

7.5.5. Diga para cuáles enteros positivos m se cumplen las siguientes afirmaciones, justificando su respuesta.

(1) $13 \equiv 5 \pmod m$
(2) $10 \equiv 9 \pmod m$
(3) $-7 \equiv 6 \pmod m$
(4) $100 \equiv -5 \pmod m$

7.5.6.

(1) Supongamos que en este momento son las 10 de la mañana; ¿qué hora será dentro de 2500 horas? ¿qué hora fue hace 2500 horas?
(2) Si son las 6 de la noche; ¿qué hora fue hace 50 horas?
(3) Si hoy es jueves; ¿qué día será dentro de 129 días?
(4) Si hoy es viernes; ¿qué día fue hace 1976 días?

7.5.7. Para los siguientes valores de a y m, encuentre $i \in \{0, 1, \ldots, m\}$ tal que $a \equiv i \ (mod\ m)$.

(1) -157 es dividido por 11;
(2) 442 es dividido por 26;
(3) -531 es dividido por89;
(4) 16^{16} es dividido por 6;
(5) 2^{35} es dividido por 7;
(6) 3^{247} es dividido por 17;
(7) 23^{1001} es dividido por17;
(8) 3^{247} es dividido por 25;
(9) 3^{1000} es dividido por 7;
(10) $37^4 - 49 \cdot 801 + 120$ es dividido por 5;
(11) $1^5 + 2^5 + 3^5 + \cdots + 11^5$ es dividido por 3;
(12) $1^5 + 2^5 + 3^5 + \cdots + 11^5$ es dividido por 7;
(13) $1! + 2! + 3! + \cdots + 100!$ es dividido por 11;
(14) $1! + 2! + 3! + \cdots + 100!$ es dividido por 15;
(15) $1! + 2! + 3! + \cdots + 300!$ es dividido por 13;
(16) $1! + 2! + 3! + \cdots + 1000!$ es dividido por 10;
(17) $1! + 2! + 3! + \cdots + 1000!$ es dividido por 12;
(18) $1! + 2! + 3! + \cdots + (10^{10})!$ es dividido por 24;
(19) $C_3^3 + C_4^3 + C_5^3 + \cdots + C_{102}^3$ es dividido por 7.

7.5.8. Sea n un entero positivo. Pruebe que

$$1 + 2 + 3 + \cdots + (n-1) \equiv 0 \ (\text{ mód } n)$$

si y sólo si n es impar.

7.5.9. Sea n un entero positivo. Demuestre que

$$1^2 + 2^2 + 3^2 + \cdots + (n-1)^2 \equiv 0 \ (\text{ mód } n)$$

si y sólo si $n \not\equiv \pm 1$ (mód 6).

7.5.10. Sea n un entero positivo. Demuestre que

$$1^3 + 2^3 + 3^3 + \cdots + (n-1)^3 \equiv 0 \ (\text{ mód } n)$$

si y sólo si $n \equiv 2$ (mód 4).

7.5.11. Demuestre los siguientes criterios de divisibilidad:

(1) Un número es divisible por 2 si y sólo si su último dígito es par.

(2) Un número es divisible por 3 si y sólo si la suma de sus dígitos es múltiplo de 3.
(3) Un número es divisible por 4 si y sólo si sus últimos dos dígitos son 00 o forman un número divisible por 4.
(4) Un número es divisible por 5 si y sólo si su último dígito es 0 ó 5.
(5) Un número es divisible por 8 si y sólo si sus últimos tres dígitos son 000 o forman un número divisible por 8.
(6) Un número es divisible por 9 si y sólo si la suma de sus dígitos el múltiplo de 9.
(7) Un número es divisible por 10 si y sólo si su último dígito es 0.

7.5.12. Encuentre criterios para determinar si un número entero es divisible por 6, 7, 11, 12 ó 13, y demuéstrelos.

7.5.13. Sea n un entero con $n > 1$. Demuestre que n es divisible por 2^m si y sólo si el entero formado por los m últimos dígitos de n es divisible por 2^m.

7.5.14.

(1) Hallar un criterio de divisibilidad por 37. (Sugerencia: $10^3 \equiv 1$ (mód 37))
(2) Hallar un criterio de divisibilidad por 73. (Sugerencia: $10^4 \equiv -1$ (mód 73))
(3) Hallar un criterio de divisibilidad por 14, 18, 19 y 21.

7.5.15. Sea $n \in \mathbb{Z}^+$ con $n = (r_k r_{k-1} \cdots r_0)_{10}$. Demuestre que

(1) n es divisible por 7, 11 y 13 si y sólo $(r_k r_{k-1} \cdots r_3)_{10} - (r_2 r_1 r_0)_{10}$ es divisible por 7, 11 y 13.
(2) n es divisible por 27 y 37 si y sólo $(r_k r_{k-1} \cdots r_3)_{10} + (r_2 r_1 r_0)_{10}$ es divisible por 27 y 37.

7.5.16. Encuéntrese los dígitos W, X, Y y Z de modo que se cumpla que:

(1) El número de cuatro dígitos $(4WX8)_{10}$ sea divisible por 2, 3, 4, 6, 8 y 9;
(2) El número de siete dígitos $(21358YZ)_{10}$ sea divisible por 99.

7. 5.17. Sean $(m_1, m_2) = 1$. ¿En qué casos se puede afirmar que $a \equiv b$ (mód m_1) y $a \equiv b$ (mód m_2) implica $a \equiv b$ (mód $m_1 \cdot m_2$)?

7.5.18. Demuestre que si $a \equiv b$ (mód m), entonces $(a, m) = (b, m)$.

7.5.19. Demuestre que si m es compuesto y $m > 4$, entonces

$$(m-1)! \equiv 0 \ (\text{ mód } m).$$

7. 5.20. Un palíndromo es un número que se lee igual hacia delante y hacia detrás. Por ejemplo, 22, 1331 y 935686539 son palíndromos. Demostrar que todo palíndromo con un número par de dígitos es divisible por 11.

7.5.21.

(1) Demostrar que ningún cuadrado tiene como último dígito 2, 3, 7 u 8.
(2) Determine si los números 98, 121 y 16151613924 son cuadrados.

7.5.22. Demostrar que la diferencia de dos cubos consecutivos nunca es divisible por 5.

7.5.23. Suponga que $ac \equiv b \pmod{m}$ y que $bc \equiv a \pmod{m}$ para algún entero c. Demuestre que $a^2 \equiv b^2 \pmod{m}$. Encuentre un ejemplo no trivial de enteros a, b, c y m que satisfacen este resultado.

7.5.24. Demostrar que para cualquiera $k > 0$ y $m \geq 1$, $x \equiv 1 \pmod{m^k}$ implica que
$x^m \equiv 1 \pmod{m^{k+1}}$.

7. 5.25. Demuestre que si $a^k \equiv b^k \pmod{m}$ y $a^{k+1} \equiv b^{k+1} \pmod{m}$, donde a, b, k y m son enteros con $k > 0$ y $m > 0$ tales que $(a, m) = 1$, entonces $a \equiv b \pmod{m}$.

7.5.26. Sean $a, b \in \mathbb{Z}$, y sea p un primo. Demuestre que

(1) Si $a^2 \equiv b^2 \pmod{p}$, entonces $a \equiv \pm b \pmod{p}$.
(2) Si $a^2 \equiv a \pmod{p}$, entonces $a \equiv 0 \pmod{p}$ o $a \equiv 1 \pmod{p}$.

7. 5.27. Sea n un entero positivo. Demostrar que $5^n \equiv 1 + 4n \pmod{16}$ y $5^n \equiv 1 + 4n + 8n(n-1) \pmod{64}$.

7.5.28. Demostrar que si $a \equiv b \pmod{n}$, entonces $a^n \equiv b^n \pmod{n^2}$. ¿Es cierto el resultado inverso?

7.5.29. Sea p un primo, y sea k un entero con $1 \leq k \leq p-1$. Demostrar que

$$C_{p-1}^k \equiv (-1)^k \pmod{p}.$$

7.5.30. Sea p un primo. Demostrar que $C_{2p}^p \equiv 2 \pmod{p}$.

7.5.31. Sea n un entero positivo y p un primo con $n < p \leq 2n$. Demostrar que $C_{2n}^n \equiv 0 \pmod{p}$, pero que $C_{2n}^n \not\equiv 0 \pmod{p^2}$.

7.5.32. Si $(a, 6) = 1$, muestre que $a^2 \equiv 1$ (mód 24). ¿Qué sucede cuando $(a, 6) > 1$?

7.5.33. Demuestra, usando congruencias, que

$$\left(a^{2^n} + 1, a^{2^m} + 1\right) = \begin{cases} 1 & \text{si } a \text{ es par} \\ 2 & \text{si } a \text{ es impar} \end{cases}$$

donde a, m, n son enteros positivos con $m \neq n$. (Sugerencia: si d es un divisor común,
$a^{2^m} \equiv -1$ (mód d). Elevar esto a la potencia 2^{n-m}, suponiendo $m < n$)

Conjunto completo de representantes módulo m

7.5.34. ¿Cuáles de los siguientes conjuntos de enteros forman un conjunto completo de representantes módulo 11?

(1) $\{0, 1, 2, 4, 8, 16, 32, 64, 128, 256, 512\}$
(2) $\{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21\}$
(3) $\{2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22\}$
(4) $\{0, 1, 2, 2^2, 2^3, ..., 2^9\}$
(5) $\{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$

7.5.35. Encuentre un conjunto completo de representantes módulo 7 cuyos elementos son todos

(1) impares;
(2) pares;
(3) primos.

¿Existe un conjunto completo de representantes módulo 7 cuyos elementos son todos cuadrados perfectos?

7.5.36. Sea $\{a_1, \ldots, a_m\}$ un conjunto completo de representantes módulo m. Suponga
$\{b_1, \ldots, b_m\}$ es un conjunto de enteros tal que $b_i \equiv a_i$ (mód m), para todo $i = 1, \ldots, m$. Demuestre que $\{b_1, \ldots, b_r\}$ es también un conjunto completo de representantes módulo m.

7.5.37. Demuestre que si los elementos del conjunto $\{a_1, \ldots a_m\}$ son todos incongruentes entre si módulo m, entonces $\{a_1, \ldots a_m\}$ es un conjunto completo de representantes módulo m.

7.5.38. Demuestre que $\{5, -4, 12, 3, 4\}$ es un conjunto completo de representantes módulo 5.

7.5.39.

(1) Dé un sistema completo de representantes módulo 17.
(2) Dé un sistema completo de representantes módulo 17 que conste de múltiplos de 3.
(3) De un sistema reducido de representantes módulo 12.

7.5.40. Demuestre que $5^{18} \equiv 1 \pmod 7$.

7.5.41. Demuestre que $a^7 \equiv a \pmod{42}$ para todo entero a.

7.5.42. Sean m un número entero impar y $\{a_1, \ldots a_m\}$ un conjunto completo de representantes módulo m. Demostrar que $a_1 + a_2 + \cdots a_m \equiv 0 \pmod m$.

7.5.43. Suponga que $\{a_1, \ldots, a_n\}$ es un conjunto completo de representantes módulo n. Sea c un entero con $(c, m) = 1$ y b cualquier entero. Pruebe que $\{ca_1 + b, \ldots, ca_r + b\}$ es un conjunto completo de representantes módulo m.

7.5.44. Suponga que $R = \{r_1, \ldots, r_n\}$ es un conjunto completo de representantes módulo n y $\{s_1, \ldots, s_m\}$ es un conjunto completo de representantes módulo m. Demuestre que si $(m, n) = 1$ entonces

$$\{mr_i + ns_j \mid \ r_i \in R,\ s_j \in S, \text{para } 1 \leq i \leq n \text{ y } 1 \leq j \leq m\}$$

forma un conjunto completo de representantes módulo mn.

Teorema de Fermat

7.5.45. Use el teorema de Fermat para encontrar el residuo cuando

(1) 29^{202} es dividido por 13;
(2) 71^{71} es dividido por 17;
(3) $3^{1000000}$ es dividido por 19;
(4) 99^{999999} es dividido por 23.

7.5.46. Sean a y b dos enteros. Demuestre que

(1) Si $a^p \equiv b^p \pmod p$, entonces $a \equiv b \pmod p$.
(2) Si $a^p \equiv b^p \pmod p$, entonces $a^p \equiv b^p \pmod{p^2}$.

7.5.47. Sean p y q primos distintos, y sea a un entero positivo. Demuestre que

(1) Si $a^p \equiv a \pmod p$ y $a^q \equiv a \pmod p$, entonces $a^{pq} \equiv a \pmod{pq}$.

(2) $a^{pq} - a^p - a^q + a \equiv 0 \pmod{pq}$.
(3) $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.
(4) $p^q + q^p \equiv p + q \pmod{pq}$.

7.5.48. Sean p y q números primos impares tales que $p - 1 \mid q - 1$. Si $a \in \mathbb{Z}$ con $(a, pq) = 1$, pruebe que $a^{q-1} \equiv 1 \pmod{pq}$.

7.5.49. Sea $a \in \mathbb{Z}$, y sea p un número primo. Demuestre que $p \mid a^p + (p-1)!a$ y $p \mid (p-1)!a^p + a$.

7.5.50. Sea p un primo impar y a un entero positivo. Demuestre que

(1) $1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \pmod{p}$;
(2) $1^p + 2^p + \cdots + (p-1)^p \equiv 0 \pmod{p}$;
(3) $(a+1)^p + (a+2)^p + \cdots + (a+p-1)^p \equiv -a \pmod{p}$.

Teorema de Wilson

7. 5.51. Demuestre el teorema de Wilson: p es un número primo si y sólo si $(p-1)! \equiv -1 \pmod{p}$.

7.5.52. Use el teorema de Wilson para encontrar $i \in \{0, \ldots, m-1\}$ tal que $a \equiv i \pmod{m}$ para cada uno de los valores dados a a y m, respectivamente.

(1) 30! es dividido por 31;
(2) 88! es dividido por 89;
(3) 21! es dividido por 23;
(4) 64! es dividido por 67;
(5) $\frac{31!}{22!}$ es dividido por 11;
(6) $\frac{65!}{51!}$ es dividido por 17.

7.5.53.

(1) Demuestre que si p es un primo impar, entonces $2(p-3)! \equiv -1 \pmod{p}$.
(2) Encuentre el residuo cuando 2(100!) es dividido por 103.

7.5.54. Sea $n \in \mathbb{N}$ con $n > 1$. Demuestre que n es un número primo si y sólo si $(n-2)! \equiv 1 \pmod{n}$.

7.5.55.

(1) Sea p un número primo, y sea r un entero tal que $1 \leq r < p$. Si $(-1)^r r! \equiv 1 \pmod{p}$, muestre que $(p-r-1)! \equiv -1 \pmod{p}$.

(2) Use el inciso anterior para probar que $259! \equiv -1 \pmod{269}$ y $463! \equiv -1 \pmod{479}$.

7.5.56. Sea p es un número primo impar. Demuestre que

(1) $1^2 \cdot 3^2 \cdots (p-2)^2 \equiv (-1)^{\frac{p+2}{2}} \pmod{p}$;
(2) $2^2 \cdot 4^2 \cdots (p-1)^2 \equiv (-1)^{\frac{p+2}{2}} \pmod{p}$.

7.5.57. Sea p es un número primo. Demuestre que si $p \equiv 3 \pmod 4$, entonces $\left(\frac{p-1}{2}\right)! \equiv \pm 1 \pmod{p}$.

§§ Ejercicios sección 7.6.

7.6.1. Demuestre la proposición 7.6.3

7.6.2. Diga si las siguientes ecuaciones tienen solución, y si sí tienen solución dé todas las soluciones incongruentes según el módulo:

(1) $2x \equiv 5 \pmod 7$;
(2) $14x - 2 \equiv x + 3 \pmod 7$;
(3) $4x + 1 \equiv 1 - 5x \pmod 3$;
(4) $-9x + 2 \equiv 3x - 2 \pmod 4$;
(5) $(2n + 1)x \equiv -7 \pmod 9$;
(6) $(3n - 2)x + 5n \equiv 0 \pmod{9n - 9}$;
(7) $3x \equiv 6 \pmod 9$;
(8) $8x \equiv 14 \pmod{24}$;
(9) $57x \equiv 208 \pmod 4$;
(10) $3x + 1 \equiv 15x - 4 \pmod{20}$;
(11) $362x \equiv 236 \pmod{24}$;
(12) $12345x \equiv 111 \pmod 6$;
(13) $980x \equiv 1500 \pmod{1600}$;
(14) $128x \equiv 833 \pmod{1001}$;
(15) $6789783x \equiv 2474010 \pmod{28927591}$.

7.6.3. Construir congruencias lineales $ax \equiv b \pmod{20}$ con ninguna solución, con 5 soluciones incongruentes módulo 20 y con 13 soluciones incongruentes módulo 20.

7.6.4. (1) ¿Para qué valores $0 \leq c < 30$ la congruencia $12x \equiv c \pmod{30}$ tiene solución?. En el caso en el que haya solución, ¿cuántas soluciones incongruentes módulo 30 tiene?

(2) ¿Para qué valores $0 \leq c < 1001$ la congruencia $154x \equiv c \pmod{1001}$ tiene solución?. En el caso en el que haya solución, ¿cuántas soluciones incongruentes módulo 1001 tiene?

7.6.5. Un astrónomo sabe que un satélite orbita la Tierra en un período que es un múltiplo exacto de una hora y que es menor que un día. Si el astrónomo observa que el satélite completa 11 órbitas en un intervalo de tiempo que comienza cuando un reloj (de 24 horas) marca las 0 horas de un día dado y termina cuando el reloj marca las 17 horas de otro día. ¿Cuánto dura el período de órbita del satélite?

7.6.6. Demuestre que para cualesquiera $a, b \in \mathbb{Z}$, si p es primo y $p \nmid a$, entonces la congruencia $ax \equiv b \pmod{p}$ tiene solución y todas las soluciones son congruentes módulo p.

7.6.7. Demuestre que si $a \equiv a' \pmod{m}$ y $b \equiv b' \pmod{m}$, entonces las congruencias lineales $ax \equiv b \pmod{m}$ y $a'x \equiv b' \pmod{m}$ tienen exactamente el mismo conjunto de soluciones.

7.6.8. Demuestre que la congruencia lineal $ax \equiv 1 \pmod{8}$ tiene solución si y sólo si a es impar.

7.6.9. Resuelva cada uno de los siguientes sistemas de congruencias.

$$(a)\begin{cases} x \equiv 4 \pmod{6} \\ x \equiv 13 \pmod{15} \end{cases} \quad (b)\begin{cases} x \equiv 10 \pmod{60} \\ x \equiv 80 \pmod{350} \end{cases} \quad (c)\begin{cases} x \equiv 2 \pmod{910} \\ x \equiv 93 \pmod{1001} \end{cases}$$

$$(d)\begin{cases} 2x \equiv 0 \pmod{3} \\ 3x \equiv 2 \pmod{5} \\ 5x \equiv 4 \pmod{7} \end{cases} \quad (e)\begin{cases} x \equiv 5 \pmod{6} \\ x \equiv 3 \pmod{10} \\ x \equiv 8 \pmod{15} \end{cases} \quad (f)\begin{cases} x \equiv 2 \pmod{9} \\ x \equiv 8 \pmod{15} \\ x \equiv 10 \pmod{25} \end{cases}$$

$$(g)\begin{cases} 3x \equiv 2 \pmod{4} \\ 4x \equiv 1 \pmod{5} \\ 6x \equiv 3 \pmod{9} \end{cases} \quad (h)\begin{cases} 5x \equiv 3 \pmod{7} \\ 2x \equiv 4 \pmod{8} \\ 3x \equiv 6 \pmod{9} \end{cases} \quad (i)\begin{cases} x \equiv 2 \pmod{6} \\ x \equiv 4 \pmod{8} \\ x \equiv 2 \pmod{14} \\ x \equiv 14 \pmod{15} \end{cases}$$

$$(j)\begin{cases} x \equiv 7 \pmod 9 \\ x \equiv 2 \pmod{10} \\ x \equiv 3 \pmod{12} \\ x \equiv 6 \pmod{15} \end{cases} \qquad (k)\begin{cases} 3x - 1 \equiv 3 \pmod 9 \\ x + 1 \equiv 0 \pmod 6 \\ 2x \equiv 5x + 1 \pmod 2 \end{cases}$$

$$(l)\begin{cases} 2x \equiv 1 \pmod 7 \\ x \equiv 1 \pmod 5 \\ 2x - 3 \equiv 29 - 2x \pmod 6 \\ x + 3 \equiv 5x - 3 \pmod 2 \end{cases}$$

7.6.10. Suponga que

$$\begin{cases} x \equiv r \ (\text{ mód } m) \\ x \equiv s \ (\text{ mód } m+1). \end{cases}$$

Demostrar que $x \equiv r(m+1) - sm \pmod{m(m+1)}$.

7.6.11. Si $m_i \geq 1$, para $1 \leq i \leq k$, demuestre que

$$x \equiv y \ (\text{ mód } [m_1, \ldots, m_k]) \iff \begin{cases} x \equiv y & (\text{ mód } m_1) \\ x \equiv y & (\text{ mód } m_2) \\ \vdots & \vdots \\ x \equiv y & (\text{ mód } m_k). \end{cases}$$

7.6.12. Sean $m_1, m_2, \ldots, m_k \in \mathbb{Z}^+$, k números primos relativos por parejas, y sean $b_1, \ldots, b_k$ enteros cualesquiera. Pongamos $m = m_1 m_2 \cdots m_k$. Para $i \in \{1, 2, \ldots, k\}$, sea a_i el producto de todos los $m_j's$ excepto el i-ésimo, esto es, $a_i = \frac{m}{m_i}$. Como $(a_i, m_i) = 1$ existe c_i tal que $c_i a_i \equiv 1 \pmod{m_i}$ (¿por qué?). Utilizando estos números definimos x_0:

$$x_0 = a_1 b_1 c_1 + a_2 b_2 c_2 + \cdots + a_k b_k c_k$$

Demuestre que x_0 es solución del sistema de congruencias lineales

$$\begin{cases} x \equiv b_1 & (\text{ mód } m_1) \\ x \equiv b_2 & (\text{ mód } m_2) \\ \vdots & \vdots \\ x \equiv b_k & (\text{ mód } m_k). \end{cases}$$

7.6.13. Considere el sistema de congruencias:

$$\begin{cases} a_1x \equiv b_1 & (\text{mód } m_1) \\ a_2x \equiv b_2 & (\text{mód } m_2) \\ \quad\vdots & \quad\vdots \\ a_kx \equiv b_k & (\text{mód } m_k), \end{cases}$$

donde $\left(m_i, m_j\right) = 1$ si $i \neq j$ y $(a_i, m_i) = 1$ para $1 \leq i \leq k$. Pongamos $m = m_1m_2 \cdots m_k$. Para $i \in \{1, 2, \ldots, k\}$, sea t_i el producto de todos los $m_j's$ excepto el i-ésimo, esto es, $t_i = \frac{m}{m_i}$. Como $(t_i, m_i) = 1$ existe y_i tal que $y_it_i \equiv 1$ (mód m_i). Como $(a_i, m_i) = 1$ cada ecuación $a_ix \equiv b_i$(mód m_i) tendrá una solución x_i. Utilizando estos números definimos x_0:

$$x_0 = y_1t_1x_1 + y_2t_2x_2 + \cdots + y_kt_kx_k$$

Demuestre que x_0 es solución del sistema de congruencias lineales y las demás soluciones son de la forma $x = x_0 + \lambda m$, $\lambda \in \mathbb{Z}$.

7.6.14. Halle cuatro enteros consecutivos que sean múltiplos de 5, 7, 9 y 11 respectivamente.

7.6.15.

(1) Encontrar n tal que $3^2 \mid n$, $4^2 \mid (n + 1)$ y $5^2 \mid (n + 2)$.
(2) ¿Puede encontrarse un n tal que $2^2 \mid n$, $3^2 \mid (n + 1)$ y $4^2 \mid n + 2$?.

7.6.16. Se tiene x número de canicas que se pueden repartir por partes iguales a 4 niños. Del número x se sabe que cuando se repartieron entre 7 niños sobraron 3 y cuando se repartieron ente 10 niños sobraron 6. ¿Cuál es el mínimo valor que puede tomar x?

7.6.17. Cuando los participantes de un desfile se alinearon de 4 en 4 sobraba una persona. Cuando se alinearon de 5 en 5 sobraron dos y cuando se alinearon de 7 en 7 sobraron 3. ¿Cuántos participantes pudo haber habido?

7.6.18. La producción diaria de huevos en una granja es inferior a 75. Cierto día el recolector informa que la cantidad de huevos recogida es tal que contada de tes en tres sobran 2, contados de cinco en cinco sobran 4 y contando de siete en siete sobran 5. El capataz dice que no es posible, ¿quién tiene razón?

7. 6.19. Los hombres de cierto ejército no podían ser divididos en grupos de $2, 3, 4, \ldots,$ o 12, pues en cada caso sobraba un hombre; sin embargo, sí era posible

dividirlos en 13 sin que sobrara ningún hombre. ¿Cuál es el menor número posible de hombres en el ejército?

7.6.20. Una banda de 17 ladrones roba un gran saco de billetes. Tratan de repartir los billetes equitativamente, pero sobran 3 billetes. Dos de los ladrones empiezan a pelear por el sobrante hasta que uno dispara al otro. El dinero se redistribuye, pero esta vez sobran 10 billetes. De nuevo empieza la pelea y otro ladrón resulta muerto. Cuando el dinero se redistribuye, no sobra nada. ¿Cuál es la menor cantidad posible de billetes que los ladrones robaron?

7.6.21. Diga qué hora indica en este momento un reloj de manecillas si:

(1) dentro de 29 horas marcaría las 11 horas y
(2) dentro de 100 horas marcaría las 2 y
(3) hace 50 horas marcaba las 6.

§§ Ejercicios sección 7.7.

7.7.1. Construya la tabla de la suma y el producto para $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_8$ y $\mathbb{Z}_{10}$. ¿En cada caso encuentre los elementos invertibles y los divisores de cero?

7.7.2. Usando las tablas de la suma y del producto en $\mathbb{Z}_5$, encuentre todas las soluciones de las siguientes ecuaciones en $\mathbb{Z}_5$.

(1) $x + \overline{3} = \overline{0}$;
(2) $\overline{2}x = \overline{1}$;
(3) $\overline{4}x = \overline{1}$;
(4) $\overline{3}x + \overline{3} = \overline{1}$;
(5) $x^2 = \overline{3}$;
(6) $x^2 = \overline{-4}$.

7.7.3. Encuentre, si existe, el inverso multiplicativo de

(1) $\overline{7}$ en $\mathbb{Z}_{13}$;
(2) $\overline{7}$ en $\mathbb{Z}_{11}$;
(3) $\overline{53}$ en $\mathbb{Z}_{111}$;
(4) $\overline{299}$ en $\mathbb{Z}_{901}$;
(5) $\overline{51}$ en $\mathbb{Z}_{187}$;
(6) $\overline{41}$ en $\mathbb{Z}_{300}$.

7.7.4. Usando las tablas de la suma y del producto en $\mathbb{Z}_{10}$, encuentre todas las soluciones de las siguientes ecuaciones en $\mathbb{Z}_{10}$.

(1) $x + \overline{7} = \overline{3}$;
(2) $\overline{2}x = \overline{4}$;
(3) $\overline{5}x = \overline{2}$;
(4) $\overline{3}x + \overline{5} = \overline{4}$.
(5) $x^2 = \overline{6}$;
(6) $x^2 = \overline{0}$.

7.7.5. Resolver las siguientes ecuaciones.
(1) $\overline{7}x = \overline{10}$ en $\mathbb{Z}_{13}$;
(2) $\overline{3}x + \overline{2} = \overline{15}$ en $\mathbb{Z}_{13}$;
(3) $\overline{299}x + \overline{20} = \overline{17}$ en $\mathbb{Z}_{901}$.

7.7.6. Sean $\overline{i}, \overline{j} \in \mathbb{Z}_m$, donde $0 \leq i, j < m$, y sea $\overline{i} + \overline{j} = \overline{k}$, con $0 \leq k < m$. Analice cómo se obtiene k a partir de i y j.

7.7.7. ¿Qué propiedad tienen los elementos $\overline{a} \in \mathbb{Z}_9$ que tienen inverso multiplicativo?

7.7.8. Sea $m > 3$ un número compuesto. Demuestre que un elemento $\overline{a}$ de $\mathbb{Z}_m$ es divisor de cero si y sólo si $(a, m) > 1$.

7.7.9. Sea m un número entero con $m > 0$. Demuestre que un elemento de $\mathbb{Z}_m$ es divisor de cero si y sólo si no tiene inverso multiplicativo.

7.7.10. Demostrar que $\mathbb{Z}_m$ es dominio entero si y sólo si $\mathbb{Z}_m$ es campo.

7.7.11. Demostrar que si para alguna ecuación $\overline{a}x = \overline{b}$ en $\mathbb{Z}_m$ tiene más de una solución, esto es, existen $\overline{x}_0, \overline{x}_1 \in \mathbb{Z}_m$, $\overline{x}_0 \neq \overline{x}_1$, que son solución de la ecuación, entonces m es compuesto.

7.7.12. Sea m un número entero con $m > 0$, y sean $\overline{a}, \overline{b} \in \mathbb{Z}_m$. Sea $d = (a, m)$.
(1) Demuestre que si $\overline{b}$ aparece en el renglón de $\overline{a}$ de la tabla del producto, entonces $\overline{b}$ aparece exactamente d veces en el renglón de $\overline{a}$.
(2) Precisamente, ¿qué elementos aparecen en el renglón de $\overline{a}$ en la tabla del producto de $\mathbb{Z}_m$?
(3) ¿Cuántos elementos distintos aparecen en el renglón de $\overline{a}$ en la tabla del producto de $\mathbb{Z}_m$?

7.7.13. Sea m un número entero con $m > 0$. Para $\overline{a}, \overline{b} \in \mathbb{Z}_m$, definimos la operación $\bullet$ como sigue:

$$\overline{a} \bullet \overline{b} = \overline{\text{máx}(a, b)}.$$

Explique por qué la operación $\bullet$ no está bien definida.

7.7.14. Sea m un número entero con $m > 0$, y sea $\overline{a} \in \mathbb{Z}_m$. Decimos que $\overline{a}$ es **par** en $\mathbb{Z}_m$ si a es un número entero par.

(1) Encuentre enteros a y b tales que $\overline{a} = \overline{b}$ en $\mathbb{Z}_9$ donde a es un entero par pero b no lo es. Concluya que el concepto de paridad no está bien definido.

(2) Si m es par, muestre que el concepto de paridad está bien definido en $\mathbb{Z}_m$.

Dios hizo los números naturales.
Los demás son cosa del hombre.
Leopold Kronecker
1823 - 1891

Capítulo **8**

Construcción de los números enteros

§ 8.1. Un modelo de los números enteros

En este capítulo construiremos, con toda formalidad, el conjunto de los números enteros partiendo del conocimiento de los números naturales. En el capítulo 6 se introdujeron los números enteros agregándose al conjunto de los números naturales una copia de ellos, a saber $\{-n \mid n \in \mathbb{N}\}$ y como se vio posteriormente, cuando se introdujo la suma, estos nuevos elemento eran justamente los inversos aditivos de los números naturales. Sin embargo la pregunta que debemos hacernos es ¿cómo podemos justificar la existencia de estos elementos en la teoría de conjuntos? Con tal fin construiremos un conjunto cuyos elementos los identificaremos con los números enteros como fueron introducidos en el capítulo 6. Partiendo de los números naturales, la idea para la construcción de este conjunto es la siguiente: cada pareja ordenada (n, m) de números naturales determina al número natural $n - m$ cuando $n \geq m$, que se definió como el único número natural que satisface $(n - m) + m = n$. En el caso en que $n < m$, entonces $m - n \in \mathbb{N}$ y por lo tanto $-(m - n)$ será un número entero. Sin embargo distintas parejas ordenadas pueden determinar el mismo número entero, por ejemplo, para cada número natural n, $(n + k, n)$ determina al número natural k, puesto que por definición $(n + k) - n = (k + n) - n = k$. Así mismo $(n, n + k)$ determina a $-k$ para cualquier $n \in \mathbb{N}$, esto es $n - (n + k) = -[(n + k) - n] = -k$. Entonces tendríamos que identificar todas las parejas ordenadas que inducen el mismo número natural y también

las parejas ordenadas que inducen $-k$. No es difícil dar esta identificación teniendo en cuenta que si (n, m) y (r, s) determinan el mismo número entero debe ser $n - m = r - s$. Esto es, $n - m = r - s$ implica que $(n - m) + s = (r - s) + s = r$ y sumando m a ambos lados obtenemos $[m + (n - m)] + s = m + r =$, es decir, $n + s = m + r$. Hay que resaltar que esta igualdad se da en $\mathbb{N}$. Estamos ahora en condiciones de construir el conjunto adecuado.
Definimos en el conjunto $\mathbb{N} \times \mathbb{N}$ la siguiente relación

Definición 8.1.1. *Sean* $(n, m), (r, s) \in \mathbb{N} \times \mathbb{N}$. $(n, m) \sim (r, s)$ *si* $n + s = m + r$.

Proposición 8.1.2. *La relación* $\sim$ *definida en* $\mathbb{N} \times \mathbb{N}$ *es de equivalencia.*

Demostración.

(1) $(n, m) \sim (n, m)$ ya que $n + m = m + n$, por la conmutatividad de $+$ en $\mathbb{N}$.
(2) Si $(n, m) \sim (r, s)$, entonces $n + s = m + r$ y por las propiedades de la suma en $\mathbb{N}$, se llega a $r + m = s + n$. Por los tanto $(r, s) \sim (n, m)$.
(3) Si $(n, m) \sim (r, s)$ y $(r, s) \sim (u, v)$, entonces $n + s = m + r$ y $r + v = s + u$. Sumando ambas igualdades $n + s + r + v = m + r + s + u$ y de aquí cancelando $s + r$ obtenemos $n + v = m + u$, que es, $(n, m) \sim (u, v)$. ∎

Observemos que en la demostración de estas propiedades sólo hemos hecho uso de la propiedades de la suma en $\mathbb{N}$.
Veamos ahora cómo son las clases de equivalencia determinadas por esta relación. En cada una de ellas existe un representante muy especial

$$\overline{(m, n)} = \begin{cases} \overline{(m-n,0)} & si\ n \leq m \\ \overline{(0,n-m)} & si\ m < n \end{cases} \tag{1}$$

Esto se puede verificar sin ninguna dificultad recordando que $\overline{(m, n)} = \overline{(r, s)}$ si y sólo si $(m, n) \sim (r, s)$ y de la definición de la diferencia en $\mathbb{N}$.
En particular se tiene que

(1) $\overline{(0, 0)} = \{(n, m) \mid (n, m) \sim (0, 0)\} = \{(n, m) \mid n + 0 = m + 0\} = \{(m, m) \mid m \in \mathbb{N}\}$.
Esto es $\overline{(n, m)} = \overline{(0, 0)}$ si y sólo si $n = m$.

(2) $\overline{(1, 0)} = \{(n, m) \mid (n, m) \sim (1, 0)\} = \{(n, m) \mid n + 0 = m + 1\} = \{(m + 1, m) \mid m \in \mathbb{N}\}$.
Luego $\overline{(n, m)} = \overline{(1, 0)}$ si y sólo si $n = m + 1$.

(3) $\overline{(0, 1)} = \{(n, m) \mid (n, m) \sim (0, 1)\} = \{(n, m) \mid n + 1 = m + 0\} = \{(n, n + 1) \mid n \in \mathbb{N}\}$.
Entonces $\overline{(n, m)} = \overline{(0, 1)}$ si y sólo si $m = n + 1$.

Definición 8.1.3. *Un número entero será una clase de equivalencia* $\overline{(m,n)}$.

Denotaremos por $\mathbb{Z}$ al conjunto de los números enteros, es decir, $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\sim$ y considerando (1) tenemos entonces que

$$\mathbb{Z} = \left\{ \overline{(n,0)} \mid n \in \mathbb{N} \right\} \cup \left\{ \overline{(0,n)} \mid n \in \mathbb{N} \right\}.$$

Así pues la identificación es clara, un número natural n lo identificamos con $\overline{(n,0)}$ y los que corresponden a $-n$ serán los de la forma $\overline{(0,n)}$. Veamos que efectivamente esta identificación es correcta

Proposición 8.1.4. *La función* $i : \mathbb{N} \longrightarrow \mathbb{Z}$ *dada por* $i(n) = \overline{(n,0)}$ *es inyectiva.*

Demostración. Supongamos que $i(n) = i(m)$. Entonces $\overline{(n,0)} = \overline{(m,0)}$ y por lo tanto $n + 0 = 0 + m$, que es, $n = m$. ∎

Definiremos ahora la suma y el producto en $\mathbb{Z}$ y lo haremos de tal manera que estas operaciones sean una extensión de las correspondientes en $\mathbb{N}$, lo que significa que, para cualesquiera $n, m \in \mathbb{N}$,

$$i(n+m) = i(n) + i(m) \quad e \quad i(n \cdot m) = i(n) \cdot i(m).$$

Esto es, el elemento identificado en $\mathbb{Z}$ de la suma (producto) de dos números naturales es el mismo que si primero identificamos cada uno de ellos con sus correspondientes en $\mathbb{Z}$ y ahí realizamos la suma (producto).

Definición 8.1.5. *Sean* $\overline{(m,n)}, \overline{(r,s)} \in \mathbb{Z}$. *Se definen*

$$\overline{(m,n)} + \overline{(r,s)} = \overline{(m+r, n+s)} \ \ (\textit{suma})$$

y

$$\overline{(m,n)} \cdot \overline{(r,s)} = \overline{(m \cdot r + n \cdot s, m \cdot s + n \cdot r)} \ \ (\textit{producto})$$

Descubrir por qué se define la suma y el producto de la manera en que lo hemos hecho no es difícil teniendo en cuenta el objetivo y esto se pide en el ejercicio 8.1.4.

Hemos definido la suma de dos enteros (clases de equivalencia) mediante representantes de cada clase, es decir, la suma (producto) de la clase de (m,n) y la clase de (r,s) será la clase de $(n+r, m+s)$ $((m \cdot r + n \cdot s, m \cdot s + n \cdot r))$ y por lo tanto debemos de verificar que estas operaciones no dependen de la elección que hagamos de éstos.

Teorema 8.1.6. *Si* $\overline{(m,n)} = \overline{(m',n')}$ *y* $\overline{(r,s)} = \overline{(r',s')}$, *entonces*

$$\overline{(m,n)} + \overline{(r,s)} = \overline{(m',n')} + \overline{(r',s')} \quad y \quad \overline{(m,n)} \cdot \overline{(r,s)} = \overline{(m',n')} \cdot \overline{(r',s')}.$$

Demostración. $\overline{(m,n)} = \overline{(m',n')}$ y $\overline{(r,s)} = \overline{(r',s')}$ implican $m + n' = m' + n$ y $r + s' = s + r'$.

Suma: $(m + n') + (r + s') = (n + m') + (s + r')$ y esto es

$$(m + r) + (n' + s') = (n + s) + (m' + r').$$

Entonces $\overline{(m + r, n + s)} = \overline{(m' + r', n' + s')}$ y por lo tanto

$$\overline{(m,n)} + \overline{(r,s)} = \overline{(m',n')} + \overline{(r',s')}.$$

Producto: A partir de las igualdades dadas al principio de la demostración se tiene

$$(m + n') \cdot r + (n + m') \cdot s + (r + s') \cdot m' + (s + r') \cdot n' = (m' + n) \cdot r + (m + n') \cdot s + (s + r') \cdot m' + (r + s') \cdot n'$$

de donde

$$(m \cdot r + n \cdot s + m' \cdot s' + n' \cdot r') + (n' \cdot r + m' \cdot s + m' \cdot r + n' \cdot s) = (m \cdot s + n \cdot r + m' \cdot r' + n' \cdot s') + (n' \cdot r + m' \cdot s + m' \cdot r + n' \cdot s)$$

cancelando se obtiene que

$$(m \cdot r + n \cdot s) + (m' \cdot s' + n' \cdot r') = (m \cdot s + n \cdot r) + (m' \cdot r' + n' \cdot s')$$

Esta última igualdad implica que

$$(m \cdot r + n \cdot s, m \cdot s + n \cdot r) \sim (m' \cdot r' + n' \cdot s', m' \cdot s' + n' \cdot r')$$

o lo que es lo mismo $\overline{(m,n)} \cdot \overline{(r,s)} = \overline{(m',n')} \cdot \overline{(r',s')}$. ∎

Ya habiendo demostrado que la suma y el producto en $\mathbb{Z}$ están bien definidos, demostraremos que $\mathbb{Z}$ con estas operaciones es un anillo en donde los neutros aditivos y multiplicativos serán precisamente los elementos en $\mathbb{Z}$ identificados con los neutros aditivo y multiplicativo, respectivamente, de $\mathbb{N}$.

Teorema 8.1.7. $(\mathbb{Z}, +, \cdot)$ *es una anillo conmutativo.*

Demostración. El neutro aditivo es $\overline{(0,0)}$:

$$\overline{(m,n)} + \overline{(0,0)} = \overline{(m + 0, n + 0)} = \overline{(m,n)}.$$

El inverso aditivo de $\overline{(m,n)}$ es $\overline{(n,m)}$:

$$\overline{(m,n)} + \overline{(n,m)} = \overline{(m + n, n + m)} = \overline{(0,0)}.$$

El neutro multiplicativo es $\overline{(1,0)}$:

$$\overline{(m,n)} \cdot \overline{(1,0)} = \overline{(m \cdot 1 + n \cdot 0, m \cdot 0 + n \cdot 1)} = \overline{(m,n)}.$$

Las restantes propiedades se demuestran sin dificultad pues son consecuencia de las respectivas propiedades de la suma y producto en $\mathbb{N}$. ∎

Mediante la proposición 8.1.4 hemos identificado cada número natural con un número entero: $n \longmapsto i(n) = \overline{(n, 0)}$ y como ya habíamos adelantado, la suma y producto en $\mathbb{Z}$ son extensión de las respectivas operaciones en $\mathbb{Z}$ donde además el neutro aditivo y el idéntico multiplicativo en $\mathbb{Z}$ son precisamente los identificados de los respectivos en $\mathbb{N}$, de tal manera que podemos pensar en $\mathbb{N}$ como un "subconjunto" de $\mathbb{Z}$.

Proposición 8.1.8.
(1) $i(0) = \overline{(0, 0)}$.
(2) $i(1) = \overline{(1, 0)}$.
(3) $i(m + n) = i(m) + i(n)$.
(4) $i(m \cdot n) = i(m) \cdot i(n)$.

Demostración.
(3) $i(m + n) = \overline{(m + n, 0)} = \overline{(m, 0)} + \overline{(n, 0)} = i(m) + i(n)$.
(4) $i(m \cdot n) = \overline{(m \cdot n, 0)} = \overline{(m, 0)} \cdot \overline{(n, 0)} = i(m) \cdot i(n)$. ∎

Hemos ya mencionado que en la clase de cada número entero $\overline{(m, n)}$ existe un representante muy especial, a saber $\overline{(m - n, 0)}$ si $n \leq m$ o $\overline{(0, n - m)}$ si $m < n$, con lo cual tenemos entonces que

$$\mathbb{Z} = \left\{ \overline{(n, 0)} \mid n \in \mathbb{N} \right\} \cup \left\{ \overline{(0, n)} \mid n \in \mathbb{N} \right\}.$$

Por obvias razones y abusando un poco de la notación a cada entero de la forma $\overline{(n, 0)}$ lo denotaremos simplemente por n y a cada entero de la forma $\overline{(0, n)}$ por $-n$. Esto último tiene sentido ya que hemos visto que $\overline{(0, n)}$ es el inverso aditivo de $\overline{(n, 0)}$, así que con esta nueva notación tenemos que $n + (-n) = 0$. Por último considerando la manera en que se introdujeron los enteros en el capítulo 6, sólo quedaría comprobar que la suma y producto ahí definidos coincide con los correspondientes que hemos dado aquí. No es difícil hacerlo así que lo dejamos como ejercicio.

Teorema 8.1.9. $(\mathbb{Z}, +, \cdot)$ *es un dominio entero.*

Demostración. Ya hemos visto que $\mathbb{Z}$ es una anillo conmutativo, por lo que sólo falta ver que no tiene divisores de cero.
Supongamos que $\overline{(m, n)} \cdot \overline{(r, s)} = \overline{(0, 0)}$ y que $\overline{(r, s)} \neq \overline{(0, 0)}$. Entonces $s < r$ o $r < s$.

$1^o/\ s < r$.

En este caso $\overline{(r,s)} = \overline{(r-s,0)}$ y

$$\overline{(m,n)} \cdot \overline{(r,s)} = \overline{(m,n)} \cdot \overline{(r-s,0)} = \overline{(m(r-s), n(r-s))} = \left(\overline{0,0}\right)$$

Esto último implica que $m(r-s) = n(r-s)$ donde $m, n, r-s \in \mathbb{N}$ y $r-s \neq 0$. Por lo tanto, cancelando $(r-s)$, obtenemos $m = n$, así que

$$\overline{(m,n)} = \overline{(m,m)} = \overline{(0,0)}\,.$$

$2^o/\ r < s$.

Aquí $\overline{(r,s)} = \overline{(0,s-r)}$ y

$$\overline{(m,n)} \cdot \overline{(r,s)} = \overline{(m,n)} \cdot \overline{(0,s-r)} = \overline{(n(s-r), m(s-r))} = \overline{(0,0)}.$$

Entonces $n(s-r) = m(s-r)$ y por lo tanto $m = n$, lo que significa que $\overline{(m,n)} \cdot \overline{(0,0)}$. ∎

Definición 8.1.10. *Para cualesquiera enteros m y n, $m - n = m + (-n)$. Esto es, $m - n$ será el entero que resulta de sumarle a m el inverso aditivo de n.*

Observación 8.1.11. Usando esta última definición, tenemos entonces que $\overline{(m,n)} = m - n$ y se tiene que $\overline{(m,n)} = \overline{(r,s)}$ si y sólo si $m - n = r - s$ (esta última igualdad es equivalente a $m + s = n + r$). En cuanto al orden que se definió en $\mathbb{Z}$ y que resulta ser una extensión del orden en $\mathbb{N}$, éste se define

Definición 8.1.12. $\overline{(m,n)} \leq \overline{(r,s)}$ *si* $\overline{(m,n)} + \overline{(a,0)} = \overline{(r,s)}$ *para algún* $a \in \mathbb{N}$.

Es evidente que esta definición coincide con la que se dio en el capítulo 6, puesto que

$$\overline{(m,n)} + \overline{(a,0)} = \overline{(r,s)} \iff \overline{(m+a,n)} = \overline{(r,s)} \iff (m+a) + s = n + r$$

y esto último visto como una igualdad en $\mathbb{Z}$, es equivalente a $(m-n) + a = r - s$. Entonces, no es necesario repetir lo que se hizo en el capítulo 6 sobre el orden. Todo permanece igual.

§8.2. Ejercicios del capítulo 8

8.1.1. [1] Demuestre la propiedades que no se demuestran en el Teorema 8.1.7, es decir:

(1) $i(0) = \overline{(0,0)}$.

[1] Parte del Teorema 8.1.7 pág. 328.

(2) $i(1) = \overline{(1,0)}$.

8. 1.2. Verifique que efectivamente $\overline{(m,n)} = \overline{(m-n,0)}$ si $n \leq m$ y $\overline{(m,n)} = \overline{(0,n-m)}$ si $m < n$. Justifique su respuesta.

8.1.3. Demuestre que

(1) $\overline{(n,m)} = \overline{(k,0)}$ si y sólo si $n = m + k$.
(2) $\overline{(n,m)} = \overline{(0,k)}$ si y sólo si $m = n + k$.

8.1.4. Demuestre que la suma y producto en $\mathbb{Z}$ definidos en el capítulo 6 coinciden con los correspondientes dadas en este capítulo.

Los números gobiernan el mundo.
Pitágoras
580 a. C. - 495 a. C.

Capítulo **9**

Los números racionales

En los números naturales, ecuaciones del tipo $a + x = b$ no necesariamente tiene solución. Más concretamente tendrá solución en $\mathbb{N}$ si y sólo si $a \leq b$ y en este caso la solución es $b - a$. (véase 2.1.9) Al construir los enteros, cualquier ecuación del tipo mencionado siempre tendrá solución ya que $b - a$ esta definido para cualesquiera enteros a y b. Sin embargo ecuaciones de la forma $bx = a$ no siempre tiene solución en los enteros. Esta ecuación tiene solución en $\mathbb{Z}$ si y sólo si $b \mid a$ y en este caso la solución es única si $b \neq 0$. Justamente en la nota 7.1.8 de la página 246 denotamos por $\frac{a}{b}$ a este único entero c tal que $b \cdot c = a$. En este capítulo introducimos los números racionales, los cuales contendrán una copia de los números enteros y en donde se definirá una suma y un producto que serán extensiones respectivamente de la suma y producto en los enteros y donde ecuaciones del tipo $r \cdot x = s$, con r y s números racionales siempre tendrán una única solución si $r \neq 0$. Así mismo extenderemos el orden de los enteros a un orden en los racionales, es decir definiremos un orden en $\mathbb{Q}$ tal que para enteros a y b, a es menor que b en $\mathbb{Q}$ si y sólo si a es menor que b en $\mathbb{Z}$. La idea es considerar expresiones del tipo $\frac{a}{b}$, donde a y b son números enteros con $b \neq 0$ y donde identificamos a $\frac{a}{b}$ con el entero c en el caso en que $b \cdot c = a$ en $\mathbb{Z}$. Sin embargo distintas parejas a, b y a', b' pueden ser identificadas con el mismo entero, como lo muestran los siguientes ejemplos: 3 es solución de $4x = 12$ y de $7x = 21$ y de acuerdo a nuestra notación tenemos entonces que $3 = \frac{12}{4} = \frac{21}{7}$, lo que significaría que el mismo entero estaría identificado mediante distintas expresiones $\frac{a}{b}$. Pero veamos qué relación hay entre

dos expresiones distintas $\frac{a}{b}, \frac{a'}{b'}$, identificadas con el mismo entero. En el siguiente análisis b y b' serán enteros distintos de cero.
Supongamos que el entero x_0 es solución de

$$b \cdot x_0 = a \ \ y \ \ b' \cdot x_0 = a'.$$

Con la notación dada anteriormente estamos suponiendo que $\frac{a}{b} = \frac{a'}{b'}$ Multiplicando la primera ecuación por b' y la segunda por b, obtenemos

$$(b' \cdot b) \cdot x_0 = b' \cdot a \ \ y \ \ (b \cdot b') \cdot x_0 = b \cdot a'.$$

lo que implica que debe ser $b' \cdot a = b \cdot a'$.
Inversamente si $b' \cdot a = b \cdot a'$ y x_0 y x_1 son enteros tales que $b \cdot x_0 = a$ y $b' \cdot x_1 = a'$, entonces $(b' \cdot b) \cdot x_0 = b' \cdot a$ y $(b \cdot b') \cdot x_1 = b \cdot a'$ y por lo tanto $(b' \cdot b) \cdot x_0 = (b \cdot b') \cdot x_1$, que por ser $b \cdot b' \neq 0$, se tiene que $x_0 = x_1$, lo que implica, según nuestra notación, que $\frac{a}{b} = \frac{a'}{b'}$.

§ 9.1. Construcción de los números racionales

Definición 9.1.1. *El conjunto de los,**números racionales** denotado por $\mathbb{Q}$, es*

$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z} \, y \, b \neq 0 \right\}$$

donde $\frac{a}{b} = \frac{a'}{b'}$ si y sólo si $a \cdot b' = a' \cdot b$ en $\mathbb{Z}$.

De acuerdo a la definición dada, un número racional tiene muchas representaciones, por ejemplo, otras representaciones de $\frac{a}{b}$ son $\frac{r \cdot a}{r \cdot b}$ para cada número entero $r \neq 0$, ya que $a \cdot (r \cdot b) = (r \cdot a) \cdot b$.
Dado un número racional $\frac{a}{b}$, a se llama el **numerador** y b se llama el **denominador**.
Hagamos ahora la identificación de los números enteros como números racionales, y para esto escogemos, para cada entero n, una representación muy especial en $\mathbb{Q}$. Teniendo en cuenta que cada entero n es solución de la ecuación $1 \cdot x = n$, identificaremos al entero n con el número racional $\frac{n}{1}$. Por supuesto, si n también es solución de una ecuación $b \cdot x = a$, como ya se ha discutido al inicio de esta sección, se debe tener $\frac{n}{1} = \frac{a}{b}$. Lo importante aquí es verificar que si dos enteros son distintos, entonces estos dos enteros vistos en $\mathbb{Q}$ también son distintos, esto es,

Proposición 9.1.2. *La función $i : \mathbb{Z} \longrightarrow \mathbb{Q}$ dada por $i(n) = \frac{n}{1}$ es inyectiva.*

Demostración. Si $i(n) = i(m)$, entonces $\frac{n}{1} = \frac{m}{1}$ y por lo tanto $1 \cdot n = m \cdot 1$, que es, $n = m$. ∎

Para definir la suma y el producto de racionales tal que extienda a las correspondientes operaciones en $\mathbb{Z}$, debemos hacerlo de tal manera que $\frac{n}{1} + \frac{m}{1} = \frac{n+m}{1}$ para el caso de la suma y que $\frac{n}{1} \cdot \frac{m}{1} = \frac{n \cdot m}{1}$ para el caso del producto. Antes de introducir estas operaciones en $\mathbb{Q}$ tomemos en cuenta las siguientes consideraciones con el afán de tener una idea de cómo definirlos.

Para la suma:

(A) Las representaciones en $\mathbb{Q}$ de $\frac{n}{1}$ son exactamente las de la forma $\frac{b \cdot n}{b}$ para cualquier entero $b \neq 0$, ya que $\frac{n}{1} = \frac{a}{b}$ si y sólo si $a = b \cdot n$.

(B) Si queremos definir la suma en $\mathbb{Q}$ tal que $\frac{n}{1} + \frac{m}{1} = \frac{n+m}{1}$, como $\frac{n}{1} = \frac{b \cdot n}{b}$ y $\frac{m}{1} = \frac{b' \cdot m}{b'}$ para cualesquiera enteros b y b' distintos de cero, se debe tener entonces que $\frac{n+m}{1} = \frac{b \cdot n}{b} + \frac{b' \cdot n}{b'}$ y como $\frac{b \cdot n}{b} = \frac{b \cdot b' \cdot n}{b \cdot b'}$ y $\frac{b' \cdot m}{b'} = \frac{b \cdot b' \cdot m}{b \cdot b'}$, entonces debe ser $\frac{n+m}{1} = \frac{b \cdot b' \cdot n}{b \cdot b'} + \frac{b \cdot b' \cdot m}{b \cdot b'}$ y ya que $\frac{n+m}{1} = \frac{b \cdot b' \cdot (n+m)}{b \cdot b'}$, por lo tanto

$$\frac{b \cdot b' \cdot n}{b \cdot b'} + \frac{b \cdot b' \cdot m}{b \cdot b'} = \frac{b \cdot b' \cdot (n+m)}{b \cdot b'} = \frac{b \cdot b' \cdot n + b \cdot b' \cdot m}{b \cdot b'}$$

(1) Para cualesquiera números racionales $\frac{a}{b}$ y $\frac{a'}{b'}$, se tiene que $\frac{a \cdot b'}{b \cdot b'} = \frac{a}{b}$ y $\frac{b \cdot a'}{b \cdot b'} = \frac{a'}{b'}$, lo que significa que dados dos números racionales cualesquiera, podemos encontrar representaciones de ambos con la propiedad de que tengan el mismo denominador. Entonces la suma en $\mathbb{Q}$ debe satisfacer que

$$\frac{a}{b} + \frac{a'}{b'} = \frac{a \cdot b'}{b \cdot b'} + \frac{b \cdot a'}{b \cdot b'} = \frac{a \cdot b' + b \cdot a'}{b \cdot b'}$$

Para el producto:

En el caso del producto, su definición debe satisfacer, $\frac{n}{1} \cdot \frac{m}{1} = \frac{n \cdot m}{1}$ y como se hizo para el caso de la suma, $\frac{n \cdot m}{1} = \frac{b \cdot n}{b} \cdot \frac{b' \cdot m}{b'}$ y como $\frac{n}{1} \cdot \frac{m}{1} = \frac{(b \cdot b') \cdot n \cdot m}{b \cdot b'}$, entonces debe ser

$$\frac{b \cdot n}{b} \cdot \frac{b' \cdot m}{b'} = \frac{(b \cdot b') \cdot n \cdot m}{b \cdot b'} = \frac{(b \cdot n) \cdot (b' \cdot m)}{b \cdot b'}.$$

Esto es, el producto de $\frac{b \cdot n}{b}$ y $\frac{b' \cdot m}{b'}$ debe ser el número racional cuyo numerador es el producto de los numeradores y denominador el producto de los denominadores.

Definición 9.1.3. *Sean $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$. La suma y producto de $\frac{a}{b}$ y $\frac{c}{d}$ son respectivamente*

$$\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + b \cdot c}{b \cdot d}$$

y

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}.$$

Como cada número racional tiene muchas representaciones deberíamos demostrar que la suma y el producto que hemos definido no depende de la elección de los representantes. Sin embargo, debido a que en el capítulo 10 construiremos formalmente los números racionales (en el sentido de exhibir un conjunto concretamente) sólo enunciaremos este resultado remitiendo su demostración al siguiente capítulo. (véase teorema 10.1.3)
En particular, $\frac{a}{b} + \frac{c}{b} = \frac{a \cdot b + c \cdot b}{b^2} = \frac{(a+c)b}{b^2} = \frac{a+c}{b}$.

Proposición 9.1.4. *La suma y el producto definidos en $\mathbb{Q}$ no dependen de la elección de los representantes, es decir, si $\frac{a}{b} = \frac{a'}{b'}$ y $\frac{c}{d} = \frac{c'}{d'}$, entonces*

$$\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'} \ \ y \ \ \frac{a}{b} \cdot \frac{c}{d} = \frac{a'}{b'} \cdot \frac{c'}{d'}.$$

El siguiente resultado muestra que efectivamente la suma y producto definidos en $\mathbb{Q}$ son una extensión de la suma y producto en $\mathbb{Z}$.

Proposición 9.1.5. *La función $i : \mathbb{Z} \longrightarrow \mathbb{Q}$ definida por $i(a) = \frac{a}{1}$ satisface:*

(1) $i(a + b) = i(a) + i(b)$.
(2) $i(a \cdot b) = i(a) \cdot i(b)$.

Demostración.

(1) $i(a) + i(b) = \frac{a}{1} + \frac{b}{1} = \frac{1 \cdot a + 1 \cdot b}{1} = \frac{a+b}{1} = i(a + b)$.
(2) $i(a) \cdot i(b) = \frac{a}{1} \cdot \frac{b}{1} = \frac{a \cdot b}{1 \cdot 1} = \frac{a \cdot b}{1} = i(a \cdot b)$. ∎

De aquí en adelante al número racional $\frac{a}{1}$, que es el identificado en $\mathbb{Q}$ del número entero a lo denotaremos por a.
En la siguiente proposición presentamos algunas propiedades de los números racionales en cuanto a sus distintas representaciones.

Proposición 9.1.6. *Sea $\frac{a}{b} \in \mathbb{Q}$.*

(1) $\frac{a}{b} = \frac{0}{1}$ *si y sólo si* $a = 0$. *Entonces* $\frac{0}{1} = \frac{0}{b}$ *para todo* $b \in \mathbb{Z} - \{0\}$.
(2) $\frac{a}{b} = \frac{m \cdot a}{m \cdot b}$ *para todo* $m \in \mathbb{Z} - \{0\}$.
(3) Existen enteros a' *y* b' *tales que* $(a', b') = 1$ *y* $\frac{a}{b} = \frac{a'}{b'}$.
(4) Si $\frac{c}{d} \in \mathbb{Q}$ *y* $(c, d) = 1$, *entonces* $\frac{a}{b} = \frac{c}{d}$ *si y sólo si* $a = m \cdot c$ *y* $b = m \cdot d$ *para algún entero* m.

(5) Si $(a, b) = 1$, $(c, d) = 1$ *y* a, b, c, d *enteros positivos, entonces* $\frac{a}{b} = \frac{c}{d}$ *si y sólo si* $a = c$ *y* $b = d$.
(6) Existe $\frac{c}{d} \in \mathbb{Q}$ *con* $d > 0$ *tal que* $\frac{a}{b} = \frac{c}{d}$.

Demostración.
(1) $\frac{a}{b} = \frac{0}{1}$ si y sólo si $a \cdot 1 = b \cdot 0$.
(2) Es inmediato de la definición.
(3) Sea $d = (a, b)$. Entonces $a = d \cdot a'$ y $b = d \cdot b'$ (en el caso $a = 0$, $(a, b) =\mid b \mid$, $a' = 0$ y $b' = -1$ según sea el caso) donde $(a', b') = 1$ por el corolario 7.2.12. Aplicando (2) tenemos que $\frac{a}{b} = \frac{d \cdot a'}{d \cdot b'} = \frac{a'}{b'}$.
(4) $\frac{a}{b} = \frac{c}{d}$ implica $a \cdot d = b \cdot c$ y como $(c, d) = 1$, por el teorema 7.2.16, $d \mid b$ y $c \mid a$. Entonces existen enteros m y n tales que $d \cdot m = b$ y $c \cdot n = a$. Sustituyendo en la igualdad $a \cdot d = b \cdot c$, obtenemos $c \cdot n \cdot d = d \cdot m \cdot c$ y ya que $c \cdot d \neq 0$, entonces $m = n$ y así $a = c \cdot m$ y $b = d \cdot m$ para algún entero $m \neq 0$. El recíproco se obtiene del inciso (2).
(5) Por el inciso (4), por ser $(a, b) = 1$ se tiene que $c = m \cdot a$ y $d = m \cdot b$ para algún entero $m > 0$ y debido a que también $(c, d) = 1$, entonces

$$1 = (c, d) = (m \cdot a, m \cdot b) = |m|(a, b) = |m|$$

Y por ser m positivo, se debe tener $m = 1$ y así $a = c$ y $b = d$.
El recíproco es inmediato.
(6) Si $b > 0$, entonces el mismo $\frac{a}{b}$ satisface la condición. En el caso en que $b < 0$, entonces $-b > 0$ y $\frac{a}{b} = \frac{(-1) \cdot a}{(-1) \cdot b} = \frac{-a}{-b}$. ∎

Así como la suma en $\mathbb{Z}$ no sólo satisface las mismas propiedades que la suma en $\mathbb{N}$, sino que tiene una propiedad adicional que es la existencia del inverso aditivo para cada número entero, el producto definido en $\mathbb{Q}$ satisface también una propiedad, que no la tiene el producto en $\mathbb{Z}$, que es la existencia del inverso multiplicativo de cada número racional distinto de cero. Las propiedades de la suma y producto en $\mathbb{Q}$ son:

Teorema 9.1.7. *Sean* $\frac{a}{b}$, $\frac{c}{d}$ *y* $\frac{e}{f}$ *números racionales arbitrarios. Entonces*

(1) $\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right)$
(2) $\frac{a}{b} + \frac{c}{d} = \frac{c}{d} + \frac{a}{b}$
(3) $\frac{a}{b} + 0 = \frac{a}{b}$
(4) Existe $\frac{a'}{b'} \in \mathbb{Q}$ *tal que* $\frac{a}{b} + \frac{a'}{b'} = 0$
(5) $\left(\frac{a}{b} \cdot \frac{c}{d}\right) \cdot \frac{e}{f} = \frac{a}{b} \cdot \left(\frac{c}{d} \cdot \frac{e}{f}\right)$

(6) $\frac{a}{b} \cdot \frac{c}{d} = \frac{c}{d} \cdot \frac{a}{b}$
(7) $\frac{a}{b} \cdot 1 = \frac{a}{b}$
(8) Si $\frac{a}{b} \neq 0$, *entonces existe* $\frac{k}{l} \in \mathbb{Q}$ *tal que* $\frac{a}{b} \cdot \frac{k}{l} = 1$
(9) $\frac{a}{b}\left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{e}{f}$

Demostración. Sean $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbb{Q}$.

(1) $\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{a\cdot d+b\cdot c}{b\cdot d} + \frac{e}{f} = \frac{(a\cdot d+b\cdot c)\cdot f+b\cdot d\cdot e}{b\cdot d\cdot f}$
$= \frac{a\cdot d\cdot f+b\cdot c\cdot f+b\cdot d\cdot e}{b\cdot d\cdot f} = \frac{a\cdot d\cdot f+(c\cdot f+e\cdot d)\cdot b}{b\cdot d\cdot f}$
$= \frac{a}{b} + \frac{c\cdot f+e\cdot d}{d\cdot f} = \frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right)$.
(2) $\frac{a}{b} + \frac{c}{d} = \frac{a\cdot d+b\cdot c}{b\cdot d} = \frac{b\cdot c+a\cdot d}{d\cdot b} = \frac{c}{d} + \frac{a}{b}$.
(3) $\frac{a}{b} + 0 = \frac{a}{b} + \frac{0}{1} = \frac{1\cdot a+b\cdot 0}{b\cdot 1} = \frac{a}{b}$.
(4) Sea $\frac{a'}{b'} = \frac{-a}{b}$. Entonces $\frac{a}{b} + \frac{a'}{b'} = \frac{a}{b} + \frac{-a}{b} = \frac{b\cdot a-b\cdot a}{b^2} = \frac{0}{b^2} = 0$.
(5) $\left(\frac{a}{b} \cdot \frac{c}{d}\right) \cdot \frac{e}{f} = \frac{a\cdot c}{b\cdot d} \cdot \frac{e}{f} = \frac{(a\cdot c)\cdot e}{(b\cdot d)\cdot f} = \frac{a\cdot(c\cdot e)}{b\cdot(d\cdot f)} = \frac{a}{b} \cdot \frac{c\cdot e}{d\cdot f} = \frac{a}{b} \cdot \left(\frac{c}{d} \cdot \frac{e}{f}\right)$.
(6) $\frac{a}{b} \cdot \frac{c}{d} = \frac{a\cdot c}{b\cdot d} = \frac{c\cdot a}{d\cdot b} = \frac{c}{d} \cdot \frac{a}{b}$.
(7) $= \frac{a}{b} \cdot 1 = \frac{a}{b} \cdot \frac{1}{1} = \frac{a\cdot 1}{a\cdot 1} = \frac{a}{b}$.
(8) $\frac{a}{b} \neq \frac{0}{1}$ implica que $a \neq 0$ (proposición 9.1.6 (1)). Entonces

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{a \cdot b}{b \cdot a} = \frac{(a \cdot b) \cdot 1}{(a \cdot b) \cdot 1} = \frac{1}{1} = 1.$$

(9) $\frac{a}{b} \cdot \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} \cdot \frac{c\cdot f+d\cdot e}{d\cdot f} = \frac{a(c\cdot f+d\cdot e)}{b\cdot d\cdot f}$
$= \frac{a\cdot c\cdot f+a\cdot d\cdot e}{b\cdot d\cdot f} = \frac{a\cdot c\cdot f}{b\cdot d\cdot f} + \frac{a\cdot d\cdot e}{b\cdot d\cdot f}$
$= \frac{a\cdot c}{b\cdot d} + \frac{a\cdot e}{b\cdot f} = \frac{a}{b} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{e}{f}$. ∎

Con esto hemos demostrado que $(\mathbb{Q}, +, \cdot, 0, 1)$ es un campo.
Al inverso aditivo de un número racional $\frac{a}{b}$ lo denotamos por $-\frac{a}{b}$ y la diferencia de dos números racionales $\frac{a}{b}$, $\frac{c}{d}$ la definimos por $\frac{a}{b} - \frac{c}{b} = \frac{a}{b} + \left(-\frac{c}{d}\right)$.

§ 9.2. Orden en los números racionales

Nuestro objetivo ahora es definir un orden en $\mathbb{Q}$ de tal manera que extienda al orden en $\mathbb{Z}$. Esto es , deseamos definir un orden $<$ tal que para cualquiera entero a y b, $a < b$ en $\mathbb{Z}$ si y sólo si $\frac{a}{1} < \frac{b}{1}$ en $\mathbb{Q}$. Recordemos que el orden en $\mathbb{Z}$ fue definido a través de $\mathbb{N}$, esto es, para enteros a y b, $a < b$ en $\mathbb{Z}$ si $b-a \in \mathbb{N}-\{0\}$, lo que da lugar a que los enteros mayores que cero son exactamente aquellos que pertenecen a $\mathbb{N} - \{0\}$. Siguiendo esta idea, definiremos el orden de $\mathbb{Q}$

utilizando un subconjunto de $\mathbb{Q}$ dado de antemano y al cual denotaremos por $\mathbb{Q}^+$ y como consecuencia de esta definición los elementos de este conjunto $\mathbb{Q}^+$ serán precisamente aquellos números racionales mayores que cero. Antes de introducir al conjunto $\mathbb{Q}^+$ necesitamos el siguiente

Lema 9.2.1. *Si $\frac{a}{b} = \frac{a'}{b'}$ en $\mathbb{Q}$, entonces $a \cdot b > 0$ si y sólo si $a' \cdot b' > 0$.*

Demostración. Si $\frac{a}{b} = \frac{a'}{b'}$, en $\mathbb{Q}$, entonces $a \cdot b' = a' \cdot b$. Multiplicando por $b \cdot b'$ obtenemos $(a \cdot b) \cdot (b')^2 = (a' \cdot b') \cdot b^2$ y por ser $(b')^2$ y b^2 ambos mayores que cero, por el ejercicio 6.3.4 (11) concluimos que $a \cdot b > 0$ si y sólo si $a' \cdot b' > 0$. ∎

Estamos ahora en condiciones de introducir el conjunto $\mathbb{Q}^+$ para, a partir de éste, definir el orden en $\mathbb{Q}$.
Denotaremos por $\mathbb{Q}^+$ al conjunto $\mathbb{Q}^+ = \left\{ \frac{a}{b} \mid a \cdot b > 0 \right\}$.
Por el lema 9.2.1, este conjunto $\mathbb{Q}^+$ está bien definido ya que no importa la representación que se toma de un número racional que pertenece a él, la propiedad que determina a estos elementos se sigue cumpliendo.
El conjunto $\mathbb{Q}^+$ tiene dos propiedades muy importantes que son la de ser *cerrado* bajo suma y cerrado bajo producto, lo que significa que la suma y producto de elementos de $\mathbb{Q}^+$ pertenecen a $\mathbb{Q}^+$. La cerradura respecto a la suma es la que nos permitirá demostrar que la relación que definiremos en $\mathbb{Q}$ es un orden parcial.

Proposición 9.2.2. *El conjunto $\mathbb{Q}^+$ tiene las siguientes propiedades*

(1) Si $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}^+$, entonces $\frac{a}{b} + \frac{c}{d} \in \mathbb{Q}^+$.
(2) Si $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}^+$, entonces $\frac{a}{b} \cdot \frac{c}{d} \in \mathbb{Q}^+$.
(3) Dado cualquier entero a, $\frac{a}{1} \in \mathbb{Q}^+$ si y sólo si $a > 0$ en $\mathbb{Z}$.

Demostración. Sean $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}^+$. Entonces $a \cdot b > 0$ y $c \cdot d > 0$.

(1) $\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + b \cdot c}{b \cdot d}$ y $(a \cdot d + b \cdot c) \cdot b \cdot d = (a \cdot b) \cdot d^2 + (c \cdot d) \cdot b^2 > 0$ debido a la proposición 6.3.6 incisos (3) y (5) y al hecho de que $a \cdot b$, $c \cdot d$, b^2 y d^2 son todos mayores a cero.
(2) $\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$ y $(a \cdot c)(b \cdot d) = (a \cdot b)(c \cdot d) > 0$ por la proposición 6.3.6 (4) y la hipótesis.
(3) Es inmediato de la definición de $\mathbb{Q}^+$. ∎

Definición 9.2.3. *Sean $\frac{a}{b}, \frac{c}{d} \in Q$. Diremos que $\frac{a}{b} < \frac{c}{d}$ si $\frac{c}{d} - \frac{a}{b} \in \mathbb{Q}^+$.*

Nota 9.2.4. Lo primero que tendríamos que hacer es demostrar que la relación $<$ dada en la definición 9.2.3 no depende de los representantes. Sin embargo esto no es necesario ¿por qué?. (ejercicio 9.2.2).

Teorema 9.2.5. *La relación $<$ definida en $\mathbb{Q}$ es un orden parcial.*

Demostración.

(1) $\frac{a}{b} \not< \frac{a}{b}$ ya que $\frac{a}{b} - \frac{a}{b} = \frac{0}{b} \notin \mathbb{Q}^+$.
(2) Si $\frac{a}{b} < \frac{c}{d}$ y $\frac{c}{d} < \frac{e}{f}$, entonces $\frac{c}{d} - \frac{a}{b} \in \mathbb{Q}^+$ y $\frac{e}{f} - \frac{c}{d} \in \mathbb{Q}^+$ y por (1) de la proposición 9.2.2, $\left(\frac{c}{d} - \frac{a}{b}\right) + \left(\frac{e}{f} - \frac{c}{d}\right) = \frac{e}{f} - \frac{a}{b} \in \mathbb{Q}^+$. Por lo tanto $\frac{a}{b} < \frac{e}{f}$. ∎

La propiedad de $<$ en $\mathbb{Z}$ de ser un orden total permanece en $\mathbb{Q}$.

Teorema 9.2.6. *El orden en $\mathbb{Q}$ es total.*

Demostración. Sean $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ tales que $\frac{a}{b} \neq \frac{c}{d}$. Entonces $\frac{a}{b} - \frac{c}{d} = \frac{a \cdot d - b \cdot c}{b \cdot d} \neq 0$ y esto implica que $a \cdot d - b \cdot c \neq 0$. Ahora, como $<$ es un orden total en $\mathbb{Z}$, $b \cdot d \cdot (a \cdot d - b \cdot c) < 0$ o $b \cdot d \cdot (a \cdot d - b \cdot c) > 0$ o lo que es lo mismo $b \cdot d \cdot (b \cdot c - a \cdot d) > 0$ o $b \cdot d \cdot (a \cdot d - b \cdot c) > 0$ y de aquí concluimos que $\frac{c}{d} < \frac{a}{b}$ o $\frac{a}{b} < \frac{c}{d}$. ∎

Veamos ahora que el orden definido en $\mathbb{Q}$ efectivamente extiende el orden de $\mathbb{Z}$.

Teorema 9.2.7. *Sean $a, b \in \mathbb{Z}$, $a < b$ en $\mathbb{Z}$ si y sólo si $\frac{a}{1} < \frac{b}{1}$ en $\mathbb{Q}$.*

Demostración. El resultado se obtiene de las equivalencias siguientes

$$\frac{a}{1} < \frac{b}{1} \text{ si y sólo si } \frac{b}{1} - \frac{a}{1} = \frac{b-a}{1} \in \mathbb{Q}^+$$
$$\frac{b-a}{1} \in \mathbb{Q}^+ \text{ si y sólo si } (b-a) \cdot 1 > 0$$
$$(b-a) \cdot 1 > 0 \text{ si y sólo si } a < b \text{ en } \mathbb{Z}.$$ ∎

Nota 9.2.8. Cabe hacer notar que el conjunto $\mathbb{Q}^+$ que utilizamos para definir el orden en $\mathbb{Q}$ resulta ser precisamente el conjunto de los números racionales mayores que cero: $0 < \frac{a}{b}$ si y sólo si $\frac{a}{b} - 0 = \frac{a}{b} \in \mathbb{Q}^+$.

El orden en $\mathbb{Q}$ tiene las siguientes propiedades

Teorema 9.2.9. *Sean $\frac{a}{b}, \frac{c}{d}, \frac{e}{f}, \frac{g}{h} \in \mathbb{Q}$. Entonces*

(1) $\frac{a}{b} < \frac{c}{d}$ *implica* $\frac{a}{b} + \frac{e}{f} < \frac{c}{d} + \frac{e}{f}$
(2) $\frac{a}{b} < \frac{c}{d}$ *y* $\frac{e}{f} < \frac{g}{h}$ *implica* $\frac{a}{b} + \frac{e}{f} < \frac{c}{d} + \frac{g}{h}$.
(3) $\frac{a}{b} < \frac{c}{d}$ *y* $0 < \frac{e}{f}$ *implica* $\frac{a}{b} \cdot \frac{e}{f} < \frac{c}{d} \cdot \frac{e}{f}$
(4) $0 < \frac{a}{b} < \frac{c}{d}$ *y* $0 < \frac{e}{f} < \frac{g}{h}$ *implica* $0 < \frac{a}{b} \cdot \frac{e}{f} < \frac{c}{d} \cdot \frac{g}{h}$.

(5) $\frac{a}{b} \neq 0$ *implica* $0 < \left(\frac{a}{b}\right)^2$.
(6) $0 < \frac{a}{b}$ *si y sólo si* $0 < \frac{b}{a}$.
(7) $0 < \frac{a}{b} < \frac{c}{d}$ *si y sólo si* $0 < \frac{d}{c} < \frac{b}{a}$.
(8) $1 < \frac{a}{b}$ *y* $m < n$ $(m, n \in \mathbb{Z})$ *implican* $\left(\frac{a}{b}\right)^m < \left(\frac{a}{b}\right)^n$.
(9) $0 < \frac{a}{b} < 1$ *y* $m < n$ $(m, n \in \mathbb{Z})$ *implican* $\left(\frac{a}{b}\right)^n < \left(\frac{a}{b}\right)^m$.

Demostración. Sean $\frac{a}{b}, \frac{c}{d}, \frac{e}{f}, \frac{g}{h} \in \mathbb{Q}$.

(1) Como $\frac{c}{d} - \frac{a}{b} \in \mathbb{Q}^+$ por hipótesis y $\left(\frac{c}{d} + \frac{e}{f}\right) - \left(\frac{a}{b} + \frac{e}{f}\right) = \frac{c}{d} - \frac{a}{b}$, entonces $\frac{a}{b} + \frac{e}{f} < \frac{c}{d} + \frac{e}{f}$.
(2) Por hipótesis $\frac{c}{d} - \frac{a}{b} \in Q$ y $\frac{g}{h} - \frac{e}{f} \in Q$ y por (1) de la proposición 9.2.2

$$\left(\frac{c}{d} - \frac{a}{b}\right) + \left(\frac{g}{h} - \frac{e}{f}\right) = \left(\frac{c}{d} + \frac{g}{h}\right) - \left(\frac{a}{b} + \frac{e}{f}\right) \in \mathbb{Q}.$$

Por lo tanto $\frac{a}{b} + \frac{e}{f} < \frac{c}{d} + \frac{g}{h}$.
(3) Por la nota 9.2.8, $\frac{e}{f} \in \mathbb{Q}^+$, y $\frac{c}{d} - \frac{a}{b} \in \mathbb{Q}^+$ por hipótesis. Entonces, por (2) de la proposición 9.2.2, $\left(\frac{c}{d} - \frac{a}{b}\right) \cdot \frac{e}{f} = \frac{c}{d} \cdot \frac{e}{f} - \frac{a}{b} \cdot \frac{e}{f} \in \mathbb{Q}^+$ y así $\frac{a}{b} \cdot \frac{e}{f} < \frac{c}{d} \cdot \frac{e}{f}$.
(4) Por hipótesis $\frac{c}{d} - \frac{a}{b}, \frac{g}{h} - \frac{e}{f}, \frac{a}{b}, \frac{e}{f} \in \mathbb{Q}^+$ y de aquí por (1) y (2) de la proposición 9.2.2, tenemos que $\left(\frac{c}{d} - \frac{a}{b}\right) \cdot \frac{g}{h} + \left(\frac{g}{h} - \frac{e}{f}\right) \cdot \frac{a}{b} = \frac{c}{d} \cdot \frac{g}{h} - \frac{a}{b} \cdot \frac{e}{f} \in \mathbb{Q}^+$.
(5) Como $\frac{a}{b} \neq 0$, entonces $a \cdot b \neq 0$ y por 7 de la proposición 6.3.6, $(ab)^2 = a^2b^2 > 0$. Por lo tanto $\left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2} > 0$.
(6) Es inmediato.
(7) Por el inciso (6), $\frac{a}{b} > 0$ y $\frac{c}{d} > 0$ implican $\frac{b}{a} > 0$ y $\frac{d}{c} > 0$. Usando ahora el inciso (3), tenemos $0 < \frac{a}{b} \cdot \frac{d}{c} < \frac{c}{d} \cdot \frac{d}{c} = 1$ y multiplicando ahora esta última desigualdad por $\frac{b}{a}$ (> 0) obtenemos el resultado deseado, es decir, $0 < \frac{d}{c} < \frac{b}{a}$.
(8) Si $m < n$, entonces existe $r \in \mathbb{N} - \{0\}$ tal que $n = m + r$. El resultado se obtiene de la siguiente afirmación: $1 < \frac{a}{b}$ implica $1 < \left(\frac{a}{b}\right)^r$ para todo $r \in \mathbb{N} - \{0\}$, que puede ser demostrada por inducción y que dejamos como ejercicio (9.2.3). A partir de aquí se obtiene el resultado multiplicando por $\left(\frac{a}{b}\right)^m$.
(9) Se demuestra de manera similar al inciso (8) y se deja como ejercicio (véase ejercicio 9.2.4).■

Hemos visto que el cuadrado de cualquier número racional es mayor o igual que cero. Sin embargo, no todo número racional mayor o igual que cero es un cuadrado, como lo muestra la siguiente

Proposición 9.2.10. *Si p es un número primo, entonces p no es el cuadrado de un número racional.*

Demostración. Supongamos que existe $\frac{a}{b} \in \mathbb{Q}$ tal que $\frac{a^2}{b^2} = p$. Por la proposición 9.1.6 (3) podemos suponer que $(a, b) = 1$. Entonces $a^2 = p \cdot b^2$ y por ser p primo, se debe tener que $p \mid a$ (teorema 7.4.4). Si $a = p \cdot r$, obtenemos $p^2 \cdot r^2 = p \cdot b^2$ y cancelando p llegamos a que $p \cdot r^2 = b^2$. Luego $p \mid b$ y por lo tanto $p \mid (a, b) = 1$, lo que es imposible. Concluimos entonces que no puede existir un número racional cuyo cuadrado es p. ∎

Una propiedad muy importante , respecto al orden, que tienen los números racionales (y que no la tienen los números enteros) es la siguiente

Teorema 9.2.11. *Si $\frac{a}{b}$ y $\frac{c}{d}$ son números racionales tales que $\frac{a}{b} < \frac{c}{d}$, entonces existe un número racional $\frac{e}{f}$ tal que $\frac{a}{b} < \frac{e}{f} < \frac{c}{d}$.*

Demostración. Como $\frac{a}{b} < \frac{c}{d}$, por el teorema 9.2.9 (3) si multiplicamos por $\frac{1}{2}$ a ambos lados de la desigualdad obtenemos que $\frac{a}{2b} < \frac{c}{2d}$. Ahora por (2) del teorema 9.2.9 se tiene, por un lado $\frac{a}{2b} + \frac{a}{2b} < \frac{a}{2b} + \frac{c}{2d}$ y por el otro, $\frac{a}{2b} + \frac{c}{2d} < \frac{c}{2d} + \frac{c}{2d}$ y por lo tanto, el número racional $\frac{e}{f} = \frac{a}{2b} + \frac{c}{2d}$ satisface que $\frac{a}{b} = \frac{a}{2b} + \frac{a}{2b} < \frac{e}{f} < \frac{c}{2d} + \frac{c}{2d} = \frac{c}{d}$. ∎

Sabemos que todo entero n tiene un sucesor, a saber $n + 1$, lo que significa que no existe un entero x tal que $n < x < n + 1$. Debido al teorema 9.2.11, esto no sucede en los números racionales. Resulta interesante mencionar que una consecuencia inmediata del teorema 9.2.11 es el hecho de que el orden en $\mathbb{Q}$ no es un buen orden, que por supuesto ya lo sabíamos debido a que el orden en $\mathbb{Q}$ es una extensión del orden en $\mathbb{Z}$ y este último no es un buen orden (véase ejercicio 6.3.1).

Corolario 9.2.12. *El orden en $\mathbb{Q}$ no es un buen orden.*

Proposición 9.2.13. *Dado $\frac{a}{b} \in \mathbb{Q}$ con $\frac{a}{b} > 0$, existe $n \in \mathbb{N}$ tal que $n > \frac{a}{b}$.*

Demostración. Como $\frac{a}{b} > 0$, podemos considerar $a > 0$ y $b > 0$.
Si $a < b$, entonces $\frac{a}{b} < 1$
Supongamos que $a \geq b$. Por el algoritmo de la división $a = b \cdot n + r$, donde $0 \leq r < b$ y $n \in \mathbb{N} - \{0\}$.
Entonces $\frac{a}{b} = n + \frac{r}{b} < n + 1$. ∎

§§ Ejercicios sección 9.1.

9.1.1. Sea $\frac{a}{b} \in \mathbb{Q}$. Demuestre que $\frac{a}{b} = \frac{c}{1} = c$ para alguna $c \in \mathbb{Z}$ si y sólo si $b \mid a$.

9.1.2. Sea $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ con $\frac{c}{d} \neq 0$. Si definimos $\frac{\frac{a}{b}}{\frac{c}{d}} = \frac{a}{b} \cdot \left(\frac{c}{d}\right)^{-1}$, demuestre que $\frac{\frac{a}{b}}{\frac{c}{b}} = \frac{a}{c}$.

§§ Ejercicios sección 9.2.

9.2.1. [1] Sean $a, b, a', b' \in \mathbb{Z}$ con $b \neq 0$ y $b' \neq 0$ si $(a \cdot b) \cdot (b')^2 = (a' \cdot b') \cdot b^2$. Demuestre que $a \cdot b > 0$ si y sólo si $a' \cdot b' > 0$

9.2.2. Justifique la nota 9.2.4, página 339.

9.2.3. [2] Sea $\frac{a}{b} \in \mathbb{Q}$ tal que $1 < \frac{a}{b}$. Demuestre que $1 < \left(\frac{a}{b}\right)^r$ para todo $r \in \mathbb{N} - \{0\}$.

9.2.4. [3] Sean $\frac{a}{b} \in \mathbb{Q}$ tal que $0 < \frac{a}{b} < 1$ y $m < n$ $(m, n \in \mathbb{Z})$. Demuestre que $\left(\frac{a}{b}\right)^n < \left(\frac{a}{b}\right)^m$.

9.2.5. Muestre que $\frac{a}{b} - \frac{c}{d} = \frac{a \cdot d - b \cdot c}{b \cdot d}$.

9.2.6. Sean $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ tales que $b > 0$ y $d > 0$. Demuestre que $\frac{a}{b} < \frac{c}{d}$ en $\mathbb{Q}$ si y sólo si $a \cdot d < b \cdot c$ en $\mathbb{Z}$.

---

[1] Parte del lema 9.2.1 pág. 339.

[2] Parte del teorema 9.2.9 pág. 340.

[3] Parte del teorema 9.2.9 pág. 340.

Un matemático que no es en algún sentido un poeta no será nunca un matemático completo.
Karl Weierstrass
1815 - 1897

***Capítulo* 10**

Construcción de los números racionales

§ 10.1. Construcción de los números racionales

En el capítulo 9 consideramos a los números racionales como expresiones del tipo $\frac{a}{b}$ donde $a, b \in \mathbb{Z}$ y $b \neq 0$, es decir, cada pareja ordenada de enteros (a, b) con $b \neq 0$ determina un número racional que denotamos por $\frac{a}{b}$. Sin embargo distintas parejas ordenadas pueden determinar al mismo número racional. Basados en las ideas del capítulo 9, construiremos formalmente los números racionales.
Definimos en el conjunto $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ la siguiente relación:

$$(1) \qquad (a, b) \sim (a', b') \underset{def}{\Leftrightarrow} a \cdot b' = b \cdot a'.$$

Proposición 10.1.1. *La relación $\sim$ en $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ es de equivalencia.*

Demostración.

(1) $(a, b) \sim (a, b)$ para todo $(a, b) \in \mathbb{Z} \times (\mathbb{Z} - \{0\})$ ya que $a \cdot b = b \cdot a$.
(2) Si $(a, b) \sim (c, d)$, entonces $a \cdot d = b \cdot c$, que es lo mismo que $c \cdot b = d \cdot a$ y por lo tanto $(c, d) \sim (a, b)$.
(3) Si $(a, b) \sim (c, d)$ y $(c, d) \sim (e, f)$, entonces $a \cdot d = b \cdot c$ y $c \cdot f = d \cdot e$. Multiplicando la primera igualdad por f tenemos $a \cdot d \cdot f = b \cdot c \cdot f = b \cdot d \cdot e$ y como $d \neq 0$, entonces $a \cdot f = b \cdot e$ que es $(a, b) \sim (e, f)$. ∎

Siendo $\sim$ una relación de equivalencia, ésta induce una partición en $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ cuyos elementos son las clases de equivalencia. Denotemos por $\frac{a}{b}$ a la clase de equivalencia de (a, b). Esto es,

$$\tfrac{a}{b} = \{(x, y) \in \mathbb{Z} \times (\mathbb{Z} - \{0\}) \mid (a, b) \sim (x, y)\} = \{(x, y) \in \mathbb{Z} \times (\mathbb{Z} - \{0\}) \mid a \cdot y = b \cdot x\}$$

Con esta notación tenemos que $\frac{a}{b} = \frac{a'}{b'}$ si y sólo si $a \cdot b' = b \cdot a'$. Nótese que esto coincide con la igualdad definida en el capítulo 9.

Definición 10.1.2. *Un número racional es una clase de equivalencia de la relación $\sim$ definida en $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ en (1), de la página 345.*

Denotando por $\mathbb{Q}$ al conjunto de números racionales (clases de equivalencia), tenemos entonces que

$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0 \right\},$$

en donde $\frac{a}{b} = \frac{a'}{b'}$ si y sólo si $a \cdot b' = a' \cdot b$.
La suma y producto en $\mathbb{Q}$ se definen como sigue: sean $\frac{a}{b} \in \mathbb{Q}$

(1) Suma
$$\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + b \cdot c}{b \cdot d}$$
(2) Suma
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$$

Como hemos definido la suma y producto de números racionales en función de sus representantes, debemos demostrar que el resultado no depende de estos representantes, es decir,

Teorema 10.1.3. *Sean $\frac{a}{b}, \frac{a'}{b'}, \frac{c}{d}, \frac{c'}{d'} \in \mathbb{Q}$ tales que $\frac{a}{b} = \frac{a'}{b'}$ $\frac{c}{d} = \frac{c'}{d'}$. Entonces*

$$\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'} \;\; y \;\; \frac{a}{b} \cdot \frac{c}{d} = \frac{a'}{b'} \cdot \frac{c'}{d'}.$$

Demostración. Como $\frac{a}{b} = \frac{a'}{b'}$, $\frac{c}{d} = \frac{c'}{d'}$, entonces $a \cdot b' = b \cdot a'$ y $c \cdot d' = d \cdot c'$.

(1) Suma:

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

Entonces

$$\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}.$$

(2) Producto:

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

Entonces

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{a'}{b'} \cdot \frac{c'}{d'}. \blacksquare$$

§ 10.2. Ejercicios del capítulo 10.

10. 2.1. Demuestre que $\mathbb{Q}$ con las operaciones definidas en este capítulo es un campo.

Los números son creaciones libres del espíritu humano, sirven como medio para concebir más fácil y claramente la diversidad de las cosas. Mediante la construcción puramente lógica de la ciencia de los números, y mediante el dominio numérico continuo que con ella se obtiene, nos encontramos por vez primera en situación de investigar con precisión nuestras representaciones de espacio y tiempo, relacionándolas con este dominio numérico creado en nuestra mente.
Richard Dedekind
1831 - 1916

***Capítulo* 11**

Los números reales

El famoso Teorema de Pitágoras llevó a los griegos a concluir que el sistema de los números racionales es incompleto para realizar mediciones. Concretamente, considérese el triángulo rectángulo donde cada uno de los catetos mide 1. Si x es la medida de la hipotenusa, por el teorema de Pitágoras debe ser $x^2 = 1^2 + 1^2 = 2$. De esta manera, x es un número cuyo cuadrado es 2. Sin embargo no existe un número racional cuyo cuadrado sea igual a 2 (véase la proposición 9.2.10). Por lo tanto $\sqrt{2}$ no es un número racional. Aunque esto no llevó a los griegos a introducir a los números reales, sí desarrollaron una teoría de segmentos de línea "inconmensurables". En realidad, mucho antes que los griegos, los babilonios trabajaron con números que no son racionales, como es el caso del número π.

No fue sino hasta el siglo XIX que Dedekind (1831 - 1916) construyó el sistema de los números reales. Esta construcción se basa en una correspondencia uno a uno entre los números racionales y puntos de una línea y la idea es como sigue:

Consideramos un punto P_0 sobre una línea ℓ y otro punto P_1 a la derecha de P_0. A partir del segmento $\overline{P_0P_1}$ podemos determinar puntos P_2, P_3, . . ., cada uno de ellos a la derecha del anterior y de tal manera que los segmentos $\overline{P_iP_{i+1}}$, para $i = 0, 1, 2, \ldots$ son todos congruentes entre sí (esto puede hacerse con un compás). Entonces, cada número natural determina un único punto en ℓ, donde P_j está a la derecha de P_i si y sólo si $i < j$.

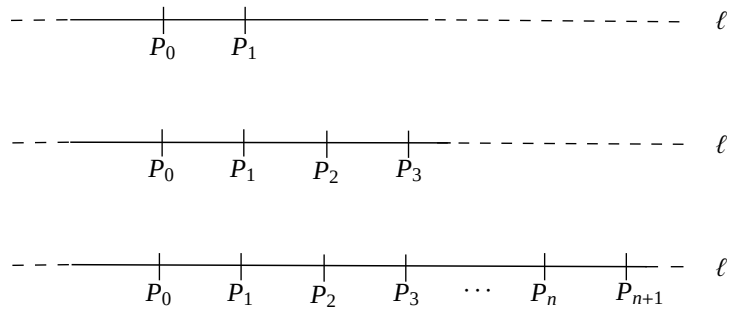


FIGURA 1. Representación geométrica de los números enteros positivos

Si hacemos lo mismo, ahora a la izquierda de P_0, usando el mismo segmento $\overline{P_0P_1}$, obtendremos puntos $P_{-1}, P_{-2}, P_{-3}, \ldots$ en ℓ tal que los segmentos $\overline{P_{-(i+1)}P_{-i}}$ son segmentos congruentes para toda $i = 0, 1, 2, \ldots$.

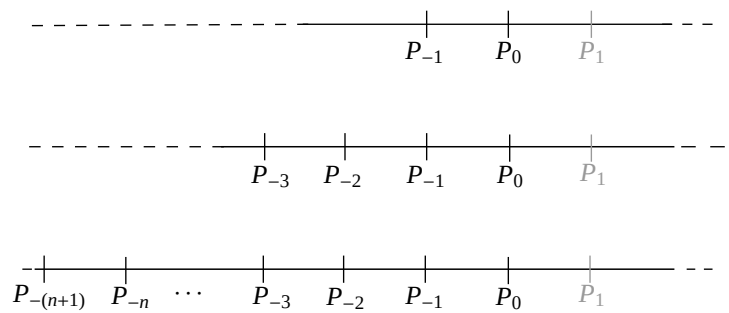


FIGURA 2. Representación geométrica de los números enteros negativos

Con esto establecemos una correspondencia biyectiva entre los números enteros y los puntos P_i, $i \in \mathbb{Z}$, donde para cualesquiera enteros i, j, $i < j$ si y sólo si P_i está a la izquierda de P_j.

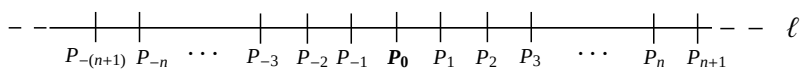


FIGURA 3. Representación geométrica de los números enteros

Ahora, si $n \in \mathbb{N}$, $n > 0$, al segmento $\overline{P_0P_1}$ lo podemos dividir en n segmentos congruentes dos a dos, determinando un punto $P_{\frac{1}{n}}$ de tal manera que la medida del segmento $\overline{P_0P_1}$ es n veces la medida del segmento $\overline{P_0P_{\frac{1}{n}}}$.

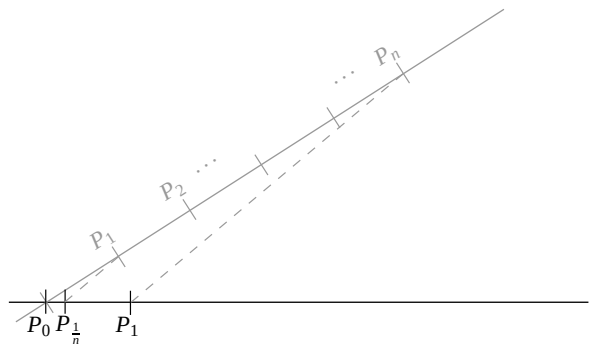


Figura 4. Construcción de un segmento de longitud $\frac{1}{n}$

Podemos repetir el proceso usando como segmento base a $\overline{P_0P_{\frac{1}{n}}}$ para obtener puntos $P_{\frac{2}{n}}, P_{\frac{3}{n}}, \ldots, P_{\frac{m}{n}}, \ldots$ y $P_{-\frac{1}{n}}, P_{-\frac{2}{n}}, \ldots, P_{-\frac{m}{n}}, \ldots$, con $m \in \mathbb{N}$. Así pues, cada número racional $\frac{m}{n}$ determina un punto $P_{\frac{m}{n}}$ en ℓ tal que $\frac{m}{n} < \frac{r}{s}$ si y sólo si $P_{\frac{m}{n}}$ está a la izquierda de $P_{\frac{r}{s}}$.

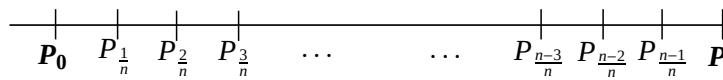


Figura 5. División de un segmento en n partes iguales

Sin embargo con esto no se agotan los puntos de la línea ℓ. Si consideramos la medida $\overline{P_0P_1}$ como 1 y construimos un triángulo rectángulo cuyos catetos son de medida 1, su hipotenusa tendrá longitud $\sqrt{2}$, y trazando un círculo con centro P_0 y radio $\sqrt{2}$, éste cortará a la línea ℓ a la derecha de P_0 es un punto que no coincide con ninguno de los ya construidos.

Finalmente, la idea para construir los números reales es la siguiente: Cada punto P de la línea ℓ determina dos subconjuntos de números racionales que son los correspondientes a los puntos que están a la izquierda de P y los que están a la derecha de P. Estos subconjuntos tienen propiedades muy especiales y son éstas las que consideraremos para obtener los números reales.

§ 11.1. Cortaduras de Dedekind

Existen dos tipos de cortaduras de Dedekind, las superiores o derechas y las inferiores o izquierdas. Para construir los números reales debemos escoger con cual de estos dos tipos de cortaduras trabajaremos. Aunque el desarrollo de la teoría es muy similar en ambos casos, hemos escogido las cortaduras superiores ya que al introducir el producto resulta menos natural la definición de éste para las cortaduras inferiores que para la superiores. Como desventaja está por ejemplo, la definición de orden. En las inferiores se define el orden para cortaduras α y β por $\alpha < \beta$ si $\alpha \subsetneq \beta$ y en las superiores la definición está dada por $\alpha < \beta$ si $\beta \subsetneq \alpha$. Daremos la definición de ambos tipos de cortaduras, pero de ahí en adelante sólo trabajaremos con las superiores.

Definición 11.1.1. *Un subconjunto α de números racionales se llama una* ***cortadura de Dedekind superior o derecha*** *(inferior o izquierda) si:*

(1) $\emptyset \neq \alpha \subsetneq \mathbb{Q}$
(2) Si $r \in \alpha$ *y* $s \in \mathbb{Q}$ *tal que* $r < s$ $(s < r)$*, entonces* $s \in \alpha$
(3) α *no tiene elemento mínimo (máximo).*

A partir de aquí trabajaremos únicamente con cortaduras superiores y por este motivo sólo nos referiremos a ellas como cortaduras.
El siguiente teorema nos provee de muchos ejemplos de cortaduras. Concretamente, cada número racional r determina una cortadura α_r como sigue.

Teorema 11.1.2. *Si* $r \in \mathbb{Q}$*, entonces* $\alpha_r = \{s \in \mathbb{Q} \mid r < s\}$ *es una cortadura.*

Demostración.

(1) $\emptyset \neq \alpha_r \subsetneq \mathbb{Q}$ ya que $r + 1 \in \alpha_r$.
(2) Sea $s \in \alpha_r$ y $t \in \mathbb{Q}$ tal que $s < t$. Como $r < s$, entonces debe ser $r < t$ y por lo tanto $t \in \alpha_r$.
(3) Si α_r tuviera mínimo, digamos r_0, por la definición de α_r, $r < r_0$. Como $r, r_0 \in \mathbb{Q}$, entonces $\frac{r+r_0}{2} \in \mathbb{Q}$ y además $r < \frac{r+r_0}{2} < r_0$ y por lo tanto $\frac{r+r_0}{2} \in \alpha_r$, lo que contradice que r_0 es el mínimo de α_r. Entonces α_r no tiene mínimo. ∎

En particular se tiene que $\alpha_0 = \mathbb{Q}^+ = \{r \in \mathbb{Q} \mid r > 0\}$ es una cortadura.

Teorema 11.1.3. *La correspondencia* $r \mapsto \alpha_r$ *es inyectiva. Es más, para* $r, r' \in \mathbb{Q}$*,* $r < r'$ *si y sólo si* $\alpha_{r'} \subsetneq \alpha_r$.

Demostración. Supongamos que $r < r'$ y sea $s \in \alpha_{r'}$. Entonces $r' < s$ y por lo tanto $r < s$, lo que implica que $s \in \alpha_r$ y así $\alpha_{r'} \subseteq \alpha_r$. Para demostrar $\alpha_{r'} \neq \alpha_r$ basta exhibir un elemento de α_r que no pertenezca a $\alpha_{r'}$, siendo este elemento $t = \frac{r+r'}{2} \in \mathbb{Q}$ ya que $r < t < r'$.
Inversamente, supongamos que $\alpha_{r'} \subsetneq \alpha_r$. Entonces existe $s \in \alpha_r$ (lo que significa $r < s$) tal que $s \notin \alpha_{r'}$. Si fuera $r' \leq r$, entonces se tendría que $r' < s$ lo que implicaría que $s \in \alpha_{r'}$, que no puede ser ya que escogimos s tal que $s \notin \alpha_{r'}$. Por lo tanto $r < r'$. Por último, que la correspondencia $r \mapsto \alpha_r$ es inyectiva es consecuencia inmediata de la equivalencia recién demostrada. ∎

***Corolario 11.1.4**. Para cualesquiera números racionales r y r′ se tiene que $\alpha_r \subseteq \alpha_{r'}$ o $\alpha_{r'} \subseteq \alpha_r$.*

Demostración. Es inmediato del teorema 11.1.3 y del hecho de que $\leq$ en $\mathbb{Q}$ es un orden total. ∎

Este último corolario nos permite afirmar que cualesquiera dos cortaduras de la forma α_r y $\alpha_{r'}$ son comparables mediante $\subseteq$. En realidad esto es cierto para dos cortaduras arbitrarias.

***Teorema 11.1.5**. Dadas dos cortaduras α y β, se satisface una y sólo una de las siguientes relaciones $\alpha = \beta$, $\alpha \subsetneq \beta$ o $\beta \subsetneq \alpha$.*

Demostración. Supongamos que $\alpha \nsubseteq \beta$. Demostraremos que $\beta \subsetneq \alpha$ y para esto sea $s \in \beta$.
Ya que $\alpha \nsubseteq \beta$, existe $r \in \alpha$ tal que $r \notin \beta$. Entonces $s \leq r$ o $r < s$. No puede ser $s \leq r$ ya que en este caso, por definición, se tendría que $r \in \beta$, que no es cierto. Por lo tanto $r < s$ y así $s \in \alpha$ y debido a que $r \in \alpha$ y $r \notin \beta$, entonces $\beta \subsetneq \alpha$. ∎

***Definición 11.1.6**. El conjunto de **números reales**, denotado por $\mathbb{R}$, es el conjunto de cortaduras de Dedekind, esto es, un número real es una cortadura de Dedekind.*

La identificación de los números racionales, como números reales, está dada por la función $i : \mathbb{Q} \longrightarrow \mathbb{R}$, dada anteriormente por $i(r) = \alpha_r$ y que ya hemos visto es inyectiva (teorema11.1.3)
Introduciremos ahora un orden en $\mathbb{R}$ a través de $\subseteq$ y que por el teorema 11.1.5 éste será total. Además resultará ser una extensión del orden en $\mathbb{Q}$ vía la identificación de los números racionales con las cortaduras de la forma α_r ($r \in \mathbb{Q}$).

Definición 11.1.7. *Dados dos números reales α y β, diremos que* ***α es menor que β*** *y lo denotaremos $\alpha < \beta$, si $\beta \subsetneq \alpha$.*

Teorema 11.1.8. *La relación $\leq$ definida en $\mathbb{R}$ es un orden total.*

Demostración. $\leq$ es un orden parcial puesto que para cualesquiera números reales α, β y γ se tiene que

(1) $\alpha \leq \alpha$, ya que $\alpha \subseteq \alpha$.
(2) Si $\alpha \leq \beta$ y $\beta \leq \alpha$, entonces, por definición, $\beta \subseteq \alpha$ y $\alpha \subseteq \beta$. Luego $\alpha = \beta$.
(3) Si $\alpha \leq \beta$ y $\beta \leq \gamma$, entonces, $\beta \subseteq \alpha$ y $\gamma \subseteq \beta$ y de aquí $\gamma \subseteq \alpha$ lo que significa $\alpha \leq \gamma$.

Este orden es total por el teorema 11.1.5. ∎

Definimos la suma y el producto en $\mathbb{R}$ en función de la suma y el producto en $\mathbb{Q}$ respectivamente y de tal manera que, como hicimos en la construcción de $\mathbb{Z}$ a partir de $\mathbb{N}$ y la construcción de $\mathbb{Q}$ a partir de $\mathbb{Z}$, estas operaciones extienden a las de $\mathbb{Q}$, en el sentido de que para la función i (que es la identificación de los números racionales como números reales) se tendrá que $i(r + r') = i(r) + i(r')$ y $i(r \cdot r') = i(r) \cdot i(r')$ para cualesquiera $r, r' \in \mathbb{Q}$.

Definición 11.1.9. *Dadas dos cortaduras α y β, su suma es el conjunto, denotado por $\alpha + \beta$, $\alpha + \beta = \{r + s \mid r \in \alpha \; s \in \beta\}$.*

Veamos, antes que otra cosa, que la suma en $\mathbb{R}$ está bien definida, es decir, $\alpha + \beta \in \mathbb{R}$.

Proposición 11.1.10. *Si α y β son cortaduras, entonces $\alpha + \beta$ es una cortadura.*

Demostración.

(1) Como $\alpha \neq \varnothing$ y $\beta \neq \varnothing$, se tiene claramente que $\alpha + \beta \neq \varnothing$. Por otro lado, como $\alpha \subsetneq \mathbb{Q}$ y $\beta \subsetneq \mathbb{Q}$, entonces existen $q, t \in \mathbb{Q}$ tales que $q \notin \alpha$ y $t \notin \beta$ y por la definición de cortadura se debe tener que $q < r$ para toda $r \in \alpha$ y $t < s$ para toda $s \in \beta$, lo que implica que $q + t < r + s$ para todo $r \in \alpha$ y $s \in \beta$ y por lo tanto $q + t \notin \alpha + \beta$. Entonces $\varnothing \neq \alpha + \beta \subsetneq \mathbb{Q}$.
(2) Sea $t \in \mathbb{Q}$ tal que $r + s < t$, donde $r \in \alpha$ y $s \in \beta$. Entonces $r < t - s$ y por lo tanto $t - s \in \alpha$. Como $s \in \beta$, concluimos que $t = (t - s) + s \in \alpha + \beta$.
(3) Para cualesquiera $r \in \alpha$ y $s \in \beta$, por ser α y β cortaduras, existen $q \in \alpha$ y $t \in \beta$ tales que $q < r$ y $t < s$ y por lo tanto $q + t \in \alpha + \beta$ y $q + t < r + s$. Con esto hemos demostrado que dado cualquier elemento en $\alpha + \beta$ (recuerde que sus elementos

son de la forma $r + s$ con $r \in \alpha$ y $s \in \beta$) existe un elemento en $\alpha + \beta$ que es menor. Concluimos entonces que $\alpha + \beta$ no tiene mínimo. ∎

Antes de presentar las propiedades de la suma, recién definida en $\mathbb{R}$, entre las que se encuentra la existencia del inverso aditivo de cada elemento, discutiremos sobre esta última para descubrir quién debe ser el inverso aditivo de una cortadura α y al que denotaremos por $\boldsymbol{-\alpha}$. Por supuesto, como es de esperar, el neutro aditivo es α_0 (la cortadura determinada por 0, dada en el teorema 11.1.2). Queda claro que definir $-\alpha = \{-r \mid r \in \alpha\}$ no tiene sentido ya que ni siquiera es cortadura (ejercicio 11.1.1). Así pues, debemos encontrar una cortadura β tal que $\alpha + \beta = \alpha_0 = \{r \in \mathbb{Q} \mid r > 0\}$, lo que nos dice que los elementos s de β, deben satisfacer que $r + s > 0$ para toda $r \in \alpha$, es decir $s > -r$ para toda $r \in \alpha$. Esto último nos conduce a considerar el conjunto $\beta = \{s \in \mathbb{Q} \mid s > -r \text{ para toda } r \in \alpha\}$. Este conjunto satisface (1) y (2) de la definición de cortadura, pero no necesariamente el inciso (3), ya que por ejemplo, en el caso concreto de una cortadura α_{r_0}, la cortadura identificada con el número racional r_0, el conjunto tendría mínimo, a saber $-r_0$. Esto es, primero porque $-r_0 \in \beta$ ya que $-r_0 > -r$ para toda $r \in \alpha_{r_0}$, y en segundo lugar, para toda $s \in \beta$, debe ser $-r_0 \leq s$, puesto que en caso contrario, $s < -r_0$ implica $-s > r_0$, lo que a su vez implica que $-s \in \alpha$ y ya que $s \in \beta$, entonces debería ser, en particular, $s > -(-s) = s$, lo que es un absurdo. Sin embargo, si a β le quitamos el elemento $-r_0$, entonces $\beta - \{r_0\}$ resulta ser una cortadura y $\alpha_{r_0} + (\beta - \{r_0\}) = \alpha_0$. Siguiendo esta idea y para, en general, eliminar de β el elemento mínimo definimos $\beta = -\alpha$ como

Definición 11.1.11. *Para cualquier cortadura α,*

$$-\alpha = \left\{ s \in \mathbb{Q} \mid s > q \text{ para algún } q \in \mathbb{Q} \text{ tal que } q > -r \text{ para todo } r \in \alpha \right\}.$$

Proposición 11.1.12. *Si α es una cortadura, entonces $-\alpha$ es una cortadura.*

Demostración.

(1) Como $\alpha \subsetneq \mathbb{Q}$, sea $q \in \mathbb{Q}$ tal que $q \notin \alpha$. Entonces $q < r$ para toda $r \in \alpha$, o lo que es lo mismo, $-q > -r$ para todo $r \in \alpha$, por lo que para cualquier $s \in \mathbb{Q}$ tal que $s > -q$ se tiene que $s \in -\alpha$. Además, de la definición de $-\alpha$ se tiene que para todo $r \in \alpha$, $-r \notin -\alpha$, lo que implica que $-\alpha \subsetneq \mathbb{Q}$.
(2) Para todo $s \in -\alpha$ y para toda $t \in \mathbb{Q}$ tal que $t > s$, de la definición de $-\alpha$, se tiene $t \in -\alpha$.

(3) Dado $s \in -\alpha$, existe $q \in \mathbb{Q}$ con $s > q$ y tal que $q > -r$ para todo $r \in \alpha$. Entonces $s' = \frac{s+q}{2} \in -\alpha$ y $s' < s$. Esto muestra que $-\alpha$ no tiene mínimo. ∎

Antes de demostrar las propiedades de la suma damos un lema que necesitaremos.

Lema 11.1.13. *Sea α una cortadura y $t \in \mathbb{Q}$, $t > 0$. Entonces existe $s \in \mathbb{Q}$, $s \notin \alpha$ tal que $t + s \in \alpha$.*

Demostración. Supongamos que para toda $s \in \mathbb{Q}$, tal que $s \notin \alpha$, se tiene que $s + t \notin \alpha$. Como $s + t \notin \alpha$, $s + 2t = (s + t) + t \notin \alpha$, etc, así que se puede demostrar sin dificultad, por inducción sobre n, que $s + nt \notin \alpha$ para toda $n \in \mathbb{N}$. Sin embargo, dado $r \in \alpha$, si tomamos $n > \frac{r-s}{t}$ (la existencia de n está garantizada por la proposición 9.2.13, tomando en cuenta que $r - s > 0$ y $t > 0$), entonces $s + nt > r$ y por lo tanto $s + nt \in \alpha$ lo que contradice la hipótesis de que $s + nt \notin \alpha$ para toda $n \in \mathbb{N}$. ∎

Teorema 11.1.14. *La suma en $\mathbb{R}$ tiene las siguientes propiedades.*

(1) *asociativa.*
(2) *conmutativa.*
(3) *α_0 es el neutro aditivo.*
(4) *$-\alpha$ es el inverso de α, para todo $\alpha \in \mathbb{R}$.*

Demostración. Las propiedades asociativa y conmutativa son consecuencia de las respectivas propiedades en $\mathbb{Q}$ (ejercicio 11.1.2).

(3) Para toda $\alpha \in \mathbb{R}$, $\alpha + \alpha_0 = \alpha$.
Si $q \in \alpha + \alpha_0$, entonces $q = r + s$ con $r \in \alpha$ y $s \in \alpha_0$ y ya que $s > 0$, debe ser $q > r$ y por lo tanto $q \in \alpha$. Ahora, si $q \in \alpha$, como α no tiene mínimo, existe $r \in \alpha$ tal que $r < q$. Entonces $q = r + (q - r)$ donde $r \in \alpha$ y $q - r > 0$ y por lo tanto $q \in \alpha + \alpha_0$.
(4) $\alpha + (-\alpha) = \alpha_0$
Sea $t \in \alpha + (-\alpha)$ y $t = r + s$ con $r \in \alpha$ y $s \in -\alpha$. Por la definición de $-\alpha$, debe ser $s > q$ para alguna $q \in \mathbb{Q}$ tal que $q > -u$ para toda $u \in \alpha$. En particular $q > -r$, lo que significa que $q + r \in \alpha_0$ y ya que $t = r + s > r + q$, concluimos que $t \in \alpha_0$. Por otro lado, si $t \in \alpha_0$, entonces $t > 0$ y por el lema 11.1.13, dado $\frac{t}{2} > 0$, existe $s \in \mathbb{Q}$, $s \notin \alpha$ y $\frac{t}{2} + s \in \alpha$. Como $s < r$ para toda $r \in \alpha$ debido a que $s \notin \alpha$, entonces $\frac{t}{2} + (-s) > -s > -r$ para toda $r \in \alpha$ y por lo tanto $\frac{t}{2} + (-s) \in -\alpha$ y así $t = \left(\frac{t}{2} + s\right) + \left(\frac{t}{2} + (-s)\right) \in \alpha + (-\alpha)$. ∎

Proposición 11.1.15. *Si $r, s \in \mathbb{Q}$, entonces $\alpha_r + \alpha_s = \alpha_{r+s}$ y $-\alpha_r = \alpha_{-r}$.*

Demostración. $\alpha_r + \alpha_s = \alpha_{r+s}$. Si $t \in \alpha_r + \alpha_s$, entonces $t = u + w$ donde $u \in \alpha_r$ y $w \in \alpha_s$. Pero $u > r$ y $w > s$ implican que $t = u + w > r + s$. Por lo tanto $t \in \alpha_{r+s}$. Ahora, $t \in \alpha_{r+s}$ implica que $t > r + s$ y entonces $t - r > s$ y $t - s > r$ y de aquí se tiene que $\frac{t-r+s}{2} > s$ y $\frac{t-s+r}{2} > r$, por lo que $\frac{t-r+s}{2} \in \alpha_s$ y $\frac{t-s+r}{2}\alpha_r$ y así $t = \frac{t-s+r}{2} + \frac{t-r+s}{2} \in \alpha_r + \alpha_s$.

$-\alpha_r = \alpha_{-r}$. $t \in -\alpha_r$ implica que existe $q \in \mathbb{Q}$ tal que $t > q$ y $q > -s$ para toda $s \in \alpha_r$. Pero si $-q < s$ para toda $s \in \alpha_r$, entonces $-q \leq r$ ya que si $r < -q$ se tendría que $-q \in \alpha_r$ y entonces $-q < -q$ lo que es absurdo. Como $-t < -q \leq r$, entonces $t > -r$ por lo que $t \in \alpha_{-r}$. Por otro lado, $t \in \alpha_{-r}$ implica $t > -r$, así que para $q = -r$, tenemos que $t > q$ y $q > -s$ para toda $s \in \alpha_r$, con lo que concluimos que $t \in -\alpha_r$. ∎

Esta última proposición nos indica que la suma que hemos definido en $\mathbb{R}$ es efectivamente una extensión de la suma en $\mathbb{Q}$ (vía la identificación de los racionales con cortaduras).
Definimos ahora el producto de cortaduras. Lo primero que se nos podría ocurrir es que, como en el caso de la suma, el producto de α y β sea $\alpha \cdot \beta = \{r \cdot s \mid r \in \alpha \text{ y } s \in \beta\}$, pero desafortunadamente, este conjunto es una cortadura sólo en el caso en que $\alpha \geq \alpha_0$ y $\beta \geq \alpha_0$. Es más, si $\alpha < \alpha_0$ o $\beta < \alpha_0$, $\{r \cdot s \mid r \in \alpha \text{ y } s \in \beta\} = \mathbb{Q}$. Sin embargo, como se verá, el producto de dos cortaduras se definirá a través del producto de cortaduras no negativas y del inverso aditivo, en los diferentes casos que se puedan presentar. Para la definición del producto nos será útil la siguiente propiedad.

Proposición 11.1.16. *Si α es una cortadura tal que $\alpha < \alpha_0$, entonces $-\alpha > \alpha_0$.*

Demostración. Por la definición de orden en $\mathbb{R}$, $\alpha < \alpha_0$ significa que $\alpha_0 \subsetneq \alpha$. Entonces existe $r \in \alpha$ tal que $r \notin \alpha_0$, es decir, $r \leq 0$. Debido a que α no tiene mínimo podemos tomar $t \in \alpha$ tal que $t < r$ y de aquí $-t > 0$, por lo que $-t \in \alpha_0$. Para demostrar que $-\alpha \subseteq \alpha_0$ ($\alpha_0 \leq -\alpha$) basta ver que cada elemento de $-\alpha$ es mayor que $-t$ (que ya hemos dicho que pertenece a α_0). Si $s \in -\alpha$, por la definición de $-\alpha$, $s > -r$ para toda r, por lo que en particular $s > -t$ ya que $t \in \alpha$ y como $-t \in \alpha_0$, entonces $s \in \alpha_0$.
Hemos probado que $-\alpha \subseteq \alpha_0$ y por último $-\alpha \neq \alpha_0$ ya que $-t \in \alpha_0$ y $-t \notin -\alpha$, concluimos que $-\alpha \subsetneq \alpha_0$, es decir, $\alpha_0 < -\alpha$. ∎

Con el propósito de fijar ideas y teniendo en cuenta que α_0 (que es el identificado con el 0 en $\mathbb{Q}$) es el neutro aditivo de $\mathbb{R}$, de aquí en adelante escribiremos 0 en lugar de α_0.

Definición 11.1.17. *Sean $\alpha, \beta \in \mathbb{R}$. El producto $\alpha \cdot \beta$ de α y β es*

(1) $\alpha \cdot \beta = \{r \cdot s \mid r \in \alpha \text{ y } s \in \beta\}$ *si* $\alpha \geq 0$ *y* $\beta \geq 0$,
(2) $\alpha \cdot \beta = -[(-\alpha) \cdot \beta]$ *si* $\alpha < 0$ *y* $\beta \geq 0$,
(3) $\alpha \cdot \beta = -[\alpha \cdot (-\beta)]$ *si* $\alpha \geq 0$ *y* $\beta < 0$,
(4) $\alpha \cdot \beta = (-\alpha) \cdot (-\beta)$ *si* $\alpha < 0$ *y* $\beta < 0$.

Lo primero que debemos hacer es verificar que este producto está bien definido y para esto basta hacerlo para el caso $\alpha \geq 0$ y $\beta \geq 0$, pues cualquiera de los otros casos, teniendo en cuenta la proposición 11.1.16, el producto se define a través de cortaduras donde ambas son mayores o iguales a cero.

Proposición 11.1.18. *Si α y β son cortaduras tales que $\alpha \geq 0$ y $\beta \geq 0$, entonces $\alpha \cdot \beta = \{r \cdot s \mid r \in \alpha \text{ y } s \in \beta\}$ es una cortadura. Además $\alpha \cdot \beta \geq 0$.*

Demostración.

(1) Es claro que $\alpha \cdot \beta \neq \emptyset$. Por otro lado, como $r \cdot s > 0$ para cualquier $r \in \alpha$ y $s \in \beta$, entonces para toda $t \in \mathbb{Q}$ tal que $t < 0$, $t \notin \alpha \cdot \beta$ y por lo tanto $\alpha \cdot \beta \subsetneq \mathbb{Q}$.
(2) Sea $t > r \cdot s$ con $r \in \alpha$ y $s \in \beta$. Como $s > 0$, $\frac{t}{s} > r$ y esto último implica que $\frac{t}{s} \in \alpha$. Entonces $t = \frac{t}{s} \cdot s \in \alpha \cdot \beta$.
(3) Sea $t \in \alpha \cdot \beta$ y $t = r \cdot s$ con $r \in \alpha$ y $s \in \beta$. Como α no tiene mínimo, sea $r' \in \alpha$ tal que $r' < r$. Entonces $r' \cdot s \in \alpha \cdot \beta$ y por ser $s > 0$ debido a que $\beta \geq 0$, se tiene que $r' \cdot s < r \cdot s = t$. Por lo tanto $\alpha \cdot \beta$ no tiene mínimo.

Por último es claro que $\alpha \cdot \beta \geq 0$ ya que los elementos de α y β son mayores que cero. ∎

Aceptemos por el momento que α_1 es el neutro multiplicativo de $\mathbb{R}$ y discutamos cómo tendría que ser definido el inverso multiplicativo (que como veremos sí existe) de un número real $\alpha > 0$. Esto es, queremos ver cómo debe ser β sabiendo que se tiene que cumplir $\alpha \cdot \beta = \alpha_1$, y adelantándonos un poco al resultado, a β lo denotamos por α^{-1}.
Todo elemento q de α^{-1} debe tener la propiedad de que $t \cdot q > 1$ para todo $t \in \alpha$, lo que significa que para cada $t \in \alpha$ debe existir $s_t \in \mathbb{Q}^+$ tal que $t \cdot q = 1 + s_t$, con lo que para todo $t \in \alpha_1$, q debe ser de la forma $q = \frac{1+s_t}{t}$. Por otro lado, para todo $s \in \mathbb{Q}$ tal que $s \in \alpha_0$ y $s \notin \alpha$ se tiene que $s < t$ para toda $t \in \alpha$, esto es, $0 < s < t$

para toda $t \in \alpha$. Entonces

$$q = \frac{1 + s_t}{t} < \frac{1 + s_t}{s}$$

y por lo tanto $\frac{1+s_t}{s}$ debe pertenecer a α^{-1} para toda $s \in \mathbb{Q}$ tal que $0 < s < t$ para toda $t \in \alpha$. Teniendo en cuenta que $1 + s_t > 1$ para toda $t \in \alpha$ podríamos considerar los números racionales de la forma $\frac{r}{s}$ donde $r > 1$ y $s \in \mathbb{Q}$ tal que $0 < s < t$ para toda $t \in \alpha$ como los posibles elementos de α^{-1}. Efectivamente, demostraremos que para $\alpha > 0$,

$$\alpha^{-1} = \left\{ \frac{r}{s} \mid r \in \mathbb{Q},\ r > 1 \text{ y } s \in \mathbb{Q} \text{ tal que } 0 < s < t \text{ para toda } t \in \alpha \right\}$$

es una cortadura y $\alpha \cdot \alpha^{-1} = \alpha_1$.

Proposición 11.1.19. *Sea $\alpha \in \mathbb{R}$ tal que $\alpha > 0$ y sea $\alpha^{-1} = \left\{ \frac{r}{s} \mid r \in \mathbb{Q},\ r > 1$ y $s \in \mathbb{Q}$ tal que $0 < s < t$ para toda $t \in \alpha \right\}$. Entonces*

(1) *α^{-1} es una cortadura.*
(2) *$\alpha \cdot \alpha^{-1} = \alpha_1$.*

Demostración.

(1) α^{-1} es cortadura.

(i) Como $\alpha > 0$, existe $s \in \alpha_0$ tal que $s \notin \alpha$ y entonces $0 < s < t$ para toda $t \in \alpha$, por lo que para $r > 1$, $\frac{r}{s} \in \alpha^{-1}$ y así $\alpha^{-1} \neq \emptyset$. Por otro lado, los elementos de α^{-1} son todos positivos, entonces $\alpha^{-1} \subsetneq \mathbb{Q}$.

(ii) Sea $w \in \alpha^{-1}$ y $q \in \mathbb{Q}$ tal que $q > w$. Entonces $w = \frac{r}{s}$, con $r, s \in \mathbb{Q}$, $r > 1$ y $0 < s < t$ para toda $t \in \alpha$. Como $q > \frac{r}{s}$ y $s > 0$, entonces $q \cdot s > r > 1$. Así que $q = \frac{q \cdot s}{s}$, es tal que $q \cdot s > 1$ y $0 < s < t$ para toda $t \in \alpha$ y por lo tanto $q \in \alpha^{-1}$.

(iii) Sea $q = \frac{r}{s} \in \alpha^{-1}$, con $r, s \in \mathbb{Q}$, $r > 1$ y $0 < s < t$ para toda $t \in \alpha$. Como $r > 1$, entonces existe $r' \in \mathbb{Q}$ (por ejemplo $\frac{1+r}{2}$) tal que $r > r' > 1$ y por lo tanto $\frac{r'}{s} \in \alpha^{-1}$ con $\frac{r'}{s} < \frac{r}{s}$. Luego α^{-1} no tiene mínimo.

(2) $\alpha \cdot \alpha^{-1} = \alpha_1$.

Como $\alpha > 0$ y $\alpha^{-1} > 0$ (ejercicio 11.1.3), $\alpha \cdot \alpha^{-1}$ está definido como

$$\alpha \cdot \alpha^{-1} = \{r \cdot s \mid r \in \alpha,\ s \in \alpha^{-1}\}.$$

Sea $q \in \alpha \cdot \alpha^{-1}$, $q = u \cdot w$ con $u \in \alpha$ y $w \in \alpha^{-1}$. Entonces $w = \frac{r}{s}$ con $r, s \in \mathbb{Q}$, $r > 1$ y $0 < s < t$ para todo $t \in \alpha$ y en particular $0 < s < u$. De aquí se tiene que $q = u \cdot w > s \cdot w = r > 1$ y por lo tanto $q \in \alpha_1$. Inversamente, sea $q \in \alpha_1$. Como α_1 no tiene mínimo, sea $q' \in \alpha_1$ tal que $q' < q$, luego $\frac{q-q'}{q'} > 0$. Sea $s \in \mathbb{Q}$

tal que $0 < s < t$ para toda $t \in \alpha$. Entonces $s\left(\frac{q-q'}{q'}\right) > 0$ y por el lema 11.1.13, existe $s' \in \mathbb{Q}$, $s' \notin \alpha$, además podemos suponer $s' > 0$ (justifique esto último), tal que $s' + s\left(\frac{q-q'}{q'}\right) \in \alpha$. También podemos considerar $s' \geq s$ ya que en caso contrario si $s' < s$ sustituimos, entonces $s' + s\left(\frac{q-q'}{q'}\right)$ por $s + s\left(\frac{q-q'}{q'}\right) \in \alpha$. Debido a que $0 < s' < t$ para toda $t \in \alpha$ y $q' > 1$, se tiene que $\frac{q'}{s'} \in \alpha^{-1}$. Entonces $q = \left[s' + s'\left(\frac{q-q'}{q'}\right)\right] \cdot \frac{q'}{s'} \geq \left[s' + s\left(\frac{q-q'}{q'}\right)\right] \cdot \frac{q'}{s'}$ y ya que $\left[s' + s\left(\frac{q-q'}{q'}\right)\right] \cdot \frac{q'}{s'} \in \alpha \cdot \alpha^{-1}$, entonces $q \in \alpha \cdot \alpha^{-1}$. ∎

Ya habiendo demostrado la existencia del inverso multiplicativo para una cortadura $\alpha > 0$, es fácil demostrarlo ahora para una cortadura $\alpha < 0$ (ejercicio 11.1.4) ya que para el caso $\alpha > 0$ se tiene que $\alpha^{-1} > 0$.

Teorema 11.1.20. *El producto en $\mathbb{R}$ tiene las siguientes propiedades.*

(1) *asociativo.*
(2) *conmutativo.*
(3) *α_1 es el neutro multiplicativo.*
(4) *Para toda $\alpha \in \mathbb{R}$, $\alpha \neq 0$, $\alpha \cdot \alpha^{-1} = \alpha_1$.*

Demostración. Podría parecer que la demostración de la asociatividad y conmutatividad se hacen muy largas debido a que el producto se definió considerando cuatro casos, pero en realidad esto no lo es tanto ya que este producto se definió a través del producto de cortaduras mayores que cero, con lo que basta demostrar estas propiedades para estos casos y no presentan mayor dificultad, por lo que los dejamos como ejercicio (ejercicio 11.1.5). La demostración de que α^{-1} es el inverso multiplicativo de α es consecuencia de la proposición 11.1.19, así que sólo demostraremos que $\alpha \cdot \alpha_1 = \alpha$ para $\alpha > 0$.

(3) $\alpha \cdot \alpha_1 = \alpha$ $(\alpha > 0)$
Sea $q \in \alpha \cdot \alpha_1$. Entonces $q = r \cdot s$ donde $r \in \alpha$ y $s \in \alpha_1$ (esto es porque $\alpha > 0$ y $\alpha_1 > 0$). Como $s > 1$, $q = r \cdot s > r$ y por lo tanto $q \in \alpha$. Inversamente, sea $q \in \alpha$. Debido a que α no tiene mínimo, existe $r \in \alpha$ tal que $r < q$ y de aquí se tiene que $\frac{q}{r} > 1$ y así para $s = \frac{q}{r}$, $q = r \cdot s$ donde $r \in \alpha$ y $s \in \alpha_1$, por lo que $q \in \alpha \cdot \alpha_1$. ∎

Teorema 11.1.21. $(\mathbb{R}; +, \cdot)$ *es un campo*

Demostración. Teniendo en cuenta el teorema 11.1.14 y el teorema 11.1.20 sólo queda por demostrar la ley distributiva, es decir, para cualesquiera $\alpha, \beta, \gamma \in \mathbb{R}$, $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$ y para esto debemos considerar los diferentes casos que se

pueden presentar. El caso en que $\alpha \geq 0, \beta \geq 0$ y $\gamma \geq 0$ no presenta ningún problema y es consecuencia de la ley distributiva en $\mathbb{Q}$. Demostraremos aquí sólo un caso de los restantes, dejando como ejercicio los demás (véase ejercicio 11.1.6). Suponemos $\alpha \geq 0, \beta \geq 0, \gamma < 0$ y $\beta + \gamma \geq 0$. Como $\gamma < 0$, por la proposición 11.1.16 debe ser $-\gamma > 0$. Por la proposición 11.1.18, se tiene que $\alpha \cdot (-\gamma) \geq 0$ y entonces $\alpha(\beta + \gamma) + \alpha(-\gamma) = \alpha((\beta + \gamma) + (-\gamma)) = \alpha \cdot \beta$. Por lo tanto $\alpha(\beta + \gamma) = \alpha \cdot \beta + \left[-(\alpha(-\gamma))\right] = \alpha \cdot \beta + \alpha \cdot \gamma$. ∎

Presentamos a continuación algunas propiedades del orden en $\mathbb{R}$.

Teorema 11.1.22. *Sean $\alpha, \beta, \gamma, \delta \in \mathbb{R}$. Entonces*

(1) $\alpha < \beta$ *implica* $\alpha + \gamma < \beta + \gamma$.
(2) $\alpha < \beta$ *y* $\gamma < \delta$ *implican* $\alpha + \gamma < \beta + \delta$.
(3) $\alpha < \beta$ *y* $\gamma > 0$ *implican* $\alpha \cdot \gamma < \beta \cdot \gamma$.
(4) $0 < \alpha < \beta$ *y* $0 < \gamma < \delta$ *implican* $0 < \alpha \cdot \gamma < \beta \cdot \delta$.
(5) *Si* $\alpha < \beta$ *y* $\gamma < 0$, *entonces* $\alpha \cdot \gamma > \beta \cdot \gamma$.
(6) $\alpha^2 \geq 0$.
(7) $\alpha > 0$ *si y sólo si* $-\alpha < 0$.
(8) $\alpha > 0$ *si y sólo si* $\alpha^{-1} > 0$.

La demostración de estas propiedades quedan como ejercicio (véase ejercicio 11.1.7)
El valor absoluto de un número real se define de la misma manera que para los números enteros.

Definición 11.1.23. *Dado un número real α, su valor absoluto, denotado por $|\alpha|$, es*

$$|\alpha| = \begin{cases} \alpha & si\ \alpha \geq 0 \\ -\alpha & si\ \alpha < 0 \end{cases}$$

Las propiedades del valor absoluto son los siguientes y su demostración se deja como ejercicio (véase ejercicio 11.1.8).

Proposición 11.1.24. *Sean α y β números reales. Entonces*

(1) $|\alpha| \geq 0$ *y* $|\alpha| = 0$ *si y sólo si* $\alpha = 0$.
(2) $|\alpha| = |-\alpha|$.
(3) $|\alpha \cdot \beta| = |\alpha| \cdot |\beta|$.
(4) $|\alpha + \beta| \leq |\alpha| + |\beta|$.

De aquí en adelante para cada $r \in \mathbb{Q}$, a su identificado en $\mathbb{R}$ α_r lo denotaremos con r mismo. Una propiedad muy importante que se satisface en el sistema de números reales es que el conjunto de los números racionales es un subconjunto "*denso*" del conjunto de los números reales, lo que significa que dado cualquier número real α, para todo $\epsilon \in \mathbb{R}$, $\epsilon > 0$ existe un número racional r, tal que $|\alpha - r| < \epsilon$, esto es, dado $\alpha \in \mathbb{R}$ siempre podemos encontrar un número racional r tan cercano a α como queramos y esta propiedad es consecuencia del siguiente

Teorema 11.1.25. *Dados dos números reales α y β tales que $\alpha < \beta$, existe un número racional r tal que $\alpha < r < \beta$.*

Demostración. Como $\alpha < \beta$, entonces $\beta \subsetneq \alpha$ y por lo tanto existe $s \in \mathbb{Q}$ tal que $s \in \alpha$ y $s \notin \beta$. Pero $s \in \alpha$ implica que $\alpha_s \subsetneq \alpha$ ($s \in \alpha$ y $s \notin \alpha_s$) y $s \notin \beta$ implica $\beta \subseteq \alpha_s$ (véase el ejercicio 11.1.9) y entonces $\alpha < \alpha_s \leq \beta$. Sin embargo no podemos tomar a s como el racional buscado ya que muy bien puede suceder que $\alpha_s = \beta$, pero si consideramos $r \in \alpha$ tal que $r < s$ (su existencia está garantizada puesto que α no tiene mínimo) se tiene que $\alpha_r \subsetneq \alpha$ y $\beta \subseteq \alpha_s \subsetneq \alpha_r \subsetneq \alpha$ y así $\alpha < r < \beta$. ∎

§ 11.2. Campos ordenados completos

En esta sección describiremos al conjunto de números reales a través de ciertas propiedades que lo determinan de manera única.

Definición 11.2.1. *Sea K un campo y suponga que $<$ es un orden total sobre K. Se dice que K es un* **campo ordenado** *si para cualesquiera $x, y, z \in K$ se cumple*

(1) Si $x < y$, entonces $x + z < y + z$,
(2) Si $x < y$ y $0 < z$, entonces $x \cdot z < y \cdot z$.

Ejemplo 11.2.2. $\mathbb{Q}$ y $\mathbb{R}$ con los órdenes correspondientes, definidos en este libro son campos ordenados.

Algunas consecuencias inmediatas de la definición de campo ordenado son

Teorema 11.2.3. *Sea K un campo ordenado. Para cualesquiera $x, y, z \in K$*

(1) Si $x < y$ y $z < w$, entonces $x + z < y + w$. En particular $0 < x$ y $0 < y$ implican $0 < x + y$.
(2) Si $0 < x$ y $0 < y$, entonces $0 < x \cdot y$.

Demostración.

(1) Por ser K un campo ordenado se tiene que $x + z < y + z$ y $y + z < y + w$ y por lo tanto, ya que $<$ es transitivo (por ser $<$ un orden), se tiene que $x + z < y + w$.
(2) Es una consecuencia inmediata de (2) de la definición de campo ordenado. ∎

Teorema 11.2.4. *Sea K un campo ordenado y sean x, y, z elementos cualesquiera de K.*

(1) Si $x < y$, entonces $-y < -x$.
(2) Si $x < y$ y $z < 0$, entonces $x \cdot z > y \cdot z$. En particular si $x < 0$ y $y < 0$, entonces $x \cdot y > 0$.
(3) Si $x \neq 0$, entonces $x^2 > 0$.
(4) $1 > 0$.

Demostración.

(1) Sumando $z = -x - y$ a ambos lados de la desigualdad $x < y$ obtenemos $-y < -x$.
(2) Por el inciso (1), $-z > 0$ y entonces $x \cdot (-z) < y \cdot (-z)$, esto es $-(x \cdot z) < -(y \cdot z)$ y nuevamente, por el inciso (1), obtenemos $x \cdot z > y \cdot z$.
(3) Si $x \neq 0$, entonces $x > 0$ o $x < 0$. Multiplicando por x en el primer caso, obtenemos $x^2 > 0$ usando (2) de la definición de campo ordenado y en el segundo caso $x^2 > 0$ se obtiene del inciso (2).
(4) Si fuera $1 < 0$, por el inciso (3) tendría que $1 > 0$ lo que es una contradicción. Entonces debe ser $(1)^2 = 1 > 0$. ∎

Ejemplo 11.2.5. Los campos $\mathbb{Z}_p$ (p primo) no pueden ser campos ordenados por la siguiente razón: Si $\mathbb{Z}_p$ fuera un campo ordenado, entonces por (4) del teorema 11.2.4, debe ser $\overline{1} > \overline{0}$ y usando iteradamente la propiedad (1) de campo ordenado se llega a que $\overline{p-1} > \overline{0}$ y de aquí obtenemos que $\overline{0} = \overline{(p-1)} + \overline{1} > \overline{1}$, lo que es absurdo.

Recordamos que la notación que hemos convenido para el neutro multiplicativo en un campo es 1 y por lo tanto la naturaleza, como elemento de un campo $K \neq \mathbb{R}$ no tiene que ver con el 1 de los números naturales. Sin embargo, como para un campo ordenado K una consecuencia de que $0 < 1$ es que $x < x + 1$ para toda $x \in K$, se puede identificar a los números naturales con un subconjunto de K. Para que quede clara esta identificación, denotamos por $\overline{1}$ al neutro multiplicativo

de K. Entonces, como consecuencia de que $0 < \overline{1}$, obtenemos $0 < \overline{1} < \overline{1} + \overline{1} < \overline{1} + \overline{1} + \overline{1} < \overline{1} + \overline{1} + \overline{1} + \overline{1} < \cdots$.
Si definimos $n \cdot \overline{1} = \underbrace{\overline{1} + \overline{1} + \cdots + \overline{1}}_{n-\text{veces}}$ para cada número natural n (en particular $n \cdot \overline{1} = 0$ si y sólo si $n = 0$), la identificación de la que hablamos es $n \longmapsto n \cdot \overline{1}$ para cada número natural n. Sin ninguna dificultad se puede demostrar que $(n+m) \cdot \overline{1} = n \cdot \overline{1} + m \cdot \overline{1}$ y $(n \cdot m) \cdot \overline{1} = (n \cdot \overline{1})(m \cdot \overline{1})$ y por lo tanto, para $n \geq m$, se tiene que $n \cdot \overline{1} = ((n - m) + m) \cdot \overline{1} = (n - m) \cdot \overline{1} + m \cdot \overline{1}$ y de aquí se obtiene que $(n - m) \cdot \overline{1} = n \cdot \overline{1} - m \cdot \overline{1}$ y usando esto último concluimos que la correspondencia es inyectiva.
Por lo anterior, para cualquier campo ordenado K, supondremos $\mathbb{N} \subseteq K$. El hecho de que $\mathbb{N} \subseteq K$, implica entonces que $\mathbb{Z} \subseteq K$ y $\mathbb{Q} \subseteq K$, debido a que el inverso aditivo de $n \in \mathbb{N}$, lo identificamos con el entero $-n \in K$ y el inverso multiplicativo n^{-1} de n ($n \neq 0$) lo identificamos con $\frac{1}{n}$ en K, entonces la *inmersión* de $\mathbb{N}$ en K induce una inmersión de $\mathbb{Q}$ en K y por tal motivo, para cualquier campo ordenado K, podemos suponer $(\mathbb{Q}; +, \cdot, <_{\mathbb{Q}}) \subseteq (K; +, \cdot, <_K)$ entendiéndose por esto que existe una función inyectiva $\varphi : \mathbb{Q} \to K$ tal que

(i) $\varphi(x + y) = \varphi(x) + \varphi(y)$,
(ii) $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$,
(iii) $x <_{\mathbb{Q}} y$ si y sólo si $\varphi(x) <_K \varphi(y)$.

En un campo ordenado se puede definir el valor absoluto de sus elementos, de la misma manera en que se hizo para los enteros.

Definición 11.2.6. *Para cualquier elemento x de un campo ordenado K, su* **valor absoluto** *es*

$$|x| = \begin{cases} x, & si\ x \geq 0; \\ -x, & si\ x < 0. \end{cases}$$

Proposición 11.2.7. *Sea K un campo ordenado y x un elemento en K. Entonces* $|x| = \max\{x, -x\}$.

La demostración se deja como ejercicio (véase ejercicio 11.2.1).
Recordemos ahora la definición de supremo e ínfimo (definición 1.7.15) de un subconjunto de un conjunto parcialmente ordenado (y por lo tanto aplica a conjuntos totalmente ordenados).
Dados un conjunto parcialmente ordenado X, un subconjunto S de X y $\alpha, \beta \in X$, diremos que

(1) α es el **supremo** de S en X si
(i) $x \leq \alpha$ para todo $x \in S$ (α es cota superior de S)
(ii) Si $z \in X$ y $x \leq z$ para todo $x \in S$, entonces $\alpha \leq z$ (α es la mínima de las cotas superiores de S en X).
(2) β es el **ínfimo** de S en X si
(i) $\beta \leq x$ para todo $x \in S$ (β es cota inferior de S)
(ii) Si $w \in X$ y $w \leq x$ para todo $x \in S$, entonces $w \leq \beta$ (β es la máxima de las cotas inferiores de S en X).

Recordamos también que un subconjunto S de un conjunto parcialmente ordenado es **acotado superiormente** (**inferiormente**) si tiene al menos una cota superior (inferior).

Ejemplo 11.2.8. En $\mathbb{Q}$ no todo conjunto acotado superiormente (inferiormente) tiene supremo (ínfimo). El conjunto $S = \{r \in \mathbb{Q} \mid r^2 < 2\}$ está acotado superiormente en $\mathbb{Q}$, por ejemplo 2 es una cota superior. Sin embargo el conjunto de cotas superiores de S en $\mathbb{Q}$ no tiene mínimo, esto es, S no tiene supremo en $\mathbb{Q}$. Este mismo conjunto también está acotado inferiormente y tampoco tiene ínfimo. Sin embargo, el conjunto S visto ahora como subconjunto de $\mathbb{R}$, tiene supremo e ínfimo en $\mathbb{R}$, a saber, $\sqrt{2}$ y $-\sqrt{2}$ respectivamente (más adelante veremos que efectivamente $\sqrt{2} \in \mathbb{R}$).

En general, veremos que cada subconjunto no vacío de $\mathbb{R}$ acotado superiormente (inferiormente) tiene supremo (ínfimo). En el ejemplo anterior se puede ver que $\mathbb{Q}$ no tiene tal propiedad. Daremos un nombre a los campos que tienen estas propiedades.

Definición 11.2.9. *Un campo ordenado K se llama* **completo** *si satisface:*

(1) *Cada subconjunto no vacío de K, acotado superiormente tiene supremo.*
(2) *Cada subconjunto no vacío de K, acotado inferiormente tiene ínfimo.*

Como ya puede verse en el ejemplo 11.2.8, $\mathbb{Q}$ es un campo ordenado que no es completo. Demostraremos que $\mathbb{R}$ es un campo ordenado completo, pero antes de hacer esto, necesitamos el siguiente lema.

Lema 11.2.10. *En un campo ordenado completo K, son equivalentes*

(1) *Cada subconjunto no vació de K, acotado superiormente tiene supremo.*
(2) *Cada subconjunto no vació de K, acotado inferiormente tiene ínfimo.*

Demostración.
(1) $\Longrightarrow$ (2)
Sea $\varnothing \neq S \subseteq K$ tal que S está acotado inferiormente y sea

$$S' = \{s \in K \mid x \text{ es cota inferior de } S\}.$$

Por hipótesis $S' \neq \varnothing$ y S' está acotado superiormente ya que cada elemento de S es una cota superior de S'. Por lo tanto, por hipótesis, S' tiene supremo, el cual es precisamente el ínfimo de S (véase ejercicio 11.2.2).
(2) $\Longrightarrow$ (1)
Se demuestra de manera análoga. ∎

Teorema 11.2.11. *$\mathbb{R}$ es un campo ordenado completo.*

Demostración. Por el lema 11.2.10, sólo necesitamos demostrar (1) o (2) de la definición de campo completo. Demostraremos (2) y para esto sea $\varnothing \neq S \subseteq \mathbb{R}$ tal que S tiene cota inferior β en $\mathbb{R}$. Recordamos que los elementos de $\mathbb{R}$ son cortaduras de Dedekind. Nuestro candidato a ínfimo de S es $\gamma = \bigcup_{\alpha \in S} \alpha$. Verifiquemos esto.
γ es cortadura:

(1) $\gamma \neq \varnothing$ ya que $S \neq \varnothing$ y $\alpha \neq \varnothing$ para cada $\alpha \in S$. Por otro lado como β es una cota inferior de S, entonces $\beta \leq \alpha$ para toda $\alpha \in S$, o lo que es lo mismo $\alpha \subseteq \beta$ para toda $\alpha \in S$ y por lo tanto $\gamma = \bigcup_{\alpha \in S} \alpha \subseteq \beta$. Como β es cortadura, $\beta \subsetneq \mathbb{Q}$ y entonces $\gamma \subsetneq \mathbb{Q}$.
(2) Sea $y \in \gamma$ y $x \in \mathbb{Q}$ tal que $y < x$. Demostraremos que $x \in \gamma$.
$y \in \gamma$ implica que existe $\alpha \in S$ tal que $y \in \alpha$, y por ser α cortadura, se debe tener $x \in \alpha$. Por lo tanto $x \in \gamma$.
(3) γ no tiene mínimo. Dado cualquier $x \in \gamma$, como $x \in \alpha$ para alguna $\alpha \in S$ y por ser α cortadura, existe $y \in \alpha$ tal que $y < x$. Por lo tanto $y \in \gamma$ y $y < x$, lo que significa que γ no tiene mínimo.

γ es el ínfimo de S:

(1) γ es cota inferior de S. Por la definición de γ, $\alpha \subseteq \gamma$ para toda $\alpha \in S$, lo que significa $\gamma \leq \alpha$ para toda $\alpha \in S$.
(2) Si δ es un cota inferior de S, entonces $\delta \leq \alpha$ para toda $\alpha \in S$, que es, $\alpha \subseteq \delta$ para toda $\alpha \in S$, por lo que $\gamma = \bigcup_{\alpha \in S} \alpha \subseteq \delta$ y así $\delta \leq \gamma$.

■

Una propiedad muy importante de los campos ordenados completos es la *propiedad Arquimediana* cuya definición damos a continuación.

Definición 11.2.12. *Un campo ordenado K es* ***Arquimediano*** *si dado $x \in K$, existe $n \in \mathbb{N}$ tal que $x < n$.*

Algunas propiedades de los campos Arquimedianos son las siguientes.

Proposición 11. 2.13. *Sea K un campo Arquimediano. Para cualesquiera $x, y \in K$ tales que $x, y > 0$, si $y - x > 1$ entonces existe $n \in \mathbb{N}$ tal que $x < n < y$.*

Demostración. Como K es Arquimediano, existe $m \in \mathbb{N}$ tal que $x < m$. Sea n el mínimo número natural tal que $x < n$. La minimalidad de n implica que $n - 1 \leq x$. Por hipótesis $1 < y - x$, así que sumando las dos desigualdades obtenemos $n = (n-1) + 1 < x + (y - x) = y$. Por lo tanto $x < n < y$. ■

Teorema 11.2.14. *Si un campo K es Arquimediano, entonces dados $x, y \in K$ con $x < y$, existe $r \in \mathbb{Q}$ tal que $x < r < y$.*

Demostración. Haremos la demostración por los casos que resultan al considerar dónde está colocado 0 respecto a x y y. Estos son cinco casos: caso 1: $0 < x < y$, caso 2: $0 = x < y$, caso 3: $x < 0 < y$, caso 4: $x < y = 0$, caso 5: $x < y < 0$. Como los casos 4 y 5 se reducen a los casos 2 y 1 respectivamente ($0 = -y < -x$ y $0 < -y < -x$) basta demostrar los primeros 3.
Caso 1: $0 < x < y$. Debido a que K es arquimediano, existe $m \in \mathbb{N}$, $m > 0$ tal que $\frac{1}{y-x} < m$ y por ser $y - x > 0$, entonces $my - mx > 1$, donde $mx, my > 0$. Por la proposición 11.2.13, existe $n \in \mathbb{N}$ tal que $mx < n < my$, por lo que para $r = \frac{n}{m} \in \mathbb{Q}$ se tiene que $x < \frac{n}{m} < y$.
Caso 2: $0 = x < y$. Por ser K Arquimediano, existe $n \in \mathbb{N}$ tal que $\frac{1}{y} < n$ y como $y > 0$, entonces para $r = \frac{1}{n} \in \mathbb{Q}$ se tiene que $0 < \frac{1}{n} < y$.
Caso 3: $x < 0 < y$. Esto es trivial, pues basta tomar $r = 0 \in \mathbb{Q}$. ■

Los campos ordenados completos son Arquimedianos como lo muestra el siguiente teorema.

Teorema 11.2.15. *Todo campo ordenado completo es Arquimediano.*

Demostración. Supongamos que K no es Arquimediano. Entonces existe $x \in K$ tal que $n < x$ para toda $n \in \mathbb{N}$, por lo que x es una cota superior de $\mathbb{N}$

y por ser K completo, entonces $\mathbb{N}$ tiene supremo que denotamos por x_0. Esto significa que $x_0 - 1$ ya no es cota superior de $\mathbb{N}$, por lo que existe $m \in \mathbb{N}$ tal que $x_0 - 1 < m$, es decir, $x_0 < m + 1$ donde $m + 1 \in \mathbb{N}$ contradiciendo el hecho de que x_0 es cota superior de $\mathbb{N}$. Por lo tanto K debe ser Arquimediano. ∎

Corolario 11.2.16. *$\mathbb{R}$ es un campo Arquimediano.*

Introducimos ahora las definiciones de isomorfismo de campos y de funciones que preservan el orden para posteriormente presentar el teorema sobre la "unicidad" de $\mathbb{R}$ como campo ordenado completo.

Definición 11.2.17. *Sean K y L campos y $\psi : K \longrightarrow L$ una función. Se dirá que ψ es un* **isomorfismo** *de campos si ψ es biyectiva , $\psi(x + y) = \psi(x) + \psi(y)$ y $\psi(x \cdot y) = \psi(x) \cdot \psi(y)$ para cualesquiera $x, y \in K$. En este caso se dirá que K y L son isomorfos.*

Definición 11.2.18. *Sean K y L campos ordenados y $\psi : K \longrightarrow L$ una función. Se dirá que ψ preserva el orden si y sólo si para cualesquiera $x, y \in K$, $x < y$ implica $\psi(x) < \psi(y)$.*

Nota 11.2.19. Obsérvese que en la definición 11.2.18 la afirmación $x < y$ implica $\psi(x) < \psi(y)$ es equivalente a la afirmación $x < y$ si y sólo si $\psi(x) < \psi(y)$.

Nota 11.2.20. Cualquier función $\psi : K \longrightarrow L$ entre campos ordenados que preserva el orden es inyectiva (ya que cualesquiera dos elementos son comparables mediante el orden).

Algunas propiedades de los isomorfismos de campos son los siguientes

Proposición 11.2.21. *Sea $\psi : K \longrightarrow L$ una función entre dos campos K y L.*
(1) Si $\psi(x + x') = \psi(x) + \psi(x')$ para cualesquiera $x, x' \in K$, entonces $\psi(0) = 0$ y $\psi(-x) = -\psi(x)$ para todo $x \in K$.
(2) Si $\psi(1) \neq 0$ y $\psi(x \cdot x') = \psi(x) \cdot \psi(x')$ para cualesquiera $x, x' \in K$, entonces $\psi(1) = 1$ y $\psi(x^{-1}) = \psi(x)^{-1}$ para todo $x \in K$.

Demostración.

(1) Como $0 + \psi(0) = \psi(0 + 0) = \psi(0) + \psi(0)$, sumando a ambos lados el inverso aditivo de $\psi(0)$, obtenemos que $\psi(0) = 0$. Ahora, utilizando este resultado y que $x + (-x) = 0$, tenemos que

$$0 = \psi(0) = \psi(x + (-x)) = \psi(x) + \psi(-x).$$

Por lo tanto $\psi(-x) = -\psi(x)$.

(2) Ya que $1\cdot\psi(1) = \psi(1\cdot 1) = \psi(1)\cdot\psi(1)$ y por ser $\psi(1) \neq 0$ por hipótesis, entonces multiplicando por el inverso multiplicativo de $\psi(1)$ obtenemos que $\psi(1) = 1$. Por otro lado, si $x \neq 0$, entonces $x \cdot x^{-1} = 1$ y así

$$\psi(x) \cdot \psi\left(x^{-1}\right) = \psi(x \cdot x^{-1}) = \psi(1) = 1$$

con lo que concluimos que $\psi(x) \neq 0$ y que $\psi(x^{-1})$ es el inverso multiplicativo de $\psi(x)$, es decir, $\psi(x^{-1}) = \psi(x)^{-1}$. ∎

Teorema 11.2.22. *Sea K un campo ordenado y sean A y B subconjuntos no vacíos de K que tienen supremo (ínfimo). Entonces*

(1) $S = \{x + y \mid x \in A \text{ y } \in B\}$ tiene supremo (ínfimo) y $\sup S = \sup A + \sup B$ ($\text{ínf}\, S = \text{ínf}\, A + \text{ínf}\, B$).

(2) Si todos los elementos de A y B son positivos, entonces

$$T = \{x \cdot y \mid x \in A \text{ y } \in B\}$$

tiene supremo (ínfimo) y $\sup T = \sup A \cdot \sup B$ ($\text{ínf}\, T = \text{ínf}\, A \cdot \text{ínf}\, B$).

Demostración. Sean $x_0 = \sup A$ y $y_0 = \sup B$.

(1) Mostraremos que $x_0 + y_0 = \sup S$. Para cualesquiera $x \in A$, $y \in B$ se tiene que $x \leq x_0$ y $y \leq y_0$, por lo que $x + y \leq x_0 + y_0$ y por lo tanto $x_0 + y_0$ es cota superior. Sea ahora $z \in K$ una cota superior de S. Entonces para cada $x \in A$, $y \in B$, $x + y \leq z$ implica $y \leq z - x$ para toda $y \in B$, por lo que $y_0 \leq z - x$, es decir, $x \leq z - y_0$, Como esta desigualdad es cierta para toda $x \in A$, entonces $x_0 \leq z - y_0$ por lo que $x_0 + y_0 \leq z$ y por lo tanto $\sup S = x_0 + y_0 = \sup A + \sup B$.

(2) Mostraremos que $x_0 \cdot y_0$ es el supremo de T. Como $0 < x \leq x_0$ y $0 < y \leq y_0$ para cualesquiera $x \in A$, $y \in B$, entonces $0 < x \cdot y \leq x_0 \cdot y_0$ para cualesquiera $x \in A$, $y \in B$, así que $x_0 \cdot y_0$ es una cota superior de T. Ahora si z es una cota superior de T, entonces $x \cdot y \leq z$ para cualesquiera $x \in A$, $y \in B$. Fijando una $x \in A$ y por ser $x > 0$, tenemos que $y \leq \frac{z}{x}$ para toda $y \in B$ y por lo tanto $y_0 \leq \frac{z}{x}$ para toda $x \in A$, por lo que $x_0 \leq \frac{z}{y_0}$, esto es, $x_0 \cdot y_0 \leq z$. Concluimos entonces que $x_0 \cdot y_0$ es el supremo de T.

Por último, los correspondientes resultados para ínfimos se demuestran de manera análoga y se deja como el ejercicio 11.2.4. ∎

Lema 11.2.23. *Sea K un campo ordenado completo y para cada $x \in K$, sean*

$$K_x = \{r \in \mathbb{Q} \mid r < x\} \text{ y } K^x = \{r \in \mathbb{Q} \mid x < r\}.$$

Entonces $x = \sup K_x = \text{ínf } K^x$.

Demostración. Claramente x es cota superior de K_x. Veamos que es la mínima. Como K_x está acotado superiormente y por ser K completo, K_x tiene supremo en K que denotamos por x_0. Entonces $x_0 \leq x$. Pero si fuera $x_0 < x$, como K es Arquimediano por el teorema 11.2.15, entonces existe $s \in \mathbb{Q}$ tal que $x_0 < s < x$ (teorema 11.2.14), por lo que $s \in K_x$. Sin embargo esto contradice que x_0 es el supremo de K_x y por lo tanto $x = x_0 = \sup K_x$. Análogamente se demuestra que $x = \text{ínf } K^x$. ∎

Lema 11.2.24. *Sea K un campo ordenado completo y $x, x' \in K$. Entonces*

(1) $\{r \in \mathbb{Q} \mid r < x + x'\} = \{s + t \in \mathbb{Q} \mid s, t \in \mathbb{Q}, s < x \text{ y } t < x'\}$.
(2) Si $x > 0$ *y* $x' > 0$, *entonces*

$$\{r \in \mathbb{Q} \mid x \cdot x' < r\} = \{s \cdot t \in \mathbb{Q} \mid s, t \in \mathbb{Q}, x < s \text{ y } x' < t\}.$$

Demostración.

(1) Es claro que $\{s + t \in \mathbb{Q} \mid s, t \in \mathbb{Q}, s < x \text{ y } t < x'\} \subseteq \{r \in \mathbb{Q} \mid r < x + x'\}$. Sea $r \in \mathbb{Q}$ tal que $r < x + x'$. Como K es Arquimediano, dadas $r - x' < x$, existe $s \in \mathbb{Q}$ tal que $r - x' < s < x$. Entonces $r - s < x'$ y por lo tanto $r = s + (r - s)$, donde $s, r - s \in \mathbb{Q}$, $s < x$ y $r - s < x'$. Luego $r \in \{s + t \in \mathbb{Q} \mid s < x \text{ y } t < x'\}$.
(2) $\{s \cdot t \in \mathbb{Q} \mid s, t \in \mathbb{Q}, x < s \text{ y } x' < t\} \subseteq \{r \in \mathbb{Q} \mid x \cdot x' < r\}$ es inmediato ya que $0 < x < s$ y $0 < x' < t$ implica $x \cdot x' < s \cdot t$. Ahora, si $r \in \mathbb{Q}$ con $x \cdot x' < r$, por ser $x' > 0$, entonces $x < \frac{r}{x'}$ y como K es Arquimediano, existe $s \in \mathbb{Q}$ tal que $x < s < \frac{r}{x'}$. Entonces $r = s \cdot \frac{r}{s}$, donde $s, \frac{r}{s} \in \mathbb{Q}$, $x < s$ y $x' < \frac{r}{s}$. ∎

Recordamos que para cualquier campo ordenado K, podemos suponer $\mathbb{Q} \subseteq K$ (véase la página 363). Teniendo en cuenta esta observación, cuando estamos trabajando con un campo ordenado K y nos referimos al supremo o ínfimo de algún subconjunto S de $\mathbb{Q}$ en el campo ordenado K, denotaremos a estos $\mathbf{sup}_K\, S$ o $\mathbf{inf}_K\, S$ respectivamente.
Estamos ya en condiciones de demostrar la "unicidad" de $\mathbb{R}$ como campo ordenado completo (salvo isomorfismos).

Teorema 11.2.25. *Sean K y L campos ordenados completos. Entonces existe un único isomorfismo de campos $\psi : K \longrightarrow L$ que preserva el orden y tal que $\psi(r) = r$ para todo $r \in \mathbb{Q}$.*

Demostración. Definimos $\psi : K \longrightarrow L$ por $\psi(x) = \sup_L\{r \in \mathbb{Q} \mid r < x\}$. Entonces

1°/ ψ está bien definida, esto es, el supremos de $\{r \in \mathbb{Q} \mid r < x\}$ existe en L, ya que dado $x \in K$, por ser K Arquimediano (teorema 11.2.15), existe $n \in \mathbb{N}$ tal que $x \leq n$ y por lo tanto n es una cota superior de $\{r \in \mathbb{Q} \mid r < x\}$ en L, y por ser L completo existe el supremo de este conjunto en L.

2°/ $\psi(s) = s$ para todo $s \in \mathbb{Q}$. Dado $s \in \mathbb{Q}$, como $s \in L$, entonces se tiene que $\psi(s) = \sup_L\{r \in \mathbb{Q} \mid r < s\} = s$, donde la primera igualdad se da por la definición de ψ y la segunda por el lema 11.2.23. Por lo tanto $\psi(s) = s$.

3°/ ψ preserva el orden. Sea $x < y$ en K. Usando dos veces el teorema 11.2.14, existen $t, s \in \mathbb{Q}$ tales que $x < t < s < y$. Entonces, debido a que $t \in \mathbb{Q}$, t es una cota superior de $\{r \in \mathbb{Q} \mid r < x\}$ en L y por lo tanto $\psi(x) \leq t$. Por lo tanto, como $s \in \{r \in \mathbb{Q} \mid r < y\}$, se tiene que $s \leq \psi(y)$. Concluimos entonces que $\psi(x) \leq t < s \leq \psi(y)$.

4°/ ψ es biyectiva. ψ es inyectiva debido a que ψ preserva el orden (Nota 11.2.20), así que sólo nos resta probar que ψ es suprayectiva. Sea $y \in L$. Por el lema 11.2.23, $y = \sup_L\{r \in \mathbb{Q} \mid r < y\}$. Consideramos entonces $x \in K$ tal que $x = sup_K\{r \in \mathbb{Q} \mid r < y\}$ (véase ejercicio 11.2.7). Demostraremos que $\psi(x) = y$. Nuevamente, recurriendo al lema 11.2.23, sabemos que x también satisface $x = \sup_K\{r \in \mathbb{Q} \mid r < x\}$. Bastará demostrar que

$$\{r \in \mathbb{Q} \mid r < y\} = \{r \in \mathbb{Q} \mid r < x\} :$$

$\subseteq$) Sea $s \in \{r \in \mathbb{Q} \mid r < y\}$ y sea $t \in \mathbb{Q}$ tal que $s < t < y$. Como $x = \sup_K\{r \in Q \mid r < y\}$, entonces $t \leq x$, por lo que $s < t \leq x$, esto es $s < x$ y de aquí $s \in \{r \in \mathbb{Q} \mid r < x\}$.

$\supseteq$) Sea $s \in \{r \in \mathbb{Q} \mid r < x\}$ y supongamos que $y \leq s$. Entonces $s \in \mathbb{Q}$ es cota superior de $\{r \in \mathbb{Q} \mid r < y\}$ en K y cuyo supremo en K es x. Por lo tanto $x \leq s$ lo que contradice la manera de tomar s y por lo tanto debe ser $s < y$.

Finalmente, $\psi(x) = \sup_L\{r \in \mathbb{Q} \mid r < x\} = \sup_L\{r \in \mathbb{Q} \mid r < y\} = y$. Luego ψ es suprayectiva.

5°/ ψ es un isomorfismo de campos. Ya hemos demostrado que ψ es biyectiva, así que sólo queda demostrar que

$$\psi(x + y) = \psi(x) + \psi(y) \text{ y } \psi(x \cdot y) = \psi(x) \cdot \psi(y).$$

Sean $x, x' \in K$. Recordamos que por (1) del lema 11.2.24,

$$\{r \in \mathbb{Q} \mid r < x + x'\} = \{s + t \in \mathbb{Q} \mid s, t \in \mathbb{Q},\ s < x,\ t < x'\}.$$

Entonces

$$\begin{aligned}
\psi(x + x') &= \sup_L\{r \in \mathbb{Q} \mid r < x + x'\} \\
&= \sup_L\{s + t \in \mathbb{Q} \mid s, t \in \mathbb{Q},\ s < x,\ t < x'\} \\
&= \sup_L\{r \in \mathbb{Q} \mid s < x\} + \sup_L\{t \in \mathbb{Q} \mid t < x'\} \\
&= \psi(x) + \psi(x')
\end{aligned}$$

donde la penúltima igualdad se da por el teorema 11.2.22.
Para el caso del producto, demostraremos que $\psi(x \cdot x') = \psi(x) \cdot \psi(x')$ para $x > 0$ y $x' > 0$ y los casos restantes se obtendrán a partir de éste. Supongamos entonces que $x > 0$ y $x' > 0$. Por el ejercicio 11.2.8, para toda $x \in K$,

$$\sup_L\{r \in \mathbb{Q} \mid r < x\} = \inf_L\{r \in \mathbb{Q} \mid x < r\}.$$

Entonces

$$\begin{aligned}
\psi(x \cdot x') &= \sup_L\{r \in \mathbb{Q} \mid r < x \cdot x'\} \\
&= \inf_L\{r \in \mathbb{Q} \mid x \cdot x' < r\} \\
&= \inf_L\{s \cdot t \in \mathbb{Q} \mid s, t \in \mathbb{Q}\ x < s,\ x' < t\} \\
&= \inf_L\{s \in \mathbb{Q} \mid x < s\} \cdot \inf_L\{t \in \mathbb{Q} \mid x' < t\} \\
&= \sup_L\{s \in \mathbb{Q} \mid x < s\} \cdot \sup_L\{t \in \mathbb{Q} \mid x' < t\} \\
&= \psi(x) \cdot \psi(x').
\end{aligned}$$

Veamos ahora los casos restantes y para esto usamos el hecho de que $\psi(0) = 0$ y $\psi(-x) = -\psi(x)$ (véase proposición 11.2.21 (1)).
Caso $x = 0$ o $x' = 0$. Entonces $\psi(x) = 0$ o $\psi(x') = 0$ y de aquí

$$\psi(x \cdot x') = \psi(0) = 0 = \psi(x) \cdot \psi(x').$$

Caso $x < 0$ y $x' > 0$.

$$-\psi(x \cdot x') = \psi(-(x \cdot x')) = \psi((-x) \cdot x') = \psi(-x) \cdot \psi(x') = -\psi(x) \cdot \psi(x').$$

Por lo tanto $\psi(x \cdot x') = \psi(x) \cdot \psi(x')$.
Caso $x > 0$ y $x' < 0$. Totalmente análogo al caso anterior.
Caso $x < 0$ y $x' < 0$.

$$\psi(x \cdot x') = \psi((-x) \cdot (-x')) = \psi(-x) \cdot \psi(-x') = (-\psi(x)) \cdot (-\psi(x')) = \psi(x) \cdot \psi(x').$$ ∎

Es importante hacer notar que hemos usado con mucha fuerza el hecho de que para cualesquiera dos elementos distintos de un campo ordenado completo, existe siempre un número racional entre ellos (teorema 11.2.14), siendo este resultado

una propiedad de los campos Arquimedianos entre los que están los campos ordenados completos (teorema 11.2.15).

Corolario 11.2.26. *$\mathbb{R}$ es el único campo ordenado completo (salvo isomorfismos)*

Hemos visto que un campo ordenado completo K, $x^2 > 0$ para todo $x \in K$, $x \neq 0$, así que dado cualquier $z \in K$ con $z < 0$, no existe ningún elemento $x \in K$ tal que $x^2 = z$. Sin embargo, para los $z \in K$ tal que $z \geq 0$, no solamente $x^2 = z$ tiene solución en K sino más general, la ecuación $x^m = z$ siempre tiene solución en K para todo número natural $m \geq 1$ y $z \in K$, $z \geq 0$ siendo además esta solución única con la propiedad de ser mayor que 0. Por ser el caso $z = 0$ trivial, no lo incluimos en el siguiente:

Teorema 11.2.27. *Sea K un campo ordenado completo, $z \in K$, $z > 0$ y $m \in \mathbb{N}$, $m > 0$. Entonces existe un único $x \in K$, $x > 0$ tal que $x^m = z$.*

Demostración. Sea $S = \{y \in K \mid y \geq 0,\ y^m < z\}$. Mostraremos que la x buscada es precisamente $x = \sup S$ y para esto lo primero que debemos demostrar es que $S \neq \emptyset$ y que S está acotado superiormente. Si $y = \min\left\{1, \frac{z}{2}\right\}$, entonces $0 < y \leq 1$ y $y \leq \frac{z}{2} < z$ y por lo tanto $y^m = y \cdot y^{m-1} \leq y \cdot 1^{m-1} = y < z$, así que $y \in S$. Para ver que está acotado superiormente consideramos $w \in K$ tal que $w \geq \max\{1, z\}$. Entonces w es cota superior de S ya que $w \geq 1$ y $w \geq z$ y de aquí, $w^m = w \cdot w^{m-1} \geq w \cdot 1^{m-1} = w \geq z$ y así $w^m > y^m$ para toda $y \in S$. Pero esto implica que $w > y$ para toda $y \in S$ (no puede ser $w \leq y$, para alguna $y \in S$ porque de esto se deduce, del ejercicio 11.2.9, que $w^m \leq y^m$). Entonces w es una cota superior de S.

Concluimos entonces, por ser K completo, que S tiene supremo al que denotaremos por x. Primero demostraremos que x satisface las siguientes propiedades obtenidas del hecho de que x es el supremo de S.

(i) $x > 0$. Precisamente el elemento $y \in K$ exhibido para mostrar que $S \neq \emptyset$, es mayor que cero, y por ser x el supremo de S, entonces debe ser $x > 0$.

(ii) Si $0 \leq y < x$, entonces $y^m < z$. Si $0 \leq y < x$, entonces existe $w \in S$ tal que $0 \leq y < w < x$, esto es porque al ser $y < x$, y no puede ser cota superior de S debido a que x es la mínima de ellas. Por lo tanto $y^m < w^m < z$.

(iii) Si $x < w$, entonces $w^m \geq z$. Si $x < w$, entonces $w \notin S$ ya que todo elemento de S es menor o igual a x y por lo tanto $z \leq w^m$.

Afirmamos que $x^m = z$ y para demostrar esta igualdad veremos que suponer $x^m < z$ o $x^m > z$ lleva a una contradicción. Supongamos entonces que $x^m > z$ y sea

$w = \text{máx}\left\{0, x - \frac{x^m - z}{m \cdot x^{m-1}}\right\}$. Entonces $x - \frac{x^m - z}{m \cdot x^{m-1}} \leq w$ y $0 \leq w$ y de aquí se obtiene que $(x - w) \cdot m x^{m-1} \leq x^m - z$. Además $0 \leq w < x$ y por lo tanto, por (*ii*), $w^m < z$. Por otro lado tenemos que

$$\begin{aligned} x^m - w^m &= (x - w)\left(x^{m-1} + x^{m-2}w + x^{m-3}w^2 + \cdots + xw^{m-2} + w^{m-1}\right) \\ &< (x - w)\left(x^{m-1} + x^{m-2} \cdot x + x^{m-3} \cdot x^2 + \cdots + x \cdot x^{m-2} + x^{m-1}\right) \\ &= (x - w)(m \cdot x^{m-1}) \leq \tfrac{x^m - z}{m \cdot x^{m-1}} \cdot (m \cdot x^{m-1}) = x^m - z. \end{aligned}$$

De donde obtenemos que $z < w^m$, lo que es una contradicción. Por lo tanto no puede ser que $x^m > z$. Ahora supongamos que $x^m < z$ y sea $w = \text{mín}\left\{2x, x + \frac{z - x^m}{2^m \cdot x^{m-1}}\right\}$. Claramente,

$$x < w \leq 2x \;\; y \;\; (w - x) \cdot (2^m \cdot x^{m-1}) \leq z - x^m.$$

Por otro lado,

$$\begin{aligned} w^m - x^m &= (w - x)\left(w^{m-1} + w^{m-2} \cdot x + \cdots + w \cdot x^{m-2} + x^{m-1}\right) \\ &\leq (w - x)\left((2x)^{m-1} + (2x)^{m-2} \cdot x + \cdots + 2x \cdot x^{m-2} + x^{m-1}\right) \\ &= (w - x)(2^{m-1} + 2^{m-2} + \cdots + 2 + 1) \cdot x^{m-1} \\ &= (w - x)\left(\tfrac{2^m - 1}{2 - 1}\right) \cdot x^{m-1} \\ &= (w - x)\,(2^m - 1) \cdot x^{m-1} \\ &< (w - x) \cdot 2^m \cdot x^{m-1} \leq z - x^m. \end{aligned}$$

De aquí obtenemos entonces que $w^m < z$, lo que contradice (*iii*) ya que como $x < w$, debe ser $w^m \geq z$.
Por lo tanto se debe cumplir la única posibilidad que queda, que es $x^m = z$.
Por último, x es única, ya que si $y \in K$, $y > 0$, satisface $y^m = z$, entonces $x^m - y^m = 0$ y

$$(x^m - y^m) = (x - y)\left(x^{m-1} + x^{m-2} \cdot y + \cdots + x \cdot y^{m-2} + y^{m-1}\right) = 0.$$

Pero esto implica que $x - y = 0$ o $x^{m-1} + x^{m-2} \cdot y + \cdots + x \cdot y^{m-2} + y^{m-1} = 0$ y como

$$x^{m-1} + x^{m-2} \cdot y + \cdots + x \cdot y^{m-2} + y^{m-1} > 0$$

puesto que $x, y > 0$, entonces debe ser $x = y$. ∎

§ 11.3. Desarrollo decimal

En esta sección asociaremos a cada número real lo que llamaremos su desarrollo decimal, que es una expresión del tipo $A.a_1a_2\cdots a_n\cdots$ donde A es un entero y donde $a_i \in \{0, 1, \ldots, 9\}$ para cada $i = 1, 2, \ldots$. Esto es, la expresión consiste de un número entero al que le sigue un punto y después de éste una sucesión infinita de números naturales, cada uno de ellos entre 0 y 9 y donde excluiremos las expresiones de la forma $A.a_1\cdots a_n 9\cdots 9\cdots$, es decir, no consideraremos expresiones que a partir de alguna n, $a_i = 9$ para toda $i > n$. La correspondencia que daremos entre los número reales y estas expresiones será biyectiva y lo que utilizaremos con fuerza será el hecho de que el orden que se tiene definido en $\mathbb{R}$ es total.
En la demostración del siguiente teorema usaremos el hecho de que $\mathbb{R}$ es un campo Arquimediano (definición 11.2.12 y teorema 11.2.15)

Teorema 11.3.1. *Sea $\alpha \in \mathbb{R}$, $\alpha \geq 0$. Entonces existe $A \in \mathbb{N}$ tal que*

$$A \leq \alpha < A + 1.$$

Demostración. Debido a que $\mathbb{R}$ es arquimediano (pág. 367), dado $\alpha \in \mathbb{R}$, existe $n \in \mathbb{N}$ tal que $\alpha < n$. Si consideramos $T = \{m \in \mathbb{N} | \alpha < m\}$, $T \neq \emptyset$ y por lo tanto tiene mínimo n_0. Entonces, dado que $\alpha \geq 0$, debe ser $n_0 \geq 1$. Luego $n_0 - 1 \in \mathbb{N}$ y por la minimalidad de n_0 se tiene que $n_0 - 1 \leq \alpha$. Esto es, $A = n_0 - 1$ satisface $A \leq \alpha < A + 1$. ∎

Nota 11.3.2. El desarrollo decimal $A.a_1a_2\cdots a_n\cdots$ de un número real $\alpha \geq 0$ se encontrará como sigue:

(i) Existe un numero natural A tal que $A \leq \alpha < A + 1$ (teorema 11.3.1).

(ii) El valor de cada a_n está dada por recursión de la siguiente manera:

(I) Puesto que $A \leq \alpha < A + 1$ y

$$A = A + \frac{0}{10} < A + \frac{1}{10} < A + \frac{2}{10} < \cdots < A + \frac{9}{10} < A + 1,$$

entonces para alguna $a_1 \in \{0, 1, \ldots, 9\}$ se tendrá

$$A + \frac{a_1}{10} \leq \alpha < A + \frac{a_1}{10} + \frac{1}{10} \leq A + 1.$$

(II) Suponiendo que para $n \geq 1$ se tienen definidas

$$a_1, \ldots, a_n \in \{0, 1, \ldots, 9\}$$

tales que

$$A + \frac{a_1}{10} + \cdots + \frac{a_n}{10^n} \leq \alpha < A + \frac{a_1}{10} + \cdots + \frac{a_n}{10^n} + \frac{1}{10^n}$$

definimos a_{n+1}, teniendo en cuenta que

$$\begin{aligned} A + \tfrac{a_1}{10} + \cdots + \tfrac{a_n}{10^n} &< A + \tfrac{a_1}{10} + \cdots + \tfrac{a_n}{10^n} + \tfrac{1}{10^{n+1}} \\ &< A + \tfrac{a_1}{10} + \cdots + \tfrac{a_n}{10^n} + \tfrac{2}{10^{n+1}} \\ &< \cdots < A + \tfrac{a_1}{10} + \cdots + \tfrac{a_n}{10^n} + \tfrac{9}{10^{n+1}} \\ &< A + \tfrac{a_1}{10} + \cdots + \tfrac{a_n}{10^n} + \tfrac{10}{10^{n+1}} \\ &= A + \tfrac{a_1}{10} + \cdots + \tfrac{a_n}{10^n} + \tfrac{1}{10^n} \end{aligned}$$

entonces para alguna $a_{n+1} \in \{0, 1, \ldots, 9\}$,

$$A + \frac{a_1}{10} + \cdots + \frac{a_n}{10^n} + \frac{a_{n+1}}{10^{n+1}} \leq \alpha < A + \frac{a_1}{10} + \cdots + \frac{a_n}{10^n} + \frac{a_{n+1} + 1}{10^{n+1}}$$

Luego de (i) y (ii), dado $\alpha \in \mathbb{R}$, $\alpha \geq 0$, se tienen determinados $A \in \mathbb{N}$ y para cada número natural $n \geq 1$, un número $a_n \in \{0, 1, \ldots, 9\}$.

Definición 11.3.3. *Dado un número real $\alpha \geq 0$, su desarrollo decimal es la expresión $A.a_1a_2 \ldots a_n \ldots$, donde $A, a_1, a_2, \ldots, a_n, \ldots$ están determinados por la nota 11.3.2. Dos desarrollos decimales $A.a_1a_2 \ldots a_n \ldots$ y $B.b_1b_2 \ldots b_n \ldots$ serán distintos si $A \neq B$ o existe $i = 1, 2, \ldots, n \ldots$ tal que $a_i \neq b_i$.*

Como mencionamos al principio de esta sección, excluimos las expresiones del tipo $A.a_1 \ldots a_n 9 \ldots 9 \ldots$, así que para demostrar que la correspondencia entre números reales $\alpha \geq 0$ y lo que hemos llamado su desarrollo decimal, debemos ver que con el proceso dado en la nota 11.3.2 la expresión correspondiente a α no puede ser de la forma $A.a_1 \ldots a_n 9 \ldots 9 \ldots$. Antes de demostrarlo necesitamos el siguiente

Lema 11.3.4. *Sea $\alpha \in \mathbb{R}$, $\alpha > 0$. Entonces existe $m \in \mathbb{N}$, $m \geq 1$ tal que $\frac{1}{10^m} < \alpha$.*

Demostración. Supongamos que para toda $m \in \mathbb{N}$,$m \geq 1$, $\alpha \leq \frac{1}{10^m}$ y consideremos $r \in \mathbb{Q}$ tal que $0 < r < \alpha$ (teorema 11.1.25). Sea $r = \frac{a}{b}$, donde $a, b \in \mathbb{Z}$ y $a > 0$, $b > 0$. Entonces $r = \frac{a}{b} < \frac{1}{10^m}$ para toda $m \in \mathbb{N}$, $m \geq 1$. Luego $10^m a < b$. Por el teorema 7.1.13, $a = a_k 10^k + \cdots + a_1 10 + a_0$ y $b = b_j 10^j + \cdots + b_1 10 + b_0$ donde $a_i, b_l \in \{0, 1, \ldots, 9\}$ para toda $i = 0, \ldots, k$ y $l = 0, \ldots, j$, $a_k \neq 0$ y $b_j \neq 0$ y sustituyendo estas igualdades obtenemos que $10^m(a_k 10^k + \cdots + a_1 10 + a_0) < b_j 10^j + \cdots + b_1 10 + b_0$. Entonces

$$\begin{aligned} 10^{m+k} &\leq 10^m(a_k 10^k + \ldots + a_1 10 + a_0) \\ &= a_k 10^{m+k} + \ldots + a_{m+1}10 + a_0 10^m \\ &< b_j 10^j + \cdots + b_1 10 + b_0 \\ &\leq 9(10^j + \cdots + 10 + 1) \\ &= 9 \cdot \tfrac{10^{j+1}-1}{10-1} \\ &= 10^{j+1} - 1. \end{aligned}$$

Siendo esta desigualdad válida para toda $m \geq 1$, en particular se tiene que para $m = j + 1$, $10^{j+1+k} \leq 10^{j+1} - 1$ lo cual es una contradicción. Por lo tanto para alguna $m \geq 1$, debe ser $\frac{1}{10^m} < r < \alpha$. ∎

Notación 11.3.5*. Si una expresión $A.a_1 \cdots a_n \cdots$ es tal que a partir de cierta $m \geq 1$, cierto bloque de R dígitos se repite continuamente uno tras otro, es decir, la expresión es de la forma*

$$A.a_1 \cdots a_m a_{m+1} \cdots a_{m+k} a_{m+1} \cdots a_{m+k} a_{m+1} \cdots$$

la denotaremos por $A.a_1 \cdots a_m \overbrace{a_{m+1} \cdots a_{m+k}}$, donde el arco encima de esos dígitos $a_{m+1} \cdots a_{m+k}$ indicará que a partir de ahí este bloque se repite indefinidamente, uno tras otro. A este tipo de expresiones les llamaremos ***periódicas*** *con periodo $a_{m+1} \cdots a_{m+k}$.*
Con esta notación, la expresión $A.a_1 \cdots a_m \widehat{9}$ significa $A.a_1 \cdots a_m 9 \cdots 9 \cdots$ (en este caso $k = 1$).

Proposición 11.3.6*. El desarrollo decimal de un número real $\alpha \geq 0$ no puede ser de la forma $A.a_1 a_2 \cdots a_n \widehat{9}$.*

Demostración. Basta suponer que $\alpha \geq 0$ ya que el desarrollo decimal de cero es $0{,}0 \ldots 0 \cdots = 0.\widehat{0}$.
Supongamos que el desarrollo decimal de α es $A.a_1 \ldots a_n \widehat{9}$, donde $a_n \neq 9$. Entonces para todo número natural $k \geq 1$ se tiene que

$$A + \frac{a_1}{10} + \cdots + \frac{a_n}{10^n} + \frac{9}{10^{n+1}} + \cdots + \frac{9}{10^{n+k}} < \alpha < A + \frac{a_1}{10} + \cdots + \frac{a_n}{10^n} + \frac{9}{10^{n+1}} + \cdots + \frac{9}{10^{n+k-1}} + \frac{9+1}{10^{n+k}}$$

Pero

$$\begin{aligned} A + \tfrac{a_1}{10} + \cdots + \tfrac{a_n}{10^n} + \tfrac{9}{10^{n+1}} + \cdots + \tfrac{9}{10^{n+k-1}} + \tfrac{9+1}{10^{n+k}} &= A + \tfrac{a_1}{10} + \cdots + \tfrac{a_n}{10^n} + \tfrac{9}{10^{n+1}} + \cdots + \tfrac{9}{10^{n+k-1}} + \tfrac{1}{10^{n+k-1}} \\ &\vdots \\ &= A + \tfrac{a_1}{10} + \cdots + \tfrac{a_n+1}{10^n} \end{aligned}$$

Luego $A + \frac{a_1}{10} + \cdots + \frac{a_n}{10^n} + \frac{9}{10^{n+1}} + \cdots + \frac{9}{10^{n+k}} < \alpha < A + \frac{a_1}{10} + \cdots + \frac{a_n+1}{10^n}$.
Obsérvese que la desigualdad de la izquierda es estricta ya que si se diera la igualdad, el desarrollo decimal de α sería $A.a_1 \ldots a_n 9 \ldots 90 \ldots 0 \ldots$ que no es el caso.
Por otro lado se tiene que

$$\begin{aligned}
A + \tfrac{a_1}{10} + \cdots + \tfrac{a_n}{10^n} + \tfrac{9}{10^{n+1}} + \cdots + \tfrac{9}{10^{n+k}} &= A + \tfrac{a_1}{10} + \cdots + \tfrac{a_n}{10^n} + 9\left(\tfrac{1}{10^{n+1}} + \cdots + \tfrac{1}{10^{n+k}}\right) \\
&= A + \tfrac{a_1}{10} + \cdots + \tfrac{a_n}{10^n} + 9\left(\tfrac{10^{k-1}+\cdots+10+1}{10^{n+k}}\right) \\
&= A + \tfrac{a_1}{10} + \cdots + \tfrac{a_n}{10^n} + \tfrac{9}{10^{n+k}}\left(10^{k-1} + \cdots + 10 + 1\right) \\
&= A + \tfrac{a_1}{10} + \cdots + \tfrac{a_n}{10^n} + \tfrac{9}{10^{n+k}}\left(\tfrac{10^k-1}{10-1}\right) \\
&= A + \tfrac{a_1}{10} + \cdots + \tfrac{a_n}{10^n} + \tfrac{10^k-1}{10^{n+k}} \\
&= A + \tfrac{a_1}{10} + \cdots + \tfrac{a_n+1}{10^n} - \tfrac{1}{10^{n+k}}
\end{aligned}$$

Entonces para toda $k \geq 1$, $A + \frac{a_1}{10} + \cdots + \frac{a_n+1}{10^n} - \frac{1}{10^{n+k}} < \alpha < A + \frac{a_1}{10} + \cdots + \frac{a_n+1}{10^n}$ y por lo tanto, restando $S = A + \frac{a_1}{10} + \cdots + \frac{a_n+1}{10^n}$ obtenemos $-\frac{1}{10^{n+k}} < \alpha - S < 0$, lo cual implica que $0 < S - \alpha < \frac{1}{10^{n+k}} < \frac{1}{10^k}$ para todo $k \geq 1$, contradiciendo así el lema 11.3.4. ∎

Teorema 11.3.7. *Si α y β son números reales no negativos y $\alpha \neq \beta$, entonces α y β tienen desarrollos decimales distintos.*

Demostración. Supongamos $\alpha < \beta$ y supongamos que α y β tienen el mismo desarrollo decimal $A.a_1a_2 \cdots a_n \cdots$. Entonces

$$A + \frac{a_1}{10} + \cdots + \frac{a_n}{10^n} \leq \alpha < A + \frac{a_1}{10} + \cdots + \frac{a_n+1}{10^n}$$

y

$$A + \frac{a_1}{10} + \cdots + \frac{a_n}{10^n} \leq \beta < A + \frac{a_1}{10} + \cdots + \frac{a_n+1}{10^n}$$

para toda $n \in \mathbb{N}$, $n \geq 1$. De estas desigualdades se obtiene que

$$0 < \beta - \alpha < \left(A + \frac{a_1}{10} + \cdots + \frac{a_n+1}{10^n}\right) - \left(A + \frac{a_1}{10} + \cdots + \frac{a_n}{10^n}\right) = \frac{1}{10^n}$$

para toda $n \in \mathbb{N}$, lo que contradice el lema 11.3.4. Por lo tanto α y β deben tener desarrollos distintos. ∎

Lema 11.3.8. *Dado $A \in \mathbb{Z}$, $A \geq 0$, $a_i \in \{0, 1, \ldots, 9\}$ para $i = 1, 2, \ldots$,*

$$A + \frac{a_1}{10} + \cdots + \frac{a_m}{10^m} < A + \frac{a_1}{10} + \cdots + \frac{a_n+1}{10^n}$$

para cualesquiera $n, m \in \mathbb{N} - \{0\}$.

Demostración. Si $m \leq n$ es inmediato, así que supongamos $m > n$. En este caso se tiene que

$$A + \tfrac{a_1}{10} + \cdots + \tfrac{a_m}{10^m} < A + \tfrac{a_1}{10} + \cdots + \tfrac{a_n+1}{10^n} \text{ si y sólo si } \tfrac{a_{n+1}}{10^{n+1}} + \cdots + \tfrac{a_m}{10^m} < \tfrac{1}{10^n}$$

así que demostraremos esta última desigualdad.

$$\begin{aligned} \tfrac{a_{n+1}}{10^{n+1}} + \cdots + \tfrac{a_m}{10^m} &\leq 9\left(\tfrac{1}{10^{n+1}} + \cdots + \tfrac{1}{10^m}\right) \\ &= \tfrac{9}{10^m}\left(10^{m-(n+1)} + \cdots + 1\right) \\ &= \tfrac{9}{10^m}\left(\tfrac{10^{m-n}-1}{10-1}\right) \\ &= \tfrac{1}{10^n} - \tfrac{1}{10^m} \\ &< \tfrac{1}{10^n}. \blacksquare \end{aligned}$$

Teorema 11.3.9*. La correspondencia entre los números reales no negativos y las expresiones $A.a_1a_2\cdots a_n\cdots$, donde $A \in \mathbb{Z}$, $A \geq 0$ $a_i \in \{0, 1, \ldots, 9\}$ para toda $i = 1, 2, \ldots$ y que no son de la forma $A.a_1a_2\cdots a_n\overline{9}$, es suprayectiva.*

Demostración. Consideremos $A.a_1a_2\cdots a_n\cdots$ distinta de $A.a_1\ldots a_m\overline{9}$, donde $A \in \mathbb{Z}$, $A \geq 0$ y $a_i \in \{0, 1, \ldots, 9\}$ para toda $i = 1, 2, \ldots$. Encontraremos un número real α cuyo desarrollo decimal es $A.a_1a_2\cdots a_n\cdots$.

Sea $X = \{r \in \mathbb{Q} \mid A + \frac{a_1}{10} + \cdots \frac{a_n}{10^n} < r$ para toda $n = 1, 2, \ldots\}$. Por el lema 11.3.8, $X \neq \emptyset$ ya que para toda $m \geq 1$,

$$A + \frac{a_1}{10} + \cdots + \frac{a_m}{10^m} < A + \frac{a_1 + 1}{10} \leq A + \frac{9 + 1}{10} = A + 1 \in \mathbb{Q},$$

así que $A + 1 \in X$.

Como A es cota inferior de X, por el teorema 11.2.11, X tiene ínfimo que denotamos por B. Sea $\alpha = X - \{B\}$. Afirmamos que α es el número real buscado. Para mostrar esto debemos probar que α es una cortadura y que $A + \frac{a_1}{10} + \cdots \frac{a_n}{10^n} \leq \alpha < A + \frac{a_1}{10} + \cdots \frac{a_n+1}{10^{n+1}}$ para toda $n = 1, 2, \ldots$.

α es una cortadura

(1) $\emptyset \neq \alpha \subsetneq \mathbb{Q}$ ya que $A + 1 \in \alpha$ y $A \notin \alpha$.
(2) Si $r \in \alpha$ y $s \in \mathbb{Q}$ tal que $s > r$, evidentemente, $s \in \alpha$.
(3) α no tiene mínimo. Si α tuviera mínimo $r_0 \in \mathbb{Q}$, entonces $r_0 \leq x$ para toda $x \in \alpha$. Pero siendo B el ínfimo de X, entonces $B \leq r_0$. Ahora, como

$r_0 \in \alpha = X - \{B\}$, entonces $r_0 \neq B$. Luego $B < r_0$ y por el teorema 11.1.25, existe $s \in \mathbb{Q}$ tal que $B < s < r_0$, contradiciendo que B es el ínfimo de X.

Como B es el ínfimo de X, por un lado se tiene que $A + \frac{a_1}{10} + \cdots \frac{a_n}{10^n} \leq B$ para cada $n = 1, 2, \ldots$ ya que $A + \frac{a_1}{10} + \cdots \frac{a_n}{10^n}$ es cota inferior para toda $n = 1, 2, \ldots$ y por el otro lado $B < t$ para toda $t \in \alpha$.

Sea $r \in \alpha$. Entonces por lo expuesto en el párrafo anterior, $B < r$ y por el teorema 11.1.25, existe $s \in \mathbb{Q}$ tal que $B < s < r$ y debido a que $A + \frac{a_1}{10} + \cdots \frac{a_n}{10^n} \leq B$ para toda $n = 1, 2, \ldots$, se tiene que $s \in \alpha$. Hemos demostrado que dado $r \in \alpha$, existe $s \in \alpha$ tal que $s < r$ y por lo tanto α no puede tener mínimo.

El desarrollo decimal de α es $A + \frac{a_1}{10} + \cdots \frac{a_n}{10^n} \cdots$.

Demostraremos que para cada $n \in \mathbb{N}$ y $n \geq 1$

$$A + \frac{a_1}{10} + \cdots \frac{a_n}{10^n} \leq \alpha < A + \frac{a_1}{10} + \cdots \frac{a_n + 1}{10^n},$$

o lo que es lo mismo,

$$\alpha_{A+\frac{a_1}{10}+\cdots\frac{a_n+1}{10^n}} \subsetneq \alpha \subseteq \alpha_{A+\frac{a_1}{10}+\cdots\frac{a_n}{10^n}}$$

para toda $n = 1, 2, \ldots$.
Si $r \in \alpha$, por la definición de α, $r > A + \frac{a_1}{10} + \cdots \frac{a_n}{10^n}$ así que $r \in \alpha_{A+\frac{a_1}{10}+\cdots\frac{a_n}{10^n}}$. Por lo tanto $\alpha \subseteq \alpha_{A+\frac{a_1}{10}+\cdots\frac{a_n}{10^n}}$. Por otro lado si $r \in \alpha_{A+\frac{a_1}{10}+\cdots\frac{a_{n+1}}{10^n}}$, entonces $r > A + \frac{a_1}{10} + \cdots \frac{a_n+1}{10^n}$ y por el lema 11.3.8, $r > A + \frac{a_1}{10} + \cdots \frac{a_m}{10^m}$ para toda $m \in \mathbb{N} - \{0\}$ y por lo tanto $r \in \alpha$. Además por el mismo lema 11.3.8, $A+\frac{a_1}{10}+\cdots \frac{a_n+1}{10^n} \in \alpha$ y como $A+\frac{a_1}{10}+\cdots \frac{a_n+1}{10^n} \notin \alpha_{A+\frac{a_1}{10}+\cdots\frac{a_n+1}{10^n}}$, entonces $\alpha_{A+\frac{a_1}{10}+\cdots\frac{a_n+1}{10^n}} \subsetneq \alpha$. ∎

Habiendo establecido la correspondencia biyectiva entre los números reales no negativos y las expresiones $A.a_1a_2 \ldots a_n \ldots$ donde $A \in \mathbb{N}$ y $a_i \in \{0, 1, \ldots, 9\}$ para toda $i = 1, 2, \ldots$ que son distintas de la forma $A.a_1a_2 \ldots a_n\widehat{9}$, extendemos esta correspondencia a todos los números reales asociando a cada número real $\alpha < 0$ la expresión $-(A.a_1a_2 \ldots a_n \ldots)$ donde $A.a_1a_2 \ldots a_n \ldots$ es el desarrollo decimal de $-\alpha$ ($-\alpha > 0$). Dentro de estas expresiones se encuentran las que hemos llamado periódicas, es decir, las de la forma $A.a_1a_2 \ldots a_m\widehat{a_{m+1} \ldots a_{m+k}}$ y una pregunta que

nos podemos hacer es la siguiente ¿existe alguna particularidad de aquellos números reales cuyo desarrollo decimal es periódico?. La respuesta es sí. Pretendemos demostrar aquí que un número real tiene desarrollo decimal periódico si y sólo si es un número racional.

Empezamos definiendo fracción decimal:

Definición 11.3.10. *Sea r un número racional no negativo y $A.a_1a_2\ldots a_n\ldots$ su desarrollo decimal. Diremos que r es una* ***fracción decimal*** *si para alguna m, $a_k = 0$ para toda $k > m$.*

El siguiente resultado caracteriza a todos los números racionales no negativos que son fracciones decimales.

Proposición 11.3.11. *Un número racional no negativo r es una fracción decimal si y sólo si existe un número natural m tal que $r = \frac{B}{10^m}$ para algún entero B.*

Demostración.
$\Rightarrow$) Supongamos que $r \geq 0$ es una fracción decimal y que $A.a_1a_2\ldots\widehat{a_m0}$ es su desarrollo decimal. Entonces para toda $k \geq 1$,

$$A + \frac{a_1}{10} + \cdots + \frac{a_m}{10^m} + \frac{0}{10^{m+1}} + \cdots \frac{0}{10^{m+k}} \leq r < A + \frac{a_1}{10} + \cdots + \frac{a_m}{10^m} + \frac{0}{10^{m+1}} + \cdots \frac{1}{10^{m+k}}$$

y por lo tanto

$$0 \leq r - (A + \frac{a_1}{10} + \cdots + \frac{a_m}{10^m} + \frac{0}{10^{m+1}} + \cdots \frac{0}{10^{m+k}}) < \frac{1}{10^{m+k}} < \frac{1}{10^k}$$

para toda $k \geq 1$. Luego por el lema 11.3.4, la única posibilidad para que esto suceda es que

$$r - (A + \frac{a_1}{10} + \cdots + \frac{a_m}{10^m} + \frac{0}{10^{m+1}} + \cdots \frac{0}{10^{m+k}}) = 0,$$

es decir,

$$\begin{aligned} r &= A + \tfrac{a_1}{10} + \tfrac{a_2}{10^2} + \cdots + \tfrac{a_m}{10^m} + \tfrac{0}{10^{m+1}} + \cdots \tfrac{0}{10^{m+k}} \\ &= \tfrac{10^m}{10^m}\left(A + \tfrac{a_1}{10} + \cdots + \tfrac{a_m}{10^m} + \tfrac{0}{10^{m+1}} + \cdots \tfrac{0}{10^{m+k}}\right) \\ &= \tfrac{A\cdot 10^m + a_1\cdot 10^{m-1} + \cdots + a_m}{10^m} = \tfrac{B}{10^m} \end{aligned}$$

$\Rightarrow$) Supongamos que $r = \frac{B}{10^m}$ para algún entero B.
Por el teorema 7.1.13, $B = s_k10^k + \cdots + s_110 + s_0$, donde $s_i \in \{0, 1, \ldots, 9\}$ para cada $i = 0, 1, \ldots, k$

Luego

$$\begin{aligned} r &= \tfrac{B}{10^m} \\ &= \tfrac{s_k\cdot 10^k+\cdot+s_1 10+s_0}{10^m} \\ &= \begin{cases} \frac{s_k}{10^{m-k}}+\cdots+\frac{s_1}{10^{m-1}}+\frac{s_0}{10^m}, & \text{si } k<m \\ \left(s_k 10^{k-m}+\cdots+s_{m+1}10+s_m\right)+\frac{s_{m-1}}{10}+\cdots+\frac{s_0}{10^m}, & \text{si } m\le k \end{cases} \end{aligned}$$

En el primer caso el desarrollo decimal de r es $0{,}0\ldots0s_k\ldots s_1\widehat{s_00}$ y en el segundo es $A.s_{m-1}\ldots\widehat{s_00}$ donde $A=s_k10^{k-m}+\cdots+s_{m+1}10+s_m$. ∎

Lema 11.3.12. *Sea $\alpha\in\mathbb{R}$, $\alpha\ge 0$ y $A.a_1\ldots a_n\ldots$ su desarrollo decimal. Entonces*

(1) Para todo entero no negativo B, el desarrollo decimal de $\alpha+B$ es $(A+B).a_1\cdots a_n\cdots$ y si $B\le A$, el desarrollo decimal de $\alpha-B$ es $(A-B).a_1\ldots a_n\ldots$.

(2) Para todo $m\ge 1$ el desarrollo decimal de $10^m\alpha$ es $B.a_{m+1}\cdots a_{m+k}\cdots$, donde $B=10^mA+10^{m-1}a_1+\cdots 10a_{m-1}+a_m$.

(3) Si el desarrollo decimal de un número real $\beta\ge 0$ es $B.a_1\cdots a_n\cdots$ y $B\le A$, entonces $\alpha-\beta=A-B$.

Demostración. Por definición se tiene que

$$A+\frac{a_1}{10}+\cdots+\frac{a_n}{10^n}\le\alpha<A+\frac{a_1}{10}+\cdots+\frac{a_n+1}{10^n}$$

para $n\ge 1$

(1) Sumando B a las desigualdades obtenemos

$$A+B+\frac{a_1}{10}+\cdots+\frac{a_n}{10^n}\le\alpha+B<A+B+\frac{a_1}{10}+\cdots+\frac{a_n+1}{10^n}$$

para todo $n\ge 1$ y por lo tanto $(A+B).a_1\ldots a_n\ldots$ es el desarrollo decimal de $\alpha+B$.

(2) Multiplicando por 10^m cada una de las desigualdades para $n=m+k$ tenemos que para todo $k\ge 1$

$$\begin{gathered}\left(10^mA+10^{m-1}a_1+\cdots+10a_{m-1}+a_m\right)+\tfrac{a_{m+1}}{10}+\cdots+\tfrac{a_{m+k}}{10^k}\le \\ 10^m\alpha<\left(10^mA+10^{m-1}a_1+\cdots+10a_{m-1}+a_m\right)+\tfrac{a_{m+1}}{10}+\cdots+\tfrac{a_{m+k}+1}{10^k}\end{gathered}$$

Luego el desarrollo decimal de $10^m\alpha$ es $B.a_{m+1}\cdots$, donde

$$B = 10^m A + 10^{m-1}a_1 + \cdots + 10a_{m-1} + a_m$$

(3) Tenemos que $B + \frac{a_1}{10} + \cdots + \frac{a_n}{10^n} \leq \beta < B + \frac{a_1}{10} + \cdots + \frac{a_n+1}{10^n}$ para toda $n \geq 1$. Entonces $(A - B) - \frac{1}{10^n} < \alpha - \beta < (A - B) + \frac{1}{10^n}$ para todo $n \geq 1$, es decir, $-\frac{1}{10^n} < (\alpha - \beta) - (A - B) < \frac{1}{10^n}$ para toda $n \geq 1$.
De aquí concluimos que debe ser $(\alpha - \beta) - (A - B) = 0$, que es $\alpha - \beta = A - B$. ∎

Teorema 11.3.13*. Sea α un número real no negativo. α es un número racional si y sólo si su desarrollo decimal es periódico.*

Demostración. $\Rightarrow$) Sea $r \in \mathbb{Q}$, $r = \frac{a}{b}$ con $a > 0$ y $b > 0$. Como el desarrollo decimal de una fracción decimal es periódico con período 0, podemos suponer que r no es fracción decimal, y en este caso debe ser $b > 1$.

Por el algoritmo de la división, para cada número natural i, existen enteros q_i y r_i tales que

$$10^i a = b \cdot q_i + r_i \text{donde } 0 \leq r_i < b$$

Luego $10^i \frac{a}{b} = q_i + \frac{r_i}{b}$ donde $0 \leq \frac{r_i}{b} < 1$. Ahora debido a que $\frac{a}{b}$ no es una fracción decimal, debe ser $r_i \neq 0$ para toda i ya que en caso contrario sería $\frac{a}{b} = \frac{q_i}{10^i}$.

Como $0 < r_i < b$ para toda $i = 0, 1, 2, \ldots$, entonces cada r_i puede tomar a lo más $b - 1$ valores (recuérdese que $b > 1$), por lo que para alguna $n \geq 1$ y alguna $k > 0$ debe ser $r_n = r_{n+k}$. Entonces $10^n \frac{a}{b} = q_n + \frac{r_n}{b}$ y $10^{n+k}\frac{a}{b} = q_{n+k} + \frac{r_{n+k}}{b}$. Tomemos la mínima n y la mínima k con esta propiedad.

Sea $A.a_1 \ldots a_n \ldots$ el desarrollo decimal de $\frac{a}{b}$. Por (2) del lema 11.3.12 se tiene que

$$(10^n A + 10^{n-1}a_1 + \cdots + 10a_{n-1} + a_n).a_{n+1} \ldots a_{n+j} \ldots$$

y

$$(10^{n+k}A + 10^{n+k-1}a_1 + \cdots + 10a_{n+k-1} + a_{n+k}).a_{n+k+1} \ldots a_{n+k+j} \ldots$$

son los desarrollos decimales de $10^n\frac{a}{b}$ y $10^{n+k}\frac{a}{b}$ respectivamente. Como q_n y q_{n+k} son enteros, por (1) del mismo teorema, los desarrollos decimales de $\frac{r_n}{b} = 10^n\frac{a}{b} - q_n$ y $\frac{r_{n+k}}{b} = 10^{n+k}\frac{a}{b} - q_{n+k}$ son respectivamente

$$(10^n A + 10^{n-1}a_1 + \cdots + 10a_{n-1} + a_n - q_n).a_{n+1} \ldots a_{n+j} \ldots$$

y

$$(10^{n+k}A + 10^{n+k-1}a_1 + \cdots + 10a_{n+k-1} + a_{n+k} - q_{n+k}).a_{n+k+1} \ldots a_{n+k+j} \ldots$$

y ya que $\frac{r_n}{b} = \frac{r_{n+k}}{b}$, por la unicidad del desarrollo decimal, se debe tener que

$$a_{n+k+1} = a_{n+1},\ a_{n+k+2} = a_{n+2}, \ldots, a_{n+2k} = a_{n+k},\ a_{n+2k+1} = a_{n+k+1} = a_{n+1},\ a_{n+2k+2} = a_{n+k+2} = a_{n+2}, \ldots,\ \text{etc.}$$

Concluimos entonces que el desarrollo decimal de $r = \frac{a}{b}$ es

$$A.a_1 \ldots a_n\widehat{a_{n+1} \ldots a_{n+k}}$$

y por lo tanto es periódico.

$\Leftarrow$) Supongamos ahora que $A.a_1 \ldots a_n\widehat{a_{n+1} \ldots a_{n+k}}$ es el desarrollo decimal del número real $\alpha > 0$. Entonces por el lema 11.3.12, el desarrollo decimal de $10^{n+k}\alpha$ es

$$10^{n+k}A + \cdots + 10a_{n+k-1} + a_{n+k}.\widehat{a_{n+1} \cdots a_{n+k}}$$

y el del $10^n\alpha$ es $(10^nA + \cdots + 10a_{n-1} + a_n).\widehat{a_{n+1} \cdots a_{n+k}}$ y por lo tanto

$$10^{n+k}\alpha - 10^n\alpha = B - C \in \mathbb{Z},$$

donde

$$B = (10^{n+k}A + \cdots + 10a_{n+k-1} + a_{n+k}) \in \mathbb{Z}$$

y

$$C = 10^nA + \cdots + 10a_{n-1} + a_n \in \mathbb{Z}.$$

Luego $\alpha = \frac{B-C}{10^{n+k}-10^n} \in \mathbb{Q}$. ∎

Ejemplo 11.3.14. El desarrollo de $\alpha = \frac{1}{8}$ lo obtenemos como sigue

(1) $0 \leq \frac{1}{8} < 0 + 1$.
(2) $0 + \frac{1}{10} \leq \frac{1}{8} < 0 + \frac{2}{10}$.
(3) $0 + \frac{1}{10} + \frac{2}{10^2} \leq \frac{1}{8} < 0 + \frac{1}{10} + \frac{3}{10^2}$.
(4) $0 + \frac{1}{10} + \frac{2}{10^2} + \frac{5}{10^3} \leq \frac{1}{8} < 0 + \frac{1}{10} + \frac{2}{10^2} + \frac{6}{10^3}$.

Ahora como $\frac{1}{10} + \frac{2}{10^2} + \frac{5}{10^3} = \frac{125}{10^3} = \frac{1}{8}$, a partir de $n > 3$, todas las a_n serán 0, así que el desarrollo decimal de $\frac{1}{8}$ es $0{,}125\widehat{0}$.

Ejemplo 11.3.15. $\alpha = \frac{11}{7}$

$1 \leq \frac{11}{7} < 2$.

$$1+\tfrac{5}{10}\leq\tfrac{11}{7}<1+\tfrac{6}{10}.$$
$$1+\tfrac{5}{10}+\tfrac{7}{10^2}\leq\tfrac{11}{7}<1+\tfrac{5}{10}+\tfrac{8}{10^2}$$
$$\vdots$$
$$1+\tfrac{5}{10}+\tfrac{7}{10^2}+\tfrac{1}{10^3}+\tfrac{4}{10^4}+\tfrac{2}{10^5}+\tfrac{8}{10^6}+\tfrac{5}{10^7}\leq\tfrac{11}{7}<1+\tfrac{5}{10}+\tfrac{7}{10^2}+\tfrac{1}{10^3}+\tfrac{4}{10^4}+\tfrac{2}{10^5}+\tfrac{8}{10^6}+\tfrac{6}{10^7}$$
$$\vdots$$
$$1+\tfrac{5}{10}+\tfrac{7}{10^2}+\tfrac{1}{10^3}+\tfrac{4}{10^4}+\tfrac{2}{10^5}+\tfrac{8}{10^6}+\tfrac{5}{10^7}+\tfrac{7}{10^8}+\tfrac{1}{10^9}+\tfrac{4}{10^{10}}+\tfrac{2}{10^{11}}+\tfrac{8}{10^{12}}+\tfrac{5}{10^{13}}\leq$$
$$\tfrac{11}{7}<1+\tfrac{5}{10}+\tfrac{7}{10^2}+\tfrac{1}{10^3}+\tfrac{4}{10^4}+\tfrac{2}{10^5}+\tfrac{8}{10^6}+\tfrac{5}{10^7}+\tfrac{7}{10^8}+\tfrac{1}{10^9}+\tfrac{4}{10^{10}}+\tfrac{2}{10^{11}}+\tfrac{8}{10^{12}}+\tfrac{6}{10^{13}}$$

El desarrollo decimal de $\frac{11}{7}$ es $1.\overbrace{571428}$.

Nota 11.3.16. Existe otra manera, más sencilla, de obtener el desarrollo decimal de un número racional $\frac{a}{b}>0$ aprovechando el algoritmo de la división y es el siguiente.

Empezamos considerando $0<\frac{a}{b}<1$ con $a>0$ y $b>0$.

$$\begin{aligned}
10a &= b\cdot a_1+r_1, \quad 0\leq r_1<b, & a &= \tfrac{a_1}{10}\cdot b+\tfrac{r_1}{10}\\
10r_1 &= b\cdot a_2+r_2, \quad 0\leq r_2<b, & \tfrac{r_1}{10} &= \tfrac{a_2}{10^2}\cdot b+\tfrac{r_2}{10^2}\\
10r_2 &= b\cdot a_3+r_3, \quad 0\leq r_3<b, & \tfrac{r_2}{10^2} &= \tfrac{a_3}{10^3}\cdot b+\tfrac{r_3}{10^3}\\
&\vdots\\
10r_{n-1} &= b\cdot a_n+r_n, \quad 0\leq r_n<b, & \tfrac{r_{n-1}}{10^{n-1}} &= \tfrac{a_n}{10^n}\cdot b+\tfrac{r_n}{10^n}\\
&\vdots
\end{aligned}$$

Lo primero que se puede observar es que $0\leq a_i\leq 9$ para toda $i=1,2,\ldots$.
De estas igualdades tenemos

$$a=\tfrac{a_1}{10}\cdot b+\tfrac{r_1}{10}=\tfrac{a_1}{10}\cdot b+\tfrac{a_2}{10^2}\cdot b+\tfrac{r_2}{10^2}=\cdots=\tfrac{a_1}{10}\cdot b+\tfrac{a_2}{10^2}\cdot b+\cdots+\tfrac{a_n}{10^n}\cdot b+\tfrac{r_n}{10^n}.$$

Luego para toda $n=1,2,\ldots$

$\frac{a}{b}=\frac{a_1}{10}+\frac{a_2}{10^2}+\cdots+\frac{a_n}{10^n}+\frac{1}{10^n}\frac{r_n}{b}$ donde $a_i\in\{0,1,\ldots,9\}$ para $i=1,\ldots,n$ y $\frac{1}{10^n}\cdot\frac{r_n}{b}<\frac{1}{10^n}$.

Por lo tanto

$$\tfrac{a_1}{10}+\tfrac{a_2}{10^2}+\cdots+\tfrac{a_n}{10^n}\leq\tfrac{a}{b}<\tfrac{a_1}{10}+\tfrac{a_2}{10^2}+\cdots+\tfrac{a_n+1}{10^n}.$$

Entonces, el desarrollo decimal de $\frac{a}{b}$ es $0.a_1a_2\ldots a_n\ldots$.

Ahora, en general para cualquier número racional $\frac{a}{b} > 0$, basta ver que $a = b\cdot A + r$, $0 \leq r < b$ implica $\frac{a}{b} = A + \frac{r}{b}$ donde $0 \leq \frac{r}{b} < 1$ y $A \in \mathbb{Z}$, así que el desarrollo decimal de $\frac{a}{b}$ sería $A.a_1a_2\ldots a_n$ donde $0.a_1a_2\ldots a_n$ es el desarrollo decimal de $\frac{r}{b}$.

Esto que hemos visto no es otra cosa que dividir el entero a entre el entero b de la manera que nos enseñaron en la escuela. Hagámoslo para $r = \frac{11}{7}$

$$
\begin{array}{r|l}
 & 1.\ 5\ 7\ 1\ 4\ 2\ 8\ 5\ 7\ \cdots \\
\hline
7 & 11 \\
 & 4\ 0 \\
 & \quad 5\ 0 \\
 & \quad\quad 1\ 0 \\
 & \quad\quad\quad 3\ 0 \\
 & \quad\quad\quad\quad 2\ 0 \\
 & \quad\quad\quad\quad\quad 6\ 0 \\
 & \quad\quad\quad\quad\quad\quad 4\ 0 \\
 & \quad\quad\quad\quad\quad\quad\quad 5\ 0 \\
 & \quad\quad\quad\quad\quad\quad\quad\quad \ddots
\end{array}
$$

Efectivamente el desarrollo decimal de $\frac{11}{7}$ es $1.\overbrace{571428}$ (compárelo con el ejemplo 11.3.15).

Ejemplo 11. 3.17. Encontraremos A, a_1, a_2, a_3, a_4 en el desarrollo decimal $A.a_1a_3a_3a_4\ldots$ de $\alpha = \sqrt{2}$. Recuerde que $\sqrt{2}$ existe en $\mathbb{R}$ (teorema 11.2.27).

(*i*) $1 \leq \sqrt{2} < 2$ (se obtiene de $1 \leq 2 < 4$).
(*ii*) $1 + \frac{4}{10} \leq \sqrt{2} < 1 + \frac{5}{10}$, se obtiene de

$$\left(1 + \frac{4}{10}\right)^2 = \frac{196}{10^2} < \frac{225}{10^2} = \left(1 + \frac{5}{10}\right)^2.$$

(*iii*) $1 + \frac{4}{10} + \frac{1}{10^2} \leq \sqrt{2} < 1 + \frac{4}{10} + \frac{2}{10^2} + \frac{5}{10^3}$, se obtiene de

$$\left(1 + \frac{4}{10} + \frac{1}{10^2}\right)^2 = \frac{19881}{10^4} \leq 2 < \frac{20164}{10^4} = \left(1 + \frac{4}{10} + \frac{2}{10^2}\right)^2.$$

(*iv*) $1 + \frac{4}{10} + \frac{1}{10^2} + \frac{4}{10^3} \leq \sqrt{2} < 1 + \frac{4}{10} + \frac{1}{10^2} + \frac{5}{10^3}$, se obtiene de

$$\left(1 + \frac{4}{10} + \frac{1}{10^2} + \frac{4}{10^3}\right)^2 = \frac{1999396}{10^6} \leq 2 < \frac{2002225}{10^6} = \left(1 + \frac{4}{10} + \frac{1}{10^2} + \frac{5}{10^3}\right)^2.$$

(*v*) $1+\frac{4}{10}+\frac{1}{10^2}+\frac{4}{10^3}+\frac{2}{10^4} \leq \sqrt{2} < 1+\frac{4}{10}+\frac{1}{10^2}+\frac{4}{10^3}+\frac{3}{10^4}$ se obtiene de

$$\left(1+\frac{4}{10}+\frac{1}{10^2}+\frac{4}{10^3}+\frac{2}{10^4}\right)^2 = \frac{199996064}{10^8} \leq 2 < \frac{200024549}{10^8} = \left(1+\frac{4}{10}+\frac{1}{10^2}+\frac{4}{10^3}+\frac{3}{10^4}\right)^2.$$

Por lo tanto el desarrollo decimal de $\sqrt{2}$ es de la forma $1{,}4142a_5 \cdots a_n \cdots$ y podemos asegurar que el número racional $1+\frac{4}{10}+\frac{1}{10^2}+\frac{4}{10^3}+\frac{2}{10^4}$ es tal que

$$\sqrt{2} - \left(1+\frac{4}{10}+\frac{1}{10^2}+\frac{4}{10^3}+\frac{2}{10^4}\right) < \frac{1}{10^4}.$$

Por último cabe mencionar que existe otra manera de construir los números reales a partir de los números racionales. Esto es hace a través de ciertas sucesiones (las así llamadas sucesiones de Cauchy) de números racionales. He aquí una idea somera de cómo se realiza esta construcción.

Una sucesión de números racionales es un función $f : \mathbb{N} \to \mathbb{Q}$, y si denotamos $f(i) = a_i$ para cada $i \in \mathbb{N}$, la notación usual para una sucesión es $(a_0, a_1, \ldots, a_n, \ldots)$ o de una manera más corta $(a_i)_{i\in\mathbb{N}}$. Una sucesión $(a_i)_{i\in\mathbb{N}}$ es de Cauchy si los términos de la sucesión a_i, a_j se acercan tanto como se desee a partir de cierta $n \in \mathbb{N}$ y donde el valor de esta n dependerá de qué tan cercano queremos que estén. Dicho esto en términos coloquiales, una sucesión $(a_i)_{i\in\mathbb{N}}$ es de Cauchy si dado $r \in \mathbb{Q}$, $r > 0$ (sin importar qué tan pequeño sea r), existe $m \in \mathbb{N}$ tal que $|a_i - a_j| < r$ para cualesquiera $i, j > m$. Cada sucesión de Cauchy de números racionales determinará un número real. Sin embargo distintas sucesiones de Cauchy pueden determinar el mismo número real y debido a esto se define una relación de equivalencia en el conjunto de sucesiones de Cauchy de números racionales de tal manera que cualesquiera dos de estas sucesiones pertenecen a la misma clase de equivalencia si y sólo si determinan el mismo número real. Esto es, el conjunto de los números reales será el conjunto de clases de equivalencia de sucesiones de Cauchy.[1]

A partir de aquí se construye el sistema de números reales, suma, producto, orden, etc. y la identificación de los números racionales como números reales se da a través de la función inyectiva $f(r) = \overline{(a_i)_{i\in\mathbb{N}}}$, donde $a_i = r$ para toda $i \in \mathbb{N}$ para cada número racional r y donde $\overline{(a_i)_{i\in\mathbb{N}}}$ denota la clase de equivalencia a la cual pertenece $(a_i)_{i\in\mathbb{N}}$.

Así pues, aun cuando, desde el punto de vista conjuntista, los objetos considerados son totalmente distintos (cortaduras y clases de equivalencia de sucesiones de Cauchy), los sistemas construidos son el mismo respecto de sus propiedades, lo

[1] Una construcción detallada se puede encontrar en el capítulo 5 de [**11**].

que significa que existe una correspondencia biyectiva entre el conjunto de cortaduras derechas (izquierdas) y el conjunto de clases de equivalencia de sucesiones de Cauchy que respeta todas las propiedades, por ejemplo, si denotamos por f a esta función biyectiva y por α' a $f(\alpha)$ (con α una cortadura derecha) se tiene que $(\alpha+\beta)' = \alpha' + \beta'$, $(\alpha\cdot\beta)' = \alpha'\cdot\beta'$, $\alpha < \beta$ si y sólo si $\alpha' < \beta'$, α es cota superior de un subconjunto S del conjunto de cortaduras si y sólo si α' es cota superior de $f(S)$ en el conjunto de clases de equivalencia de sucesiones de Cauchy, etc. Esta correspondencia se puede dar de la manera siguiente: dada una cortadura α y su desarrollo decimal $A.a_1a_2\cdots a_n\cdots$, asociamos a α la clase de equivalencia de $\left(A, A+\frac{a_1}{10}, \ldots, A+\frac{a_1}{10}+\cdots+\frac{a_n}{10^n}, \ldots\right)$ y que sin ninguna dificultad se puede demostrar que es de Cauchy.

Para terminar este párrafo, recordamos que por la proposición 11.3.6 el desarrollo decimal de un número racional no negativo no puede tener un desarrollo decimal de la forma $A.a_1\ldots a_n\widehat{9}$ ¿qué pasa con estas expresiones que son las únicas periódicas que han quedado descartadas en nuestra discusión? supongamos por un momento que existe un número racional $\alpha \geq 0$ cuyo desarrollo decimal es precisamente $A.a_1\ldots a_n\widehat{9}$ donde $a_n \neq 9$. trabajando con la misma idea que en la demostración del teorema 11.3.13 obtenemos que (en este caso $k=1$)

$$\begin{aligned} 10^{n+1}\alpha - 10^n\alpha &= 9\cdot 10^n\alpha \\ &= (10^{n+1}A + 10^n a_1 + \cdots + 10a_n + 9) - (10^nA + 10^{n-1}a_1 + \cdots + a_n) \\ &= 9\cdot 10^nA + 9\cdot 10^{n-1}a_1 + \cdots + 9\cdot a_n + 9 \\ &= 9\cdot(10^nA + 10^{n-1}a_1 + \cdots + a_n + 1) \end{aligned}$$

y por lo tanto $10^n\alpha = 10^nA + 10^{n-1}a_1 + \cdots + (a_n+1)$ y así $\alpha = A + \frac{a_1}{10} + \cdots + \frac{a_n+1}{10^n}$ donde $a_n + 1 \leq 9$. Resumiendo, si hubiera un número racional no negativo cuyo desarrollo decimal es $A.a_1\ldots a_n\widehat{9}$, $a_n \neq 9$, éste debería ser $A + \frac{a_1}{10} + \cdots + \frac{a_n+1}{10^n}$. Es por esta razón que se suele identificar a $A.a_1\ldots a_n\widehat{9}$ con la fracción decimal $A + \frac{a_1}{10} + \cdots + \frac{a_n+1}{10^n}$. En particular a la expresión $0.\widehat{9} = 0.99\ldots9\ldots$ se le identifica con 1.

§§ Ejercicios sección 11.1.

11.1.1. Muestre que para un cardinal α, $\{-r \mid r \in < \alpha\}$ no es una cortadura.

11.1.2. Demuestre que la suma en $\mathbb{R}$ es asociativa y conmutativa.

11.1.3. Demuestre que si $\alpha \in \mathbb{R}$ y $\alpha > 0$, entonces $\alpha^{-1} > 0$.

11.1.4. Sea α una cortadura tal que $\alpha < 0$, muestre que α tiene inverso multiplicativo.

11.1.5. [2] Demuestre las propiedades el teorema 11.1.20 para el caso en que al menos una de las cortaduras de Dedekind no es positiva.

11.1.6. Demuestre los casos no demostrados en el teorema 11.1.21.

11.1.7. Demuestre el teorema 11.1.22.

11.1.8. Demuestre la proposición 11.1.24.

11.1.9. [3] Sean α y β cortaduras de Dedekind y $s \in \mathbb{Q}$. Demuestre que

(1) $s \in \alpha$ implica que $\alpha_s \subsetneq \alpha$.
(2) $s \notin \beta$ implica $\beta \subseteq \alpha_s$.

11.1.10. Sea $s \in \mathbb{Q}$ y β una cortadura. Demuestre que si $s \notin \beta$, entonces $\beta \subseteq \alpha_s$. (Sugerencia: Use que $<$ es un orden total.)

11.1.11. Sea $A \subseteq \mathbb{Z}$ y suponga que existe $a \in \mathbb{Z}$ tal que $a \leq x$ para toda $x \in A$. Demuestre que A tiene mínimo.

11.1.12. Sea K un campo ordenado y $x \in K$. Demuestre que $|x| = \max\{x, -x\}$.

11.1.13. Demuestre que $S = \{r \in \mathbb{Q} \mid r^2 < 2\}$ no tiene supremo en $\mathbb{Q}$.

11.1.14. Sean $r, s \in \mathbb{R}$ con $r, s \geq 0$. Si $r \leq s$, demuestre que $\sqrt{r} \leq \sqrt{s}$.

§§ Ejercicios sección 11.2.

11.2.1. Muestre que $| x | = \max\{x, -x\}$.

11.2.2. [4] Sea K un campo ordenado completo y $S \subseteq K$ no vacío acotado inferiormente y sea $S' = \{s \in K \mid x \text{ es cota inferior de } S\}$. Demuestre que S' está acotado superiormente y que el supremo de S' es precisamente el ínfimo de S.

11.2.3. Si A tiene supremo (ínfimo), entonces $S = \{-x \mid x \in A\}$ tiene ínfimo (supremo) y $\inf S = -\sup A$ ($\sup S = -\inf A$).

11.2.4. [5] Sea K un campo ordenado y sean A y B subconjuntos no vacíos de K que tienen ínfimo. Entonces

(1) $S = \{x + y \mid x \in A\, y \in B\}$ tiene ínfimo y $\inf S = \inf A + \inf B$.

[2] Parte del teorema 11.1.20 pág. 360.
[3] Parte del teorema 11.1.25 pág. 362.
[4] Parte del lema 11.2.10 pág. 365.
[5] Parte del teorema 11.2.22 pág. 369.

(2) Si todos los elementos de A y B son positivos, entonces

$$T = \{x \cdot y \mid x \in A\, y \in B\}$$

tiene ínfimo y ínf T = ínf $A \cdot$ ínf B.

11.2.5. Si A tiene supremo (ínfimo), entonces $S = \{-x \mid x \in A\}$ tiene ínfimo (supremo) y ínf $S = -\sup A$ ($\sup S = -$ ínf A).

11.2.6. Demostrar que $x = \acute{i}nfK^x$ con las hipótesis del lema 11.2.23.

11.2.7. En la demostración de 4°/ del teorema 11.2.25, justifique por qué existe el supremo en K de $\{r \in \mathbb{Q} \mid r < y\}$.

11.2.8. Para la función ψ definida en la demostración del teorema 11.2.25 justifique la igualdad $sup_L = \{r \in \mathbb{Q} \mid r < x\} = \acute{i}nf_L = \{r \in \mathbb{Q} \mid x < r\}$ para toda $x \in K$.

11.2.9. [6] Sea K un campo ordenado completo. Demuestre que si $0 \leq x \leq y$, entonces $x^m \leq y^m$ para todo $m \in \mathbb{N}$.

§§ Ejercicios sección 11.3.

11.3.1. En el contexto de la nota 11.3.16, verificar que efectivamente $0 \leq a_i \leq 9$ para toda $i = 1, 2, \ldots$.

[6] Parte del teorema 11.2.27 pág. 369.

No es el conocimiento, sino el acto de aprendizaje, y no la posesión, sino el acto de llegar allí, que concede el mayor disfrute.
Carl Friedrich Gauss
1777 - 1855

***Capítulo* 12**

Los números complejos

§ 12.1. Introducción del sistema de los números complejos

El último sistema numérico que construiremos será el de los números complejos y como se ha venido haciendo a lo largo del libro, este sistema, que será campo, resultará ser una extensión de los números reales, es decir, contendrá a los números reales como subcampo. En el capítulo anterior demostramos que para cualquier número real $z \geq 0$, ecuaciones del tipo $x^m = z$ tiene siempre solución en $\mathbb{R}$ para todo número natural $m \geq 1$. Sin embargo en el caso de que $z < 0$, este tipo de ecuaciones no siempre tiene solución en $\mathbb{R}$ como es el caso cuando m es par. Nos gustaría entonces construir un campo, que denotaremos por $\mathbb{C}$ que contenga a $\mathbb{R}$ como subcampo y donde ecuaciones del tipo $x^m = z$ tenga solución para toda $z \in \mathbb{R}$. Observando que dado $z \in \mathbb{R}$, si $z < 0$, entonces $z = (-1)(-z)$, donde $-z > 0$, en realidad bastaría construir un campo que contenga a $\mathbb{R}$ como subcampo y que contenga un elemento $\boldsymbol{i}$ tal que $i^2 = -1$, ya que $x^2 = z$ tendría como solución a $i \cdot s$, donde s es solución de $x^2 = -z$, esto es, $(i \cdot s)^2 = i^2 \cdot s^2 = (-1)(-z) = z$. Resumiendo, queremos construir un campo $\mathbb{C}$ que tenga a $\mathbb{R}$ como subcampo y que contenga un elemento i tal que $i^2 = -1$. Con estas condiciones tratemos de descubrir cómo podemos construir este campo $\mathbb{C}$. Partamos del hecho de que este campo existe y podemos suponerlo "mínimo" con las propiedades deseadas (que es, contiene a $\mathbb{R}$ y contiene un elemento i tal que $i^2 = -1$). Primero, como cada número real a deberá ser elemento de $\mathbb{C}$, o más formalmente, identificado con un elemento de $\mathbb{C}$,

denotando a este identificado de a con la misma letra, $\mathbb{C}$ deberá contener también a los elementos de la forma $b \cdot i$, con $b \in \mathbb{R}$ y por lo tanto deberá contener a los elementos de la forma $a + bi$ para cualesquiera $a, b \in \mathbb{R}$. La suma y producto, por ser $\mathbb{C}$ campo, satisfacen

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$

y

$$(a+bi)\cdot(c+di) = (a+bi)\cdot c + (a+bi)\cdot di = ac + bci + adi + bdi^2 = (ac - bd) + (bc + ad)i.$$

Además si $a + bi = c + di$, entonces $a - c = (b - d)i$ y esto último implica $b = d$ y por lo tanto $a = c$, ya que si se tuviera $b - d \neq 0$, que es $b \neq d$, entonces sería $i = \frac{a-c}{b-d}$ y de aquí $-1 = i^2 = \frac{(a-c)^2}{(b-d)^2}$, lo que no puede ser pues $\frac{a-c}{b-d} \in \mathbb{R}$ y que sabemos que el cuadrado de un número real siempre es mayor o igual a cero. Concluimos entonces que $a + bi = c + di$ si y sólo si $a = c$ y $b = d$. Teniendo en cuenta esto último, cada elemento $a+bi$ estará determinado entonces por la pareja ordenada (a, b). Es natural entonces intentar introducir como nuestro modelo a $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(a, b) \mid a, b \in \mathbb{R}\}$, en donde la suma y el producto en este conjunto deberán definirse de acuerdo a nuestros objetivos, sabiendo que (a, b) hará el papel de $a + bi$. Considerando la discusión anterior definimos entonces

Definición 12.1.1. *El sistema de los números complejos $\mathbb{C}$ es el conjunto de las parejas ordenadas de números reales (a, b), donde la suma y producto están dadas por*

$$(a, b) + (c, d) = (a + c, b + d) \;\; y \;\; (a, b) \cdot (c, d) = (ac - bd, bc + ad).$$

Nota 12.1.2. $(a, b) \neq (0, 0)$ si y sólo si $a \neq 0$ o $b \neq 0$. Además teniendo en cuenta que $a^2 \geq 0$ para todo $a \in \mathbb{R}$, se tiene que $a^2 + b^2 = 0$ si y sólo si $a = b = 0$ o equivalentemente $a^2 + b^2 \neq 0$ si y sólo si $a \neq 0$ o $b \neq 0$ y por lo tanto $(a, b) \neq (0, 0)$ si y sólo si $a^2 + b^2 \neq 0$.

Teorema 12.1.3. *El conjunto $\mathbb{C}$, con las operaciones definidas en él, es un campo.*

Demostración. Las propiedades de la suma y el producto en $\mathbb{C}$ son consecuencia directa de las propiedades de suma y producto en $\mathbb{R}$:

(1) La suma es asociativa:

$$\begin{aligned}[(a,b)+(c,d)]+(e,f) &= (a+c,b+d)+(e,f)\\ &= ((a+c)+e,(b+d)+f)\\ &= (a+(c+e),b+(d+f))\\ &= (a,b)+(c+e,d+f)\\ &= (a,b)+\big[(c,d)+(e,f)\big].\end{aligned}$$

(2) La suma es conmutativa:

$$(a,b)+(c,d)=(a+c,b+d)=(c+a,d+b)=(c,d)+(a,b).$$

(3) $(0,0)$ es el neutro aditivo:

$$(a,b)+(0,0)=(a+0,b+0)=(a,b).$$

(4) $(-a,-b)$ es el inverso de (a,b):

$$(a,b)+(-a,-b)=(a-a,b-b)=(0,0).$$

(5) El producto es asociativo:

$$\begin{aligned}[(a,b)\cdot(c,d)]\cdot(e,f) &= (ac-bd,bc+ad)\cdot(e,f)\\ &= ((ac-bd)e-(bc+ad)f,(bc+ad)e+(ac-bd)f)\\ &= (a(ce-df)-b(de+cf),b(ce-df)+a(de+cf))\\ &= (a,b)\cdot(ce-df,de+cf)\\ &= (a,b)\cdot\big[(c,d)\cdot(e,f)\big]\end{aligned}$$

(6) El producto es conmutativo:

$$\begin{aligned}(a,b)\cdot(c,d) &= (ac-bd,bc+ad)\\ &= (ca-db,da+cb)\\ &= (c,d)\cdot(a,b).\end{aligned}$$

(7) $(1,0)$ es el neutro multiplicativo:

$$(a,b)\cdot(1,0)=(a\cdot 1-b\cdot 0,b\cdot 1+a\cdot 0)=(a,b).$$

(8) Si $(a,b)\neq(0,0)$, el inverso multiplicativo de (a,b) es $\left(\frac{a}{a^2+b^2},\frac{-b}{a^2+b^2}\right)$:

$$(a,b)\cdot\left(\frac{a}{a^2+b^2},\frac{-b}{a^2+b^2}\right)=\left(\frac{a^2}{a^2+b^2}-\frac{(-b)b}{a^2+b^2},\frac{ba}{a^2+b^2}+\frac{a(-b)}{a^2+b^2}\right)=(1,0).$$

(9) El producto distribuye a la suma:

$$\begin{aligned}(a,b)\cdot\big[(c,d)+(e,f)\big] &= (a,b)\cdot(c+e,d+f)\\ &= (a\cdot(c+e)-b\cdot(d+f),b\cdot(c+e)+a\cdot(d+f))\\ &= (ac+ae-bd-bf,bc+be+ad+af)\\ &= ((ac-bd)+(ae-bf),(bc+ad)+(be+af))\\ &= (ac-bd,bc+ad)+(ae-bf,be+af)\\ &= (a,b)\cdot(c,d)+(a,b)\cdot(e,f).\end{aligned}$$

■

Tomando en cuenta la definición de suma y producto en $\mathbb{C}$, se puede ver sin ninguna dificultad que cada elemento (a,b) en $\mathbb{C}$ se expresa como $(a,b) = (a,0) + (b,0)\cdot(0,1)$, así que si denotamos $i = (0,1)$,

$$(a,b) = (a,0) + (b,0)\cdot i.$$

Notamos que los elementos de $\mathbb{C}$ de la forma $(a,0)$ están determinados de manera única por el número real a. Así que si identificamos al número real a con el número complejo $(a,0)$ y si denotamos por $\overline{a} = (a,0)$, entonces cada número complejo (a,b) puede ser expresado como $(a,b) = \overline{a} + \overline{b}i$, donde

$$i^2 = (0,1)\cdot(0,1) = (-1,0) = \overline{-1}.$$

Formalicemos esta idea:

Proposición 12.1.4. *La función $\varphi : \mathbb{R} \longrightarrow \mathbb{C}$ dada por $\varphi(a) = (a,0)$ satisface:*

(1) *φ es inyectiva.*
(2) *$\varphi(a+b) = \varphi(a) + \varphi(b)$.*
(3) *$\varphi(a\cdot b) = \varphi(a)\cdot\varphi(b)$.*
(4) *$\varphi(0) = (0,0)$ (el neutro aditivo de $\mathbb{R}$ se aplica en el neutro aditivo de $\mathbb{C}$).*
(5) *$\varphi(-a) = -\varphi(a)$ (el inverso aditivo de a se aplica en el inverso aditivo de $\varphi(a)$).*
(6) *$\varphi(1) = (1,0)$ (el neutro multiplicativo de $\mathbb{R}$ se aplica en el neutro multiplicativo de $\mathbb{C}$).*
(7) *Si $a \neq 0$ en $\mathbb{R}$, entonces $\varphi(a^{-1}) = \varphi(a)^{-1}$ (el inverso multiplicativo de a se aplica en el inverso multiplicativo de $\varphi(a)$).*

Demostración. Sean $a, b \in \mathbb{R}$.

(1) Si $\varphi(a) = \varphi(b)$, entonces $(a,0) = (b,0)$ y por lo tanto $a = b$.
(2) $\varphi(a+b) = (a+b,0) = (a,0) + (b,0) = \varphi(a) + \varphi(b)$.
(3) $\varphi(a\cdot b) = (a\cdot b,0) = (a,0)\cdot(b,0) = \varphi(a)\cdot\varphi(b)$.
(4) $\varphi(0) = (0,0)$ por la definición de φ.

(5) Como $a + (-a) = 0$, entonces

$$(0, 0) = \varphi(0) = \varphi(a + (-a)) = \varphi(a) + \varphi(-a).$$

De donde debe ser $\varphi(-a) = -\varphi(a)$.
(6) $\varphi(1) = (1, 0)$ por la definición de φ.
(7) Si $a \neq 0$, entonces $\varphi(a) = (a, 0) \neq (0, 0)$ y

$$(1, 0) = \varphi(1) = \varphi(a \cdot a^{-1}) = \varphi(a) \cdot \varphi(a^{-1}),$$

por lo que $\varphi(a^{-1}) = \varphi(a)^{-1}$. ∎

Con la identificación que hemos hecho de los números reales como números complejos, sin ningún problema, podemos denotar al número complejo (a, b) por $a+bi$, donde $a, b \in \mathbb{R}$ e $i^2 = -1$. Entonces de aquí en adelante consideraremos a los números complejos como el conjunto

$$\mathbb{C} = \left\{ a + bi \mid a, b \in \mathbb{R},\ i^2 = -1 \right\},$$

donde, para $a + bi,\ c + di \in \mathbb{C}$,

$$a + bi = c + di \text{ si y sólo si } a = c \text{ y } b = d,$$

$(a+bi)+(c+di) = (a+c)+(b+d)i$ y $(a+bi)\cdot(c+di) = (ac-bd)+(bc+ad)i$, y donde además $0 + 0i$, que lo denotaremos sencillamente por 0 y $1 + 0i$ que denotamos por 1, son el neutro aditivo y multiplicativo, respectivamente, de $\mathbb{C}$.

§ 12.2. El conjugado y el valor absoluto de un número complejo

Partiendo de $\mathbb{N}$, hemos construido los distintos sistemas numéricos

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{R} \subset \mathbb{C}$$

y en cada uno de ellos las operaciones se fueron extendiendo al siguiente hasta llegar a $\mathbb{C}$, no solamente eso, sino que hasta $\mathbb{R}$ se fue extendiendo el orden también, así que lo primero que uno podría pensar es en extender el orden de $\mathbb{R}$ a un orden en $\mathbb{C}$. Si bien es cierto que esto puede hacerse, el orden resultante en $\mathbb{C}$, cualquiera que sea éste, no puede llevar nunca a que $\mathbb{C}$ es un campo ordenado y la razón es muy sencilla: En cada campo ordenado K debe ser $1 > 0$ (teorema 11.2.4) y también $x^2 \geq 0$ para toda $x \in K$; sin embargo para el elemento $i \in \mathbb{C}$ se tiene que $i^2 = -1$, así que si $\mathbb{C}$ fuera un campo ordenado, por un lado debería ser $i^2 > 0$ y por el otro $i^2 = -1 < 0$. Así pues, aunque se pierde la propiedad de ser campo ordenado, veremos que $\mathbb{C}$ tiene propiedades muy importantes que sus antecesores no tienen. Empezaremos definiendo el conjugado y el valor absoluto o módulo

de un número complejo y demostraremos algunas propiedades. En particular el conjugado de un número complejo desempeñará una propiedad muy importante en el capítulo siguiente.

Definición 12.2.1. *Dado un número complejo $z = a + bi$, su* **parte real** *denotada por* $\mathrm{Re}(z)$ *y su* **parte imaginaria** *denotada por* $\mathrm{Im}(z)$ *son* $\mathrm{Re}(z) = a$ *e* $\mathrm{Im}(z) = b$, *respectivamente.*

Proposición 12.2.2. *Sean* $z, w \in \mathbb{C}$. *Entonces*

(1) $\mathrm{Re}(z + w) = \mathrm{Re}(z) + \mathrm{Re}(w)$, $\mathrm{Im}(z + w) = \mathrm{Im}(z) + \mathrm{Im}(w)$.
(2) $\mathrm{Re}(-z) = -\mathrm{Re}(z)$, $\mathrm{Im}(-z) = -\mathrm{Im}(z)$.

La demostración de esta proposición queda como ejercicio (véase ejercicio 12.2.1).

Nota 12.2.3. Al número complejo $z = a + (-b)i$ lo denotaremos simplemente por $\boldsymbol{a - bi}$, al número complejo $z = a + 0 \cdot i$, lo denotaremos simplemente por a y al número complejo $z = 0 + bi$, por bi.

Definición 12.2.4. *Dado un número complejo* $z = a + bi$, *su* **conjugado** *denotado por* $\overline{\boldsymbol{z}}$ *es* $\boldsymbol{\overline{z} = a - bi}$.

Ejemplo 12.2.5.
$\overline{1 + 3i} = 1 - 3i$, $\overline{5 - 2i} = 5 + 2i$, $\overline{-7 - i} = -7 + i$, $\overline{\sqrt{2} \cdot i} = -\sqrt{2} \cdot i$, $\overline{13} = 13$.

Las propiedades de la conjugación son

Teorema 12.2.6. *Sean* $z, w \in \mathbb{C}$. *Entonces*

(1) $\overline{z} = z$ *si y sólo si* $\mathrm{Im}(z) = 0$ *(esto es* $z \in \mathbb{R}$*).*
(2) $\overline{z} = -z$ *si y sólo si* $\mathrm{Re}(z) = 0$.
(3) $\overline{(-z)} = -\overline{z}$.
(4) $\overline{\overline{z}} = z$
(5) $\overline{(z + w)} = \overline{z} + \overline{w}$.
(6) $\overline{(z - w)} = \overline{z} - \overline{w}$.
(7) $\overline{(z \cdot w)} = \overline{z} \cdot \overline{w}$.
(8) Si $w \neq 0$, *entonces* $\overline{w} \neq 0$ *y* $\left(\overline{\frac{z}{w}}\right) = \frac{\overline{z}}{\overline{w}}$, *En particular* $\overline{(w^{-1})} = (\overline{w})^{-1}$.
(9) $z + \overline{z} = 2\mathrm{Re}(z)$ *y* $z - \overline{z} = 2\mathrm{Im}(z) \cdot i$.
(10) Si $z = a + bi$, *entonces* $z \cdot \overline{z} = a^2 + b^2$, *es decir que* $z \cdot \overline{z} \in \mathbb{R}^+ \cup \{0\}$.

Demostración. Como todas las demostraciones son bastante sencillas ya que se realizan aplicando la definición del conjugado, sólo demostraremos los incisos

(5), (7), (8) y (10) como ilustración y dejamos la demostración de los restantes como ejercicio (véase ejercicio 12.2.8).
Sean $z = a + bi$ y $w = c + di$. Entonces $\overline{z} = a - bi$ y $\overline{w} = c - di$.

(5) $z + w = (a + c) + (b + d)i$ implica

$$\overline{(z + w)} = (a + c) - (b + d)i = a - bi + c - di = \overline{z} + \overline{w}.$$

(7) $z \cdot w = (ab - cd) + (bc + ad)i$ implica $\overline{z \cdot w} = (ab - cd) - (bc + ad)i$. Entonces

$$\overline{z} \cdot \overline{w} = (a - bi) \cdot (c - di) = (ac - bd) + (-bc - ad)i = (ac - bd) - (bc + ad)i = \overline{z \cdot w}.$$

(8) Primero $w \neq 0$ implica $c \neq 0$ o $d \neq 0$, así que $\overline{w} \neq 0$. Ahora, $\left(\frac{z}{w}\right) \cdot w = z$ implica $\overline{\left(\frac{z}{w}\right) \cdot w} = \overline{z}$ y aplicando (7) obtenemos $\overline{\left(\frac{z}{w}\right)} \cdot \overline{w} = \overline{z}$, de donde $\overline{\left(\frac{z}{w}\right)} = \frac{\overline{z}}{\overline{w}}$.
En el caso en que $z = 1$ se tiene que $\overline{w^{-1}} = \overline{\left(\frac{1}{w}\right)} = \frac{\overline{1}}{\overline{w}} = (\overline{w})^{-1}$.

(10) $z \cdot \overline{z} = (a + bi) \cdot (a - bi) = (a^2 + b^2) + (ba - ab)i = a^2 + b^2 \in \mathbb{R}$ y como $a^2 \geq 0$ y $b^2 \geq 0$, entonces $z \cdot \overline{z} \geq 0$. ∎

Siendo $z \cdot \overline{z}$ un número real no negativo para cualquier número complejo z, por el teorema 11.2.27, $z \cdot \overline{z}$ tiene una única raíz cuadrada no negativa en $\mathbb{R}$. Daremos un nombre especial a esta raíz cuadrada, que como se verá más adelante nos será de mucha utilidad.

Definición 12.2.7. *Dado un número complejo z, su* ***valor absoluto*** *o* ***módulo****, denotado por* $\mathbf{|z|}$*, es el número real no negativo* $|z| = \sqrt{z \cdot \overline{z}}$.

El valor absoluto o módulo de un número complejo es en realidad una extensión a $\mathbb{C}$ del valor absoluto definido en $\mathbb{R}$. Para ver esto, sea $z \in \mathbb{C}$ tal que $z \in \mathbb{R}$, es decir, $z = a + 0i = a \in \mathbb{R}$. Entonces por definición,

$$|z| = \sqrt{z \cdot \overline{z}} = \sqrt{a^2 + 0^2} = \sqrt{a^2} = \begin{cases} a & \text{si } a \geq 0 \\ -a & \text{si } a < 0 \end{cases} = |a|_{\mathbb{R}},$$

en donde hemos denotado por $|a|_{\mathbb{R}}$ al valor absoluto de a definido en $\mathbb{R}$ y por esta razón no necesitamos utilizar el índice $\mathbb{R}$ en el caso en que $z \in \mathbb{R}$.
Las propiedades del valor absoluto son las siguientes

Teorema 12.2.8. *Sean $z, w \in \mathbb{C}$. Entonces*

(1) $|z| \geq 0$ *y* $|z| = 0$ *si y sólo si* $z = 0$.
(2) $z \cdot \overline{z} = |z|^2$.
(3) $|\mathrm{Re}(z)| \leq |z|$, $|\mathrm{Im}(z)| \leq |z|$.
(4) $|\overline{z}| = |z|$

(5) $|-z| = |z|$.
(6) $|z \cdot w| = |z| \cdot |w|$
(7) *Si* $w \neq 0$, *entonces* $\left|\frac{z}{w}\right| = \frac{|z|}{|w|}$. *En particular* $\left|w^{-1}\right| = |w|^{-1}$.
(8) $|z + w| \leq |z| + |w|$.

Demostración. Sólo demostraremos (6), (7) y (8) dejando los restantes como ejercicio (véase ejercicio 12.2.9)

(6) Usando el inciso (2) y las propiedades de la conjugación,

$$|z \cdot w|^2 = (z \cdot w)\overline{(z \cdot w)} = (z \cdot w)\,(\overline{z} \cdot \overline{w}) = (z \cdot \overline{z}) \cdot (w \cdot \overline{w}) = |z|^2 \cdot |w|^2 = (|z| \cdot |w|)^2 .$$

De donde, tomando raíz cuadrada y debido a que tanto $|z \cdot w|$ como $|z| \cdot |w|$ son ambos no negativos, se obtiene $|z \cdot w| = |z| \cdot |w|$.

(7) Por el inciso (1), $w \neq 0$ implica $|w| \neq 0$. Usando el inciso (6) se tiene que

$$|z| = \left|\frac{z}{w} \cdot w\right| = \left|\frac{z}{w}\right| \cdot |w| .$$

Por lo tanto $\left|\frac{z}{w}\right| = \frac{|z|}{|w|}$. En particular, si $z = 1$, entonces

$$\left|w^{-1}\right| = \left|\frac{1}{w}\right| = \frac{|1|}{|w|} = \frac{1}{|w|} = |w|^{-1}.$$

(8) Usando los incisos (2), (3) y (4) y las propiedades del conjugado tenemos

$$\begin{aligned}
|z + w|^2 &= (z + w) \cdot \overline{(z + w)} && \text{def. valor absoluto}\\
&= (z + w) \cdot (\overline{z} + \overline{w}) && \text{teorema 12.2.6 (5)}\\
&= z \cdot \overline{z} + w \cdot \overline{z} + z \cdot \overline{w} + w \cdot \overline{w} && \text{distibutividad del producto}\\
&= |z|^2 + w \cdot \overline{z} + \overline{(w \cdot \overline{z})} + |w|^2 && \text{teorema 12.2.6 (4) y (7)}\\
&= |z|^2 + 2\mathrm{Re}\,(w \cdot \overline{z}) + |w|^2 && \text{teorema 12.2.6 (9)}\\
&\leq |z|^2 + 2\,|\mathrm{Re}\,(w \cdot \overline{z})| + |w|^2 &&\\
&\leq |z|^2 + 2\,|w \cdot \overline{z}| + |w|^2 && \text{inciso (3)}\\
&= |z|^2 + 2|w| \cdot |\overline{z}| + |w|^2 && \text{inciso (6)}\\
&= |z|^2 + 2|w| \cdot |z| + |w|^2 && \text{inciso (4)}\\
&= (|z| + |w|)^2 &&
\end{aligned}$$

Como $|z + w| \geq 0$ y $|z| + |w| \geq 0$, tomando la raíz cuadrada positiva en ambos miembros de la desigualdad (la desigualdad se conserva por el ejercicio 11.1.14) obtenemos $|z + w| \leq |z| + |w|$. ∎

En la siguiente sección demostraremos que ecuaciones del tipo $x^m = w$ tiene solución en $\mathbb{C}$ para todo $w \in \mathbb{C}$ (como hemos visto, en $\mathbb{R}$ este resultado no es cierto

en general), pero no sólo veremos la existencia de soluciones, si no que además la ecuación tiene exactamente m soluciones distintas. Por el momento veremos el caso particular en que $m = 2$. Consideramos entonces la ecuación $x^2 = w$, con $w \in \mathbb{C}$. En el supuesto de que exista solución $z \in \mathbb{C}$, veamos cómo debe ser esta solución z. $z^2 = w$ implica $|w| = |z|^2 = z \cdot \overline{z}$. Entonces

$$|w| + w = z \cdot \overline{z} + z^2 = (\overline{z} + z) \cdot z = 2\mathrm{Re}(z) \cdot z. \tag{1}$$

Si pudiéramos expresar $\mathrm{Re}(z)$ en función de w, tendríamos cómo debe ser z.

$$\begin{aligned}(2\mathrm{Re}(z))^2 &= (z + \overline{z})^2 = z^2 + 2z \cdot \overline{z} + \overline{z}^2 = w + 2|z|^2 + \overline{w} = w + \overline{w} + 2|w| \\ &= 2\mathrm{Re}(w) + 2|w| \\ &= 2\left(\mathrm{Re}(w) + |w|\right)\end{aligned}$$

Considerando la raíz cuadrada de ambos miembros de la igualdad obtenemos

$$2\mathrm{Re}(z) = \pm\sqrt{2\left(\mathrm{Re}(w) + |w|\right)}$$

Hay dos casos a considerar, $\mathrm{Re}(w) + |w| = 0$ o $\mathrm{Re}(w) + |w| \neq 0$.
Si $\mathrm{Re}(w) + |w| = 0$, entonces $\mathrm{Re}(w) = -|w|$, lo que implica que w es un número real no positivo ya que $(\mathrm{Re}(w))^2 = |w|^2 = (\mathrm{Re}(w))^2 + (\mathrm{Im}(w))^2$ y por lo tanto $\mathrm{Im}(w) = 0$, es decir, $w \in \mathbb{R}$ y de la igualdad $\mathrm{Re}(w) = -|w|$, por ser $|w| \geq 0$, se tiene que $w = \mathrm{Re}(w) = -|w| \leq 0$. Así pues, en el caso $\mathrm{Re}(w) + |w| = 0$, debe ser $w = -|w|$ y por lo tanto los únicos posibles valores para z son $z = \pm i\sqrt{|w|}$.
Si $\mathrm{Re}(w) + |w| \neq 0$, entonces, por (1), los posibles valores para z son $z = \pm\frac{|w|+w}{\sqrt{2(\mathrm{Re}(w)+|w|)}}$.
Veamos ahora que, para los posibles valores de z encontrados, z efectivamente es solución de la ecuación y como es claro que el caso $w = 0$, tiene como única solución a $z = 0$, excluimos este caso en el siguiente

Teorema 12.2.9. *Dado $w \in \mathbb{C}$, $w \neq 0$, existen exactamente dos números complejos z_1 y z_2 que son solución de la ecuación $x^2 = w$, a saber,*

$$z_1 = \frac{|w|+w}{\sqrt{2(\mathrm{Re}(w)+|w|)}} \quad y \quad z_2 = -\frac{|w|+w}{\sqrt{2(\mathrm{Re}(w)+|w|)}} \quad si \ \ \mathrm{Re}(w) + |w| \neq 0$$

y

$$z_1 = i\sqrt{|w|} \qquad y \quad z_2 = -i\sqrt{|w|} \qquad si \ \ \mathrm{Re}(w) + |w| = 0$$

Demostración. En vista de la discusión anterior al teorema, sólo nos queda demostrar que efectivamente z_1 y z_2 son soluciones de la ecuación en cada uno de los dos casos.
Si $\mathrm{Re}(w) + |w| \neq 0$, entonces

$$z_1^2 = z_2^2 = \frac{(|w|+w)^2}{2(\mathrm{Re}(w)+|w|)} = \frac{|w|^2+2w\cdot|w|+w^2}{2(\mathrm{Re}(w)+|w|)}$$
$$= \frac{w\cdot(\overline{w}+w+2|w|)}{2(\mathrm{Re}(w)+|w|)} = \frac{w\cdot(2\mathrm{Re}(w)+2|w|)}{2(\mathrm{Re}(w)+|w|)}$$
$$= w$$

Si $\mathrm{Re}(w) + |w| = 0$, entonces $z_1^2 = z_2^2 = i^2|w| = -|w| = w$. ∎

Ejemplo 12.2.10.

(1) Sea $w = 3 + 2i$. Entonces $\mathrm{Re}(w) + |w| = 3 + \sqrt{9+4} = 3 + \sqrt{13} \neq 0$ y por lo tanto las raíces cuadradas de $3 + 2i$ son $\pm\frac{|w|+w}{\sqrt{2(\mathrm{Re}(w)+|w|)}} = \pm\frac{\left(3+\sqrt{13}\right)+2i}{\sqrt{2\left(3+\sqrt{13}\right)}}$.

(2) Si $w = -i$, entonces $\mathrm{Re}(w) + |w| = 0 + \sqrt{(-1)^2} = 1$. Las dos raíces de $-i$ son $\pm\frac{|w|+w}{\sqrt{2(\mathrm{Re}(w)+|w|)}} = \pm\frac{1-i}{\sqrt{2}}$.

§ 12.3. Interpretación geométrica de los números complejos

El estudio de la Geometría Analítica se basa en la implementación de un sistema de coordenadas para los puntos del plano. Esto se realiza a través de dos líneas rectas ℓ_1 y ℓ_2 perpendiculares entre sí, en donde el punto de intersección P_0 le corresponde la pareja ordenada de números reales $(0, 0)$.

Recordamos que escogiendo un punto P_0 en la recta ℓ_1 (ℓ_2), cada punto en la línea determina un número real, en donde a P_0 le corresponde el número real 0, a los puntos a la derecha (arriba) de P_0 les corresponde los números reales positivos y a la izquierda (abajo) de P_0 les corresponde los números reales negativos.

De aquí se establece una correspondencia biyectiva entre los puntos del plano y las parejas ordenadas de números reales, llamadas las ***coordenadas cartesianas*** de los puntos. Esto es, dado un punto P del plano, sus coordenadas cartesianas (a, b) están determinadas como sigue: trazamos una paralela a la línea ℓ_2 que pasa por P y esta paralela determinará un número real a que corresponde al punto de intersección de la paralela con la línea ℓ_1. Igualmente, la recta paralela a ℓ_1 que pasa por P, determina un número real b que corresponde al punto de intersección de la paralela con ℓ_2 (Figura 1)

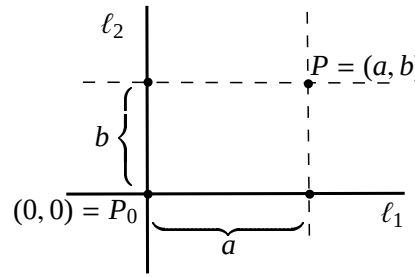


FIGURA 1. Interpretación geométrica de un número complejo

Bajo esta correspondencia se pueden describir figuras en el plano mediante ecuaciones cuyos coeficientes son números reales.

Por ejemplo, una línea recta queda descrita como el conjunto de puntos del plano cuyas coordenadas (x, y) satisfacen la relación $ax + by = c$, donde a, b y c son números reales fijos determinados por la línea recta.

Así pues, considerando que los números complejos son parejas ordenadas de números reales, podemos aprovechar la correspondencia mencionada arriba para interpretar geométricamente en el plano las operaciones definidas en $\mathbb{C}$.

(I) **Módulo de un número complejo**.

Dado un número complejo $z = a + bi$, su módulo es $|z| = \sqrt{a^2 + b^2}$. El punto del plano correspondiente al complejo z es (a, b) y $|z|$ no es otra cosa que la distancia del origen $(0, 0)$ al punto (a, b).

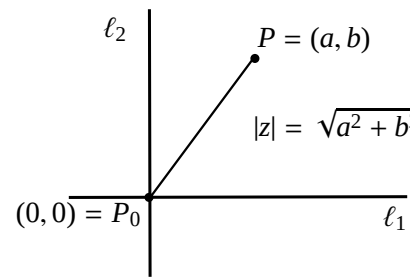


FIGURA 2. Módulo de un número complejo

(II) **Suma de números complejos.**
La suma de los números complejos $z = a + bi$ y $w = c + di$ es

$$z + w = (a + c) + (b + d)i.$$

Denotamos por P_z, P_w y P_{z+w} a los puntos del plano correspondientes a z, w y $z + w$ respectivamente. Se pueden considerar dos casos:
(i) P_w pertenece a línea ℓ determinada por el origen $\overline{0} = (0, 0)$ y P_z
(ii) P_w no pertenece a la línea ℓ.
En el caso (*i*), si P_z y P_w están en el mismo cuadrante, P_{z+w} se encontrará a una distancia $|z| + |w|$ del $\overline{0}$ sobre la línea ℓ (figura 3) y si $\overline{0}$ se encuentra entre P_z y P_w, entonces P_{z+w} se encontrará sobre la línea ℓ a una distancia $||z| - |w||$ del $\overline{0}$ y según sea el caso, se encontrará entre P_z y $\overline{0}$ si $|w| < |z|$, se encontrará entre $\overline{0}$ y P_w si $|z| < |w|$ y si $z + w = 0$, $P_{z+w} = \overline{0}$ (figura 4).
En el caso (*ii*), es decir, si $\overline{0}$, P_z y P_w no son colineales, P_{z+w}estará determinado por lo que se conoce como la ley del paralelogramo, que es, los puntos $\overline{0}$, P_z, P_{z+w} y P_w son los vértices de un paralelogramo (figura 5).

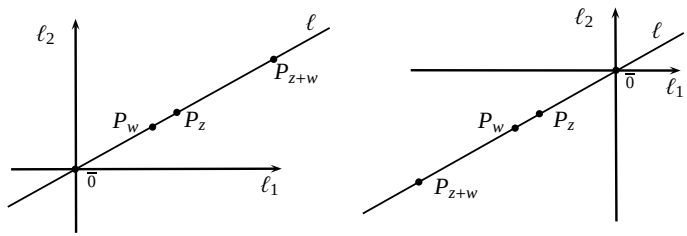


Figura 3. Suma de número complejo en el caso (*i*)

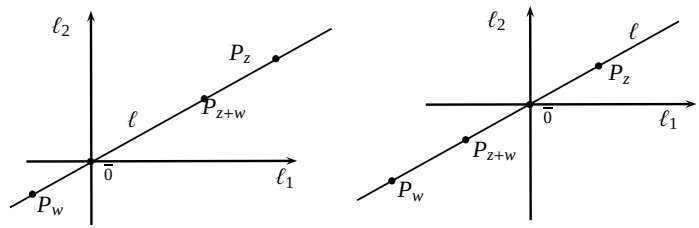


Figura 4. Suma de número complejo en el caso (*i*)

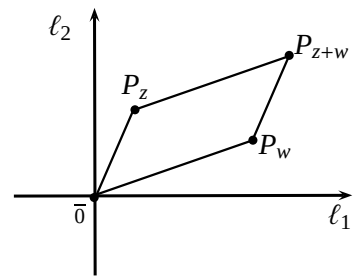


FIGURA 5. Suma de número complejo en el caso (*ii*)

(III) **Producto de dos números complejos.**

Para interpretar geométricamente el producto utilizaremos las coordenadas polares. Recordemos cómo están definidas a partir de las coordenadas cartesianas. Dado un punto P, distinto del origen, de coordenadas (a, b), éste determina un número real positivo que es la distancia al origen de P y un ángulo formado por el semieje positivo de las abscisas y el segmento OP (el determinado por $(0, 0)$ y P) medido en sentido opuesto a las agujas del reloj (figura 6). Esto es, cada punto distinto de $(0, 0)$ tiene asociado, de manera única, una pareja (r, θ), donde r es un número real positivo y θ un ángulo tal que $0 \leq \theta < 360°$.

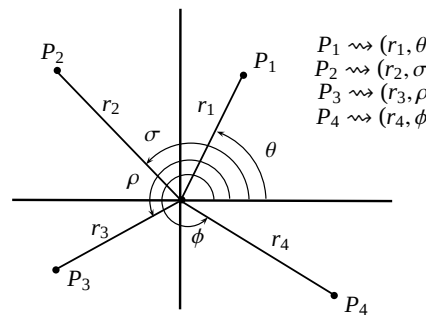


FIGURA 6. Coordenadas polares

Ahora, si las coordenadas cartesianas del punto P son (a, b) y las coordenadas polares son (r, θ), entonces con un poco de trigonometría obtenemos (figura7)

$$a = r \cdot \cos(\theta), \quad b = r \cdot \operatorname{sen}(\theta). \tag{2}$$

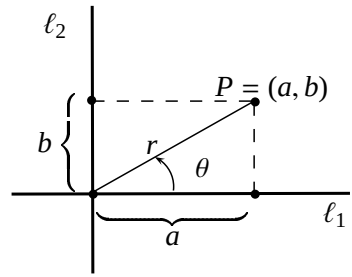


FIGURA 7. Relación entre coordenadas cartesianas y polares

Resumiendo, dado un número complejo $z = a + bi \neq 0$, podemos expresar a z por:

$$z = |z|\,(\cos(\theta) + i\,\mathrm{sen}\,(\theta))\,. \tag{3}$$

Donde θ es el ángulo tal que $0 \leq \theta \leq 360°$. A $(|z|, \theta)$ las llamaremos las coordenadas polares de z y a la ecuación (3) la representación polar del número complejo z. Al ángulo θ lo llamamos el ***argumento de*** z y lo denotamos por $arg(z)$ y según lo dicho aquí, $0 \leq arg(z) < 360°$. Entonces la relación entre las coordenadas polares (r, θ) y las coordenadas cartesianas (a, b) de z es $a = r \cdot \cos(\theta)$ y $b = r \cdot \mathrm{sen}\,(\theta)$, donde $r = \sqrt{a^2 + b^2} = |z|$. Ahora, ya que $\frac{b}{a} = \frac{r \cdot \mathrm{sen}(\theta)}{r \cdot \cos(\theta)} = \tan(\theta)$, la representación polar del complejo $z = a + bi$ es $z = \sqrt{a^2 + b^2}\,(\cos(\theta) + i\,\mathrm{sen}\,(\theta))$, donde θ es el ángulo entre 0° y 360° que está dado por

$$\theta = \begin{cases} \tan^{-1}\left(\frac{b}{a}\right) & \text{si } a > 0 \text{ y } b \geq 0 \quad (1^{\text{er}} \text{ cuadrante}) \\ \pi - \tan^{-1}\left(\frac{b}{|a|}\right) & \text{si } a < 0 \text{ y } b \geq 0 \quad (2^{\text{o}} \text{ cuadrante}) \\ \pi + \tan^{-1}\left(\frac{b}{a}\right) & \text{si } a < 0 \text{ y } b < 0 \quad (3^{\text{er}} \text{ cuadrante}) \\ 2\pi - \tan^{-1}\left(\frac{|b|}{a}\right) & \text{si } a < 0 \text{ y } b < 0 \quad (4^{\text{o}} \text{ cuadrante}) \\ \frac{\pi}{2} & \text{si } a = 0 \text{ y } b > 0 \\ \frac{3\pi}{2} & \text{si } a = 0 \text{ y } b < 0 \end{cases}$$

Ejemplo 12.3.1. Si $z = 1 + i$, entonces $|z| = \sqrt{2}$ y

$$\theta = \tan^{-1}\left(\frac{1}{1}\right) = \tan^{-1}(1) = 45° = \frac{\pi}{4},$$

por lo que $z = \sqrt{2}\,(\cos(45°) + i\,\mathrm{sen}(45°))$ es su representación polar.

Usando la representación polar podemos ubicar en el plano el producto de dos números complejos.
Sean $z = |z|(\cos(\theta) + i\,\mathrm{sen}(\theta))$ y $w = |w|(\cos(\phi) + i\,\mathrm{sen}(\phi))$. Entonces su producto es

$$z \cdot w = |z||w| \left[(\cos(\theta)\cos(\phi) - \mathrm{sen}(\theta)\,\mathrm{sen}(\phi)) + i\,(\cos(\theta)\,\mathrm{sen}(\phi) + \mathrm{sen}(\theta)\cos(\phi))\right]$$

Aplicando las identidades trigonométricas

$$\cos(\theta + \phi) = \cos(\theta)\cos(\phi) - \mathrm{sen}(\theta)\,\mathrm{sen}(\phi) \quad \text{y}$$
$$\mathrm{sen}(\theta + \phi) = \cos(\theta)\,\mathrm{sen}(\phi) + \mathrm{sen}(\theta)\cos(\phi)$$

obtenemos (figura 8)

$$z \cdot w = |z \cdot w|(\cos(\theta + \phi) + i\,\mathrm{sen}(\theta + \phi)).$$

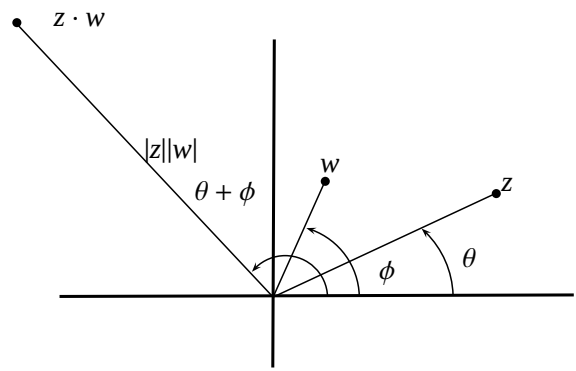


FIGURA 8. Interpretación geométrica del producto de dos números complejos

Ahora bien, como $0 \le \theta, \phi < 360°$, se tiene que $0 \le \theta + \phi < 720°$. Sin embargo debido a que $\cos(\theta + k \cdot 360°) = \cos(\theta)$ y $\mathrm{sen}(\theta + k \cdot 360°) = \mathrm{sen}(\theta)$ para cualquier entero k, obtenemos $z \cdot w = |z \cdot w|(\cos(\delta) + i\,\mathrm{sen}(\delta))$, donde

$$\delta = \begin{cases} \theta + \phi & \text{si } \theta + \phi < 360° \\ \theta + \phi - 360° & \text{si } \theta + \phi \ge 360°, \end{cases}$$

que expresado en términos de los argumentos es

$$arg(z \cdot w) = \begin{cases} arg(z) + arg(w) & \text{si } arg(z) + arg(w) < 360°, \\ arg(z) + arg(w) - 360° & \text{si } arg(z) + arg(w) \ge 360°. \end{cases}$$

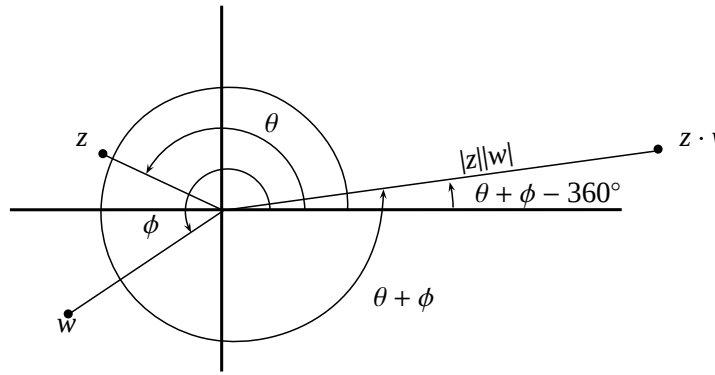


Figura 9. Argumento del producto de números complejos

En particular, se puede demostrar por inducción sobre n, (véase ejercicio 12.3.1), que la potencia n-ésima de un número complejo z está dada por la fórmula siguiente

$$z^n = |z|^n \left(\cos(n\theta) + i \operatorname{sen}(n\theta)\right),$$

donde $z = |z|\left(\cos(\theta) + i \operatorname{sen}(\theta)\right)$ y $n \in \mathbb{N}$.
La igualdad $\left(\cos(\theta) + i \operatorname{sen}(\theta)\right)^n = \cos(n\theta) + i \operatorname{sen}(n\theta)$ se conoce como la ***fórmula de De Moivre***.
Sean $z, w \in \mathbb{C}$. Diremos que z es una raíz ***n*-ésima** de w si $z^n = w$. Apliquemos todo lo anterior para encontrar todas las raíces n-ésimas de un número complejo. Recordemos que 360° es equivalente a 2π radianes.

Teorema 12.3.2. *Sea $w \neq 0$ un número complejo y $n \neq 0$ un número natural. Entonces existen exactamente n números complejos distintos $z_0, \ldots, z_{n-1}$ tales que $z_k^n = w$ para toda $k = 0, \ldots, n-1$ y están dados por*

$$z_k = \sqrt[n]{|w|}\left(\cos\left(\frac{\theta + k \cdot 2\pi}{n}\right) + i \operatorname{sen}\left(\frac{\theta + k \cdot 2\pi}{n}\right)\right),$$

donde $w = |w|\left(\cos(\theta) + i \operatorname{sen}(\theta)\right)$.

Demostración. Aplicando la fórmula de De Moivre, se tiene que para toda $k = 0, \ldots, n-1$

$$\begin{aligned} z_k^n &= \left(\sqrt[n]{|w|}\left(\cos\left(\tfrac{\theta+k\cdot 2\pi}{n}\right) + i\,\mathrm{sen}\left(\tfrac{\theta+k\cdot 2\pi}{n}\right)\right)\right)^n \\ &= |w|\left(\cos\left(n\tfrac{\theta+k\cdot 2\pi}{n}\right) + i\,\mathrm{sen}\left(n\tfrac{\theta+k\cdot 2\pi}{n}\right)\right) \\ &= |w|\left(\cos\left(\theta + k\cdot 2\pi\right) + i\,\mathrm{sen}\left(\theta + k\cdot 2\pi\right)\right) \\ &= |w|\left(\cos\left(\theta\right) + i\,\mathrm{sen}\left(\theta\right)\right) = w \end{aligned}$$

lo que significa que cada z_k ($k = 0, \ldots, n-1$) es una raíz n-ésima de w. Además todas son distintas: primero observamos que

$$\frac{\theta + 2k\pi}{2\pi} = \frac{\theta}{2\pi} + k < 1 + (n-1) = n$$

y por lo tanto $0 \leq \frac{\theta+2k\pi}{n} < 2\pi$, así que para cualesquiera $0 \leq k,\ j \leq n-1$, $k \neq j$ implica $\frac{\theta+2k\pi}{n} \neq \frac{\theta+2j\pi}{n}$.
Veamos que éstas son todas. Supongamos que $z = r\left(\cos\left(\phi\right) + i\,\mathrm{sen}\left(\phi\right)\right)$ es una raíz n-ésima de w, es decir, $z^n = w$. Entonces $|z^n| = |z|^n = r^n = |w|$, $\cos\left(n\phi\right) = \cos\left(\theta\right)$ y $\mathrm{sen}\left(n\phi\right) = \mathrm{sen}\left(\theta\right)$ y por lo tanto $\phi = \frac{\theta+k\cdot 2\pi}{n}$ para algún entero k. Para terminar lo único que nos queda demostrar es que $0 \leq k < n$ con lo que tendríamos que

$$z = z_k = \sqrt[n]{|w|}\left(\cos\left(\frac{\theta + k\cdot 2\pi}{n}\right) + i\,\mathrm{sen}\left(\frac{\theta + k\cdot 2\pi}{n}\right)\right),$$

donde $0 \leq k < n$. Pero esto se debe a que como $0 \leq \phi, \theta < 2\pi$, entonces $k = \frac{n\phi-\theta}{2\pi}$ satisface las desigualdades

$$k \geq \tfrac{0-\theta}{2\pi} > \tfrac{-2\pi}{2\pi} = -1 \ \text{ y } \ k \leq \tfrac{n\phi}{2\pi} < \tfrac{n\cdot 2\pi}{2\pi} = n$$

y ya que k es un entero, entonces $0 \leq k < n$. ∎

Ejemplo 12.3.3. Para cada $n > 0$, las raíces n-ésimas de 1, están dadas por

$$z_k = \cos\left(\frac{360^\circ \cdot k}{n}\right) + i\,\mathrm{sen}\left(\frac{360^\circ \cdot k}{n}\right), \quad k = 0, \ldots, n-1.$$

Para $n = 2$ las dos raíces de 1 son
$z_0 = \cos(0) + i\,\mathrm{sen}(0) = \cos(0) = 1$ y $z_1 = \cos\left(\frac{\pi}{2}\right) + i\,\mathrm{sen}\left(\frac{\pi}{2}\right) = \cos\left(\frac{\pi}{2}\right) = -1$.

Para $n = 3$ las raíces de 1 son
$z_0 = \cos(0) + i\,\mathrm{sen}(0) = \cos(0) = 1$,
$z_1 = \cos(\frac{5\pi}{6}) + i\,\mathrm{sen}(\frac{5\pi}{6}) = -\frac{1}{2} + \frac{1}{2}\sqrt{3}i$ y
$z_2 = \cos(240^\circ) + i\,\mathrm{sen}(240^\circ) = -\frac{1}{2} - \frac{1}{2}\sqrt{3}i$.

Para $n = 4$ las raíces de 1 son
$z_0 = \cos(0) + i\,\mathrm{sen}(0) = \cos(0) = 1$,
$z_1 = \cos(\frac{\pi}{2}) + i\,\mathrm{sen}(\frac{\pi}{2}) = i$,
$z_2 = \cos(\pi) + i\,\mathrm{sen}(\pi) = -1$ y
$z_3 = \cos(\frac{3\pi}{2}) + i\,\mathrm{sen}(\frac{3\pi}{2}) = -i$.

Ejemplo 12.3.4. Sea ξ una raíz n-ésima de la unidad, es decir, $\xi^n = 1$. Diremos que ξ es una **raíz n-ésima primitiva de 1** si $\xi^i \neq \xi^j$ para $i \neq j$, con $0 \leq i, j < n$. Esto es, una raíz n-ésima de 1, es primitiva si y sólo si $\xi^0, \xi^1, \xi^2, \ldots, \xi^{n-1}$ son todas las n raíces distintas de $z^n = 1$.
Para cada $n > 0$, siempre existe una raíz n-ésima primitiva de 1, siendo ésta,

$$\xi = \cos\left(\frac{2\pi}{n}\right) + i\,\mathrm{sen}\left(\frac{2\pi}{n}\right).$$

Por el teorema 12.3.2 y con la notación dada aquí las soluciones de $z^n = 1$ son

$$z_k = \cos\left(\frac{0 + 2k\pi}{n}\right) + i\,\mathrm{sen}\left(\frac{0 + 2k\pi}{n}\right) = \xi^k.$$

¿Existirá alguna otra raíz n-ésima de la unidad distinta de ξ que también sea primitiva? Como las raíces n-ésimas de 1 son de la forma ξ^k, la pregunta equivalente sería entonces ¿para qué valores de k, ξ^k es una raíz n-ésima primitiva de 1?
Supongamos que ξ^k es una raíz n-ésima primitiva de la unidad. Luego $\left(\xi^k\right)^i \neq \left(\xi^k\right)^j$ para $i \neq j$ con $0 \leq i, j \leq n-1$. Sea $d = (k, n)$ y supongamos que $d > 1$. Entonces $\frac{n}{d} < n$ y $\left(\xi^k\right)^{\frac{n}{d}} = (\xi^n)^{\frac{k}{d}} = 1$, lo cual contradice que ξ^k sea primitiva y por lo tanto debe ser $d = 1$. Inversamente, si $(k, n) = 1$, entonces ξ^k es una raíz n-ésima primitiva de 1 (véase ejercicio 12.3.39).

§§ Ejercicios sección 12.1.

12.1.1. Considerando los números complejos como pares ordenados, efectúese cada una de las siguientes operaciones:

(*a*) $(-2, 5) + (-1, 1)$
(*b*) $(0, 1) \cdot (1, -1)$
(*c*) $(4, -3) \cdot (2, 1)$
(*d*) $(3, 0) \cdot (-2, 5)$
(*e*) $\left(-\frac{1}{2}, \frac{3}{4}\right) \cdot \left(\frac{1}{4}, 1\right)$
(*f*) $(-2, 5) + (-2, 5) + (-2, 5)$ (compare con (d))

(*g*) $(1,1)\cdot(2,1)\cdot(3,1)$

12.1.2. Encuéntrese que $(a,b)\in\mathbb{R}^2$ satisface la expresión

$$(a,b)\cdot(2,-1)=(3,-4).$$

12.1.3. Véase qué propiedades de campo cumplen las siguientes operaciones $\widehat{+}$ y $\widehat{\cdot}$ definidas sobre $\mathbb{R}^2$:

$$(a,b)\widehat{+}(c,d)=(a+c,bd)\ \text{ y }\ (a,b)\widehat{\cdot}(c,d)=(ac,b+d).$$

En qué puntos fallan estas operaciones.

12.1.4. Dados complejos $z,w\in\mathbb{C}$ con $w\neq 0$ se define $\frac{z}{w}=z\cdot\left(w^{-1}\right)$.
Para $z_1,z_2,z_3,z_4\in\mathbb{C}$ con $z_1\neq 0$ y $z_2\neq 0$, demuestre que:

(1) $z_2\cdot\left(\frac{z_1}{z_2}\right)=z_1$;
(2) $\frac{z_1}{z_2}+\frac{z_3}{z_4}=\frac{z_1\cdot z_4+z_2\cdot z_3}{z_2\cdot z_4}$;
(3) $\frac{z_1}{z_2}\cdot\frac{z_3}{z_4}=\frac{z_1\cdot z_3}{z_2\cdot z_4}$;
(4) Si $z_3\neq 0$, entonces $\frac{\frac{z_1}{z_2}}{\frac{z_3}{z_4}}=\frac{z_1\cdot z_4}{z_2\cdot z_3}$.

12.1.5. Sea $z\in\mathbb{C}-\{0\}$. Definimos, para $n\in\mathbb{Z}$,

$$\begin{aligned} z^0&=1\\ z^{n+1}&=z^n\cdot z \quad \text{si } n>0\\ z^n&=(z^{-1})^{-n} \quad \text{si } n<0\end{aligned}$$

Demuestre que para todo $m,n\in\mathbb{Z}$ se cumple que:

(a) $z^m\cdot z^n=z^{m+n}$.
(b) $\frac{z^m}{z^n}=z^{m-n}$.
(c) $(z^m)^n=z^{mn}$.
(d) $(z\cdot w)^n=z^n\cdot w^n$.
(e) $\left(\frac{z}{w}\right)^n=\frac{z^n}{w^n}$.

12.1.6.
(1) Encontrar los valores de i^n para cada $n\in\mathbb{Z}$. (Sugerencia: Utilice el algoritmo de la división para n y 4.)
(2) Determine el valor de la suma $\sum_{k=0}^{n} i^k$ con $n\in\mathbb{N}$.

12.1.7. Encontrar los valores de $(1+i)^n+(1-i)^n$ para cada $n\in\mathbb{Z}$.

12.1.8. Calcular $\frac{(1+i)^n}{(1-i)^{n-2}}$, donde n es un entero tal que $n \geq 2$.

12.1.9. Demuestre que, si z_1, z_2 y $z_3 \in \mathbb{C}$, entonces

$$z_1^2 + z_2^2 + z_3^2 = z_1z_2 + z_2z_3 + z_3z_1$$

si y sólo si $\frac{z_3-z_1}{z_2-z_1} = \frac{z_1-z_2}{z_3-z_2}$.

12.1.10. Efectúese las operaciones indicadas y al final exprese el resultado en la forma $a + bi$:

(1) $(5 + 7i) + (8 + 2i)$
(2) $(11 + 2i) + (3 - 14i)$
(3) $(\sqrt{2} + \sqrt{3}i) - (6\sqrt{2} - 7\sqrt{3}i)$
(4) $2 - 8i + 7i^3 - 3i^7 + 16i^{20}$
(5) $i^8 + i^9 + \ldots + i^{17}$
(6) $(2 + i) \cdot (5 - 6i) + (-1 - i) \cdot (3 + i)$
(7) $(2 + 6i) \cdot (6 - 5i) - (4 - 11i)^3$
(8) $(7 - 6i)^2 + (6 - 7i)^2$
(9) $(1 + i) \cdot (2 + i) \cdot (3 + i)$
(10) $(3 + 2i) \cdot (7 - 8i) \cdot (-2 + 9i)$
(11) $(-5 + 3i)^4$
(12) $(i - 1)^6$
(13) $\left(2i^3\right)^5 - \left(3i^5\right)^4$
(14) $\frac{2-11i}{3-2i}$
(15) $\frac{5i}{6-7i} + \frac{2-3i}{5-8i}$
(16) $\frac{\sqrt{3}-\sqrt{7}i}{2\sqrt{3}+3\sqrt{7}i}$
(17) $\frac{8\sqrt{5}+21\sqrt{3}i}{2\sqrt{5}-3\sqrt{7}i} - \frac{\sqrt{5}+6\sqrt{3}i}{2\sqrt{5}-3i}$
(18) $\frac{(2+3i)\cdot(3-4i)}{4+5i}$
(19) $\frac{(1+2i)-(2+3i)}{(3+4i)+(4+5i)}$
(20) $\frac{(3-5i)\cdot(7+4i)}{(5+3i)\cdot(6-i)}$
(21) $\left(1 + \frac{3}{1+i}\right)^2$
(22) $\left(\frac{1+i}{1-i}\right)^{16} + \left(\frac{1-i}{1+i}\right)^8$
(23) $\left(\frac{-1+\sqrt{3}i}{2}\right)^6 + \left(\frac{1-\sqrt{7}i}{2}\right)^6$
(24) $1 + \frac{i}{1+\frac{i}{1+\frac{i}{1+i}}}$

12.1.11. Encuéntrese todos los números complejos $z \in \mathbb{C}$ tales que $z^2 \in \mathbb{R}$.

12.1.12. Encuentre los números complejos z tales que $w = \frac{2z-i}{2+iz}$ es

(a) Un número real;
(b) Un número imaginario puro.

12.1.13.

(1) Hallar todos los números reales a y b para que $-4 + ai = (b - 2i)(2 - 3i)$.
(2) Determine todos los valores de a en $\mathbb{R}$ para que $\frac{4+ai}{2+i}$ sea:
(a) Un número real;
(b) Un número imaginario puro.

§ § Ejercicios sección 12.2.

12.2.1. [1] Sean $z, w \in \mathbb{C}$. Demuestre que

(1) $Re(z + w) = Re(z) + Re(w)$, $Im(z + w) = Im(z) + Im(w)$.
(2) $Re(-z) = -Re(z)$, $Im(-z) = -Im(z)$.

12. 2.2. Demuestre que para $z, w \in \mathbb{C}$, $Re(z + w) = Re(z) + Re(w)$, $Im(z + w) = Im(z) + Im(w)$, $Re(-z) = -Re(z)$ y $Im(-z) = -Im(z)$.

12.2.3. Sean $z_1, z_2, \ldots, z_n \in \mathbb{C}$, $n \geq 2$. Demuestre que

[1] Proposición 12.2.2 pág. 396.

(a) $\overline{\left(\sum_{k=1}^{n} z_k\right)} = \sum_{k=1}^{n} \overline{z_k}$;
(b) $\overline{\left(\prod_{k=1}^{n} z_k\right)} = \prod_{k=1}^{n} \overline{z_k}$;
(c) $\left|\prod_{k=1}^{n} z_k\right| = \prod_{k=1}^{n} |z_k|$;
(d) $\left|\sum_{k=1}^{n} z_k\right| \leq \sum_{k=1}^{n} |z_k|$.

12.2.4. Sea $z \in \mathbb{C} - \{0\}$. Demuestre que para todo $m \in \mathbb{Z}$ se cumple que $\overline{z^m} = \overline{z}^m$.

12.2.5. Encuentre las partes real e imaginaria de los siguientes números complejos, donde $z = a + bi$, $a, b \in \mathbb{R}$:

(a) iz (b) $(1+i)(z+2)$ (c) $\frac{1+z}{1-z}$ (d) $\frac{1}{3z+2}$ (f) $\frac{z+3}{z-2}$
(g) $\frac{z+1}{2z-5}$ (h) $\frac{1-z}{1-z^2}$ (i) $\frac{z}{1+z^2}$ (j) $\frac{z+1}{z^2+z}$

12.2.6. Calcule el módulo de los siguientes números complejos:

(1) $(2-i)(-2+4i)(i-2)$ (2) $\left(\sqrt{3}-i\right)^6$ (3) i^{203}
(4) $\frac{3-i}{\sqrt{2}-i}$ (5) $\frac{\left(2+\sqrt{5}i\right)\left(1+\sqrt{3}i\right)^3}{\sqrt{3}+\sqrt{5}i}$

12.2.7. Si $z_1 = 1-i$, $z_2 = -2+4i$, $z_3 = \sqrt{3}-2i$. Hallar el valor numérico de cada una de las expresiones:

(1) $|2z_2 - 3z_1|^2$ (2) $(z_3 - \overline{z_3})^5$ (3) $|z_1\overline{z_2} + z_1\overline{z_1}|$
(4) $\left|\frac{z_1+z_2+1}{z_1-z_2+i}\right|$ (5) $\frac{1}{2}\left(\frac{z_3}{\overline{z_3}} + \frac{\overline{z_3}}{z_3}\right)$ (6) $\overline{(z_2+z_3)(z_1-z_3)}$
(7) $Re\left(2z_1^3 + 3z_2^2 - 5z_3^2\right)$ (8) $Im\left(\frac{z_1 z_2}{z_3}\right)$

12.2.8. [2] Sean $z, w \in \mathbb{C}$. Demuestre que

(1) $\overline{z} = z$ si y sólo si $Im(z) = 0$ (esto es $z \in \mathbb{R}$).
(2) $\overline{z} = -z$ si y sólo si $Re(z) = 0$.
(3) $\overline{(-z)} = -\overline{z}$.
(4) $\overline{\overline{z}} = z$.
(5) $\overline{(z-w)} = \overline{z} - \overline{w}$.

[2] Parte de la proposición 12.2.6 pág. 396.

(6) $z + \overline{z} = 2Re(z)$ y $z - \overline{z} = 2Im(z) \cdot i$.

12.2.9. [3] Sean $z, w \in \mathbb{C}$. Demuestre que

(1) $|z| \geq 0$ y $|z| = 0$ si y sólo si $z = 0$.
(2) $z \cdot \overline{z} = |z|^2$.
(3) $|Re| \leq |z|$, $|Im(z)| \leq |z|$.
(4) $|\overline{z}| = |z|$
(5) $|-z| = |z|$.

12.2.10. Demuestre que

(1) $z_1 = (2 + \sqrt{5}i)^7 + (2 - \sqrt{5}i)^7 \in \mathbb{R}$;
(2) $z_2 = \left(\frac{19+7i}{9-i}\right)^n + \left(\frac{20+5i}{7+6i}\right)^n \in \mathbb{R}$.

12.2.11. Encuentre todos los números complejos z tales que $w = \frac{z-1-i}{z+1+i}$ es

(a) Un número real;
(b) Tiene módulo 1.

12.2.12. Sean $z, w \in \mathbb{C} - \{0\}$. Demuestre que $|z + w| = |z| + |w|$ si y sólo si $z = \lambda \cdot w$ para algún $\lambda \in \mathbb{R}^+$.

12.2.13. Sean $z, w \in \mathbb{C}$. Demuestre que:

(a) $|z| - |w| \leq |z + w|$.
(b) $||z| - |w|| \leq |z - w|$.
(c) $\frac{1}{2}(|z| + |w|)\left|\frac{z}{|z|} + \frac{w}{|w|}\right| \leq |z + w|$, con $z \neq 0$ y $w \neq 0$.

12.2.14. Demuestre que $\pm i$ son los únicos números complejos cuyo cuadrado es -1.

12.2.15. Demuestre que

(1) Si z y w son números complejos tales que $z + w$ y $z \cdot w$ son ambos números reales, entonces $z = \overline{w}$.
(2) Si z y w son números complejos tales que $z + w$ es un número real y $z \cdot w$ es un número real negativo, entonces z y w son ambos números reales.

12.2.16. Hallar los números complejos z tales que $\overline{z} = z^2$.

12.2.17. (a) Dos números complejos no nulos son tales que $|z_1 + z_2| = |z_1 - z_2|$. Si $z_2 \neq 0$, demuestre que $\frac{z_1}{z_2}$ es imaginario puro.

[3] Parte del teorema 12.2.8 pág. 397.

(b) Si $|z_1| = |z_2|$ y $z_1 \neq z_2$, demuestre que $\frac{z_1+z_2}{z_1-z_2}$ es imaginario puro.

12.2.18. Determinar cuando se cumple la igualdad $Re(z \cdot w) = Re(z) \cdot Re(w)$.

12.2.19. Sea $z \in \mathbb{C}$ con $z \neq 0$. Demuestre que $z + \frac{1}{z}$ es un número real si y sólo si $Im(z) = 0$ o $|z| = 1$.

12.2.20. Dados $z, w \in \mathbb{C}$, definimos $d : \mathbb{C} \times \mathbb{C} \longrightarrow \mathbb{R}^+ \cup \{0\}$ como:

$$d(z, w) = |z - w|.$$

Pruebe que

(1) d está bien definida, esto es, $d(z, w) \geq 0$;
(2) $d(z, w) = 0$ si y sólo si $z = w$;
(3) $d(z, w) = d(w, z)$, para todo $z, w \in \mathbb{C}$;
(4) $d(z, w) \leq d(z, u) + d(u, w)$, para todo $z, w, u \in \mathbb{C}$.

12.2.21. Sean $z, w \in \mathbb{C}$ con $z \neq w$. Demuestre que $Re\left(\frac{w+z}{w-z}\right) = \frac{|w|^2-|z|^2}{|w-z|^2}$.

12.2.22. Sean $z_1, z_2 \in \mathbb{C}$ tales que $|z_1 + z_2| = \sqrt{3}$ y $|z_1| = |z_2| = 1$. Calcule $|z_1 - z_2|$.

12.2.23. Demuestre que para cualquier número complejo z

$$|z + 1| \geq \frac{1}{\sqrt{2}} \quad \text{o bien} \quad |z + 1| \geq 1.$$

12.2.24. Sea $z \in \mathbb{C}$. Demuestre que:

(a) Si $|z| = 2$, entonces $8 \leq |z + 6 + 8i| \leq 12$.
(b) Si $|z| = 1$, entonces $2 \leq |z^2 - 3| \leq 4$.

12.2.25. Sean $z_1, z_2, z_3 \in \mathbb{C}$. Demuestre las siguientes identidades:

(a) $|1 + z_1\overline{z_2}|^2 + |z_1 - z_2|^2 = (1 + |z_1|^2)(1 + |z_2|^2)$.
(b) $|z_1 + z_2|^2 + |z_1 + \overline{z_2}|^2 = 2(|z_1|^2 + |z_2|^2) + 2 \cdot Re(z_1) \cdot Re(z_2)$.
(c) $|z_1 + z_2 + z_3|^2 = |z_1 + z_2|^2 + |z_2 + z_3|^2 + |z_3 + z_1|^2$.
(d) $|z_1 + z_2 + z_3|^2 + |-z_1 + z_2 + z_3|^2 + |z_1 - z_2 + z_3|^2 + |z_1 + z_2 - z_3|^2 = 4\left(|z_1|^2 + |z_2|^2 + |z_3|^2\right)$.

12.2.26. Sean $z, w \in \mathbb{C}$.

(a) Demuestre que $|1 - \overline{z}w|^2 - |z - w|^2 = \left(1 - |z|^2\right)\left(1 - |w|^2\right)$.
(b) Suponga que $\overline{z}w \neq 1$ y que $|z| = 1$ o $|w| = 1$. Demuestre que

$$\left|\frac{z - w}{1 - \overline{z}w}\right| = 1.$$

(c) Suponga que $\overline{z}w \neq 1$ y que $|z| < 1$. Demuestre que $0 < |w| < 1$ si y sólo si

$$\left|\frac{z-w}{1-\overline{z}w}\right| < 1.$$

12.2.27. Sean $z_1, z_2, z_3 \in \mathbb{C}$ tales que

$$z_1 + z_2 + z_3 = 0 \quad \text{y} \quad |z_1| = |z_2| = |z_3| = 1.$$

Demuestre que $z_1^2 + z_2^2 + z_3^2 = 0$.

12.2.28. Encuentre algebraicamente las raíces cuadradas de

(1) $1 + \sqrt{3}i$	(2) $-1 - \sqrt{3}i$	(3) $2i$	(4) -16
(5) $-2i$	(6) $-i$	(7) $24 - 10i$	(8) $2 + 2\sqrt{3}i$
(9) $-8i$	(10) $5 - 12i$	(11) $3 - 4i$	(12) $3 + 4i$
(13) $-3 + 4i$	(14) $-3 - 4i$	(15) $12 + 5i$	(16) $15 + 8i$
(17) $-40 + 42i$			

12.2.29. La suma de dos números complejos es $5 - i$ y su producto es $8 + i$. Hallar los números.

12.2.30. Resolver las siguientes ecuaciones:

(1) $z^2 - 8(1-i)z + 63 - 16i = 0$	(2) $z^2 - 2iz - 9 - 6i = 0$	(3) $-5z^2 + \sqrt{2}z - 1 = 0$
(4) $z^2 + (2-3i)z - (5-5i) = 0$	(5) $iz^2 + (1+2i)z + 1 = 0$	(6) $z^4 + 6(1+i)z^2 + 5 + 6i = 0$
(7) $4z^4 - 5iz^2 + 1 = 0$	(8) $z^6 + z^3 + 1 = 0$	

12. 2.31. ¿Cuáles de las siguientes afirmaciones son ciertas? (Justifique su respuesta)

(1) $Im(4 + 7i) = 7i$	(2) $Im(z \cdot w) = Im(z) \cdot Im(w)$
(3) $Re(z \cdot w) = Re(\overline{z} \cdot w)$	(4) $\|z + w\| = \|z\| + \|w\|$
(5) Si $Im(z) > 0$, entonces $Re\left(\frac{1}{z}\right) < 0$.	(6) $z\overline{(w+i)} = \overline{z}(\overline{w} + i)$
(7) $\overline{z+w} = \overline{z} - \overline{w}$	(8) $\|z-1\| = \|\overline{z} - 1\|$
(9) $z^2 = \|z\|^2$	(10) Si $(z)^2 = (\overline{z})^2$, entonces $z \in \mathbb{R}$.
(11) $Re\,(z\overline{w} + \overline{z}w) = z\overline{w} + \overline{z}w$	(12) $Im\,(z\overline{w} - \overline{z}w) = z\overline{w} - \overline{z}w$

12.2.32. Sea $w = a + bi$ donde $a, b \in \mathbb{Z}$. Demuestre que $|w|$ es un entero si y sólo si $w = t \cdot z^2$ o $w = it \cdot z^2$, donde $z = r + si$ y $r, s, t \in \mathbb{Z}$.

12.2.33. Demuestre que existe una única función $\alpha : \mathbb{C} \longrightarrow \mathbb{R}$ tal que:

(1) $\alpha(x) = x$ para todo $x \in \mathbb{R}^+ \cup \{0\}$;
(2) $\alpha\,(z \cdot w) = \alpha\,(z) \cdot \alpha\,(w)$, para todo $z, w \in \mathbb{C}$;

(3) $\alpha(z+w) \leq \alpha(z) + \alpha(w)$, para todo $z, w \in \mathbb{C}$.

(Sugerencia: Demuestre que $\alpha(z) = 1$ para todo $z \in \mathbb{C}$ tal que $|z| = 1$.)

§§ Ejercicios sección 12.3.

12.3.1. Sea $z = |z|(\cos(\theta) + i\,\mathrm{sen}(\theta))$ un número complejo. Demuestre que para todo $n \in \mathbb{N}$:

$$z^n = |z|^n (\cos(n\theta) + i\,\mathrm{sen}(n\theta)),$$

12.3.2. Haga un dibujo que interprete geométricamente la definición de argumento de un número complejo. Véase página 404.

12.3.3. Sean $z_0, w \in \mathbb{C}$ tales que $z_0^n = w$. Demuestre que las n raíces distintas n-ésimas de w están dadas por $z_0 \cdot \xi^k$ para $k = 0, \ldots, n-1$ y donde ξ es una raíz n-ésima primitiva de 1.

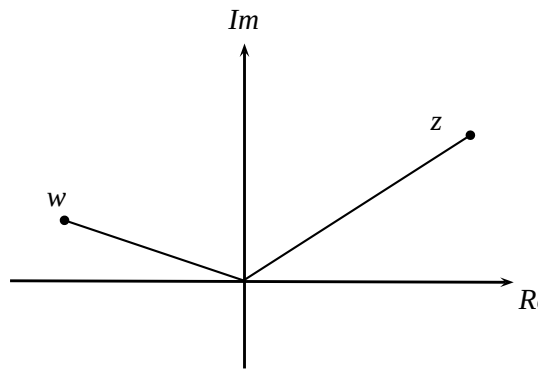
12.3.4. Represente cada uno de los siguientes números complejos en el plano complejo:

(1) $2 + i$	(2) -6	(3) $-1 - i$	(4) $6 - \sqrt{2}i$
(5) $3i$	(6) $2 - 7i$	(7) $-7 + \sqrt{3}i$	(8) $\left(1 - \sqrt{2}\right) i$

12.3.5. Sea $z \in \mathbb{C}$, $z \neq 0$.

(1) Explique como construir geométricamente a $-z$ y $\overline{z}$.
(2) Usando la identidad $z^{-1} = \frac{\overline{z}}{|z|^2}$, explique como construir a z^{-1}.

12.3.6. Considere la siguiente figura



Encuentre geométricamente los siguientes números complejos: $-z$, $\overline{w}$, $z+w$, $w-z$, $2\overline{w}+z$, $\frac{1}{2}z+(\overline{z+w})$.

12.3.7. Describa geométricamente los siguientes subconjuntos de $\mathbb{C}$:

(1) $\{z\in\mathbb{C}\mid Im(z)>0\}$
(2) $\{z\in\mathbb{C}\mid Re(z)>\frac{3}{2}\}$
(3) $\{z\in\mathbb{C}\mid Im(z)>0,-\frac{1}{2}\leq Re(z)\leq\frac{1}{2}\}$
(4) $\{z\in\mathbb{C}\mid Im(z)>0,-\frac{1}{2}\leq Re(z)\leq\frac{1}{2},|z|\geq 1\}$
(5) $\{z\in\mathbb{C}\mid z=-\overline{z}\}$
(6) $\{z\in\mathbb{C}\mid \overline{z}=z^{-1}\}$
(7) $\{z\in\mathbb{C}\mid |z-2i|\leq 1\}$
(8) $\{z\in\mathbb{C}\mid |z+1|>2\}$
(9) $\{z\in\mathbb{C}\mid |z-i|+|z+3|=10\}$
(10) $\{z\in\mathbb{C}\mid |z-2|>|z-3|\}$
(11) $\{z\in\mathbb{C}\mid |z|=Im(z)\}$
(12) $\{z\in\mathbb{C}\mid Re(z^2+5)=0\}$
(13) $\left\{z\in\mathbb{C}\mid \frac{\pi}{4}<arg\,(z)\leq\frac{3\pi}{4}\right\}$
(14) $\left\{z\in\mathbb{C}\mid \frac{\pi}{2}\leq arg\,(z)\leq\frac{7\pi}{4}\text{ y }|z|\leq 2\right\}$

12.3.8. Si $z,w\in\mathbb{C}$, demuestre la identidad del paralelogramo:

$$|z+w|^2+|z-w|^2=2\left(|z|^2+|w|^2\right).$$

Interprete geométricamente la identidad anterior.

12.3.9. Sea $z=a+bi\neq 0$, con $a,b\in\mathbb{R}$.

(1) Si $a\neq 0$, compruebe que el argumento de z viene está dado por

$$arg\,(z)=\tan^{-1}\left(\frac{b}{a}\right)+k\pi,$$

donde

$$k=\begin{cases}0 & \text{si } a>0 \text{ y } b\geq 0\\ 1 & \text{si } a<0\\ 2 & \text{si } a>0 \text{ y } b\leq 0.\end{cases}$$

(2) Si $a=0$ y $b\neq 0$, compruebe que el argumento de z viene está dado por

$$arg\,(z)=\begin{cases}\frac{\pi}{2} & \text{si } b>0\\ \frac{3\pi}{2} & \text{si } b<0.\end{cases}$$

12.3.10. Determinar el módulo, el argumento y la forma polar de los siguientes números complejos:

(1) $8i$
(2) $-3i$
(3) $4+4\sqrt{3}i$
(4) $2\sqrt{3}+2i$
(5) $7+7i$
(6) $\sqrt{3}-i$
(7) $-5+5i$
(8) $-3+3\sqrt{3}i$
(9) $\sqrt{2}+\sqrt{6}i$
(10) $(1-i)(6+6i)$
(11) $\left(-\frac{1}{4}+\frac{\sqrt{3}}{4}i\right)(2\sqrt{3}+2i)$
(12) $(1+i)^5$
(13) $\frac{1}{\sqrt{3}-i}$
(14) $\frac{-2i}{3+4i}$
(15) $\cos\left(\frac{\pi}{4}\right)-i\,\text{sen}\left(\frac{\pi}{4}\right)$
(16) $-\cos\left(\frac{7\pi}{6}\right)-i\,\text{sen}\left(\frac{7\pi}{6}\right)$

12.3.11. Calcule las coordenadas de los puntos del plano cuyo módulo es r y cuyo argumento es θ:

(1) $r = 3\sqrt{2}$, $\theta = \frac{5\pi}{4}$ (2) $r = 2$, $\theta = \frac{\pi}{6}$ (3) $r = 3$, $\theta = \frac{\pi}{2}$ (4) $r = 2$, $\theta = \frac{3\pi}{2}$
(5) $r = \sqrt{2}$, $\theta = \frac{\pi}{4}$ (6) $r = 4$, $\theta = \frac{2\pi}{3}$ (7) $r = 2$, $\theta = \frac{5\pi}{3}$ (8) $r = 5$, $\theta = \pi$

12.3.12. Encuentre los números complejos z tales que $w = \frac{2z-1}{z-2}$ tiene argumento igual a $\frac{\pi}{2}$.

12.3.13. Sean $a \in \mathbb{R}$ y $z \in \mathbb{C}$. Si $arg(z + a) = \frac{\pi}{6}$ y $arg(z - a) = \frac{2\pi}{3}$, hállese z.

12.3.14. Utilice la fórmula de De Moivre para elevar a la potencia indicada.

(1) $\left[\sqrt{2}\left(\cos\left(\frac{\pi}{12}\right) + i\,\mathrm{sen}\left(\frac{\pi}{12}\right)\right)\right]^3$ (2) $\left[\sqrt{3}\left(\cos\left(\frac{\pi}{10}\right) + i\,\mathrm{sen}\left(\frac{\pi}{10}\right)\right)\right]^4$ (3) $\left(-\cos\left(\frac{\pi}{6}\right) - i\,\mathrm{sen}\left(\frac{\pi}{6}\right)\right)^6$
(4) $\left(\cos\left(\frac{\pi}{60}\right) + i\,\mathrm{sen}\left(\frac{\pi}{60}\right)\right)^{40}$ (5) $\left(\cos\left(\frac{\pi}{60}\right) - i\,\mathrm{sen}\left(\frac{\pi}{60}\right)\right)^{75}$ (6) $(-2\sqrt{3} + 2i)^8$
(7) $\left(1 + \sqrt{3}i\right)^{12}$ (8) $(1 - \sqrt{3}i)^9$ (9) $(1 + i)^{1000}$

12.3.15. Para $n \in \mathbb{N}$. Demostrar que

(*a*) $(1 + i)^n = 2^{\frac{n}{2}}\left(\cos\left(\frac{n\pi}{4}\right) + i\,\mathrm{sen}\left(\frac{n\pi}{4}\right)\right)$.
(*b*) $(\sqrt{3} - i)^n = 2^n\left(\cos\left(\frac{n\pi}{6}\right) - i\,\mathrm{sen}\left(\frac{n\pi}{6}\right)\right)$.

12.3.16. Suponga que $0 \leq \theta < 2\pi$. Determinar la forma polar de los siguientes números complejos:

(*a*) $\cos(\theta) - i\,\mathrm{sen}(\theta)$.
(*b*) $\mathrm{sen}(\theta) + i(1 + \cos(\theta))$.
(*c*) $\cos(\theta) + \mathrm{sen}(\theta) + i(\mathrm{sen}(\theta) - \cos(\theta))$.
(*d*) $(1 - \cos(\theta)) + i\,\mathrm{sen}(\theta)$.

12.3.17. Expresa $arg(\overline{z})$ y $arg(-z)$ en términos de $arg(z)$.

12.3.18. Sean $z, w \in \mathbb{C}$, con $w \neq 0$.

(1) Demuestre que si $z = |z|(\cos(\theta) + i\,\mathrm{sen}(\theta))$ y $w = |w|(\cos(\phi) + i\,\mathrm{sen}(\phi))$, entonces

$$\frac{z}{w} = \frac{|z|}{|w|}(\cos(\theta - \phi) + i\,\mathrm{sen}(\theta - \phi))$$

(2) Explique por qué

$$arg\left(\frac{z}{w}\right) = \begin{cases} arg(z) - arg(w) & \text{si } arg(z) - arg(w) \geq 0°, \\ 360° + arg(z) - arg(w) & \text{si } arg(w) - arg(z) > 0°. \end{cases}$$

12.3.19. Si $z = \cos(\theta) + i\,\mathrm{sen}(\theta)$, exprésese

$$\frac{1}{1+z}, \quad \frac{1}{1-z} \quad \text{y} \quad \frac{1-z}{1+z}$$

en la forma $a + bi$.

12.3.20. El número complejo cuyo módulo es 8 y argumento 70° es el producto de dos números complejos uno de ellos tiene módulo 2 y argumento 40°. ¿Quién es el otro número complejo?

12.3.21. Demuestre por inducción que

$$(\cos(\theta_1) + i\,\mathrm{sen}(\theta_1)) \cdot \ldots \cdot (\cos(\theta_n) + i\,\mathrm{sen}(\theta_n)) = \cos(\theta_1 + \ldots + \theta_n) + i\,\mathrm{sen}(\theta_1 + \ldots + \theta_n)$$

12.3.22. Separando las partes real e imaginaria en

$$(\cos(\theta) + i\,\mathrm{sen}(\theta))^4 = \cos(4\theta) + i\,\mathrm{sen}(4\theta),$$

hállense expresiones de $\cos(4\theta)$ y $\mathrm{sen}(4\theta)$ en términos de $\cos(\theta)$ y $\mathrm{sen}(\theta)$.

12.3.23. Exprese $\cos(5\theta)$

(1) en términos de $\cos(\theta)$ y $\mathrm{sen}(\theta)$;
(2) sólo en términos de $\cos(\theta)$;
(3) sólo en términos de $\mathrm{sen}(\theta)$.

12.3.24. Exprese $\tan(6\theta)$ en términos de $\tan(\theta)$. Utilícese el desarrollo de $\tan(6\theta)$ para calcular $\tan(15°)$.

12.3.25. Deduce las identidades de Lagrange:

(1) $1 + \cos(\theta) + \cos(2\theta) + \ldots + \cos(n\theta) = \dfrac{\cos\left(\frac{n\theta}{2}\right)\mathrm{sen}\left(\frac{(n+1)\theta}{2}\right)}{\mathrm{sen}\left(\frac{\theta}{2}\right)}$,

(2) $\mathrm{sen}(\theta) + \mathrm{sen}(2\theta) + \ldots + \mathrm{sen}(n\theta) = \dfrac{\mathrm{sen}\left(\frac{n\theta}{2}\right)\mathrm{sen}\left(\frac{(n+1)\theta}{2}\right)}{\mathrm{sen}\left(\frac{\theta}{2}\right)}$,

donde θ es un ángulo tal que $\mathrm{sen}\left(\frac{\theta}{2}\right) \neq 0$ (Sugerencia: Usar la fórmula para la suma de una progresión geométrica)

12.3.26. Demuestre que la fórmula de De Moivre es válida para exponentes negativos, es decir,

$$(\cos(\theta) + i\,\mathrm{sen}(\theta))^{-n} = \cos(-n\theta) + i\,\mathrm{sen}(-n\theta)$$

para todo $n \in \mathbb{N} - \{0\}$.

12.3.27. Utilizando la representación polar de un número complejo calcula:

(1) $\dfrac{\left(\sqrt{3}+i\right)^5 (1-i)^{10}}{\left(-1-\sqrt{3}i\right)^{10}}$;

(2) $\dfrac{\left(2\sqrt{3}+2i\right)^8}{(1-i)^6} + \dfrac{(1+i)^6}{\left(2\sqrt{3}-2i\right)^8}$;

(3) $\frac{(-1+i)^4}{\left(\sqrt{3}-i\right)^{10}} + \frac{1}{\left(2\sqrt{3}+2i\right)^4}$;
(4) $\left(1+\sqrt{3}i\right)^n + \left(1-\sqrt{3}i\right)^n$.

12. 3.28. En cada caso, calcule las raíces que se indican y represéntalas en el plano:

(1) Raíces cúbicas de 8.
(2) Raíces cuartas de -16.
(3) Raíces cuartas de $-1+\sqrt{3}i$.
(4) Raíces cuartas de i.
(5) Raíces quintas de $-i$.
(6) Raíces quintas de $-4+4i$.
(7) Raíces sextas de i.
(8) Raíces sextas de -3^6.
(9) Raíces octavas de 2^8.

12.3.29. Resuelve las siguientes ecuaciones.

(1) $z^3 = (1-z)^3$
(2) $(2z-1)^3 = (z-2)^3$
(3) $(z+1)^4 = 81z^4$
(4) $16z^4 = (z-1)^4$

12.3.30.

(*a*) Demuestre que $\frac{1+\cos(\alpha)+i\,\mathrm{sen}(\alpha)}{1-\cos(\alpha)-i\,\mathrm{sen}(\alpha)} = i\cot\left(\frac{\alpha}{2}\right)$.
(*b*) Utilizando el inciso (*a*), pruebe que las soluciones de la ecuación

$$(z-1)^5 - (z+1)^5 = 0$$

son:

$$0,\ \pm i\cot\left(\frac{\pi}{5}\right),\ \pm i\cot\left(\frac{2\pi}{5}\right).$$

12.3.31. Demuestre que las n raíces n-ésimas de 1 son los vértices de un n-ágono regular inscrito en el círculo unitario, uno de cuyos vértices es 1.

12.3.32. El centro de un cuadrado es el punto $-2+i$. Un vértice es $1+3i$. Hállense los otros.

12. 3.33. Hallar los vértices de un hexágono regular con centro en 0 y uno de cuyos vértices es i.

12.3.34. Si w es una raíz n-ésima de la unidad, $w \neq 1$, demuestre que

(1) $1 + w + w^2 + \cdots + w^{n-1} = 0$.
(2) $1 + 2w + 3w^2 + \cdots + nw^{n-1} = -\frac{1}{1-w}$.

¿Cuánto valen estas sumas si $w = 1$?

12.3.35. Demuestre que

(1) La suma de las raíces n-ésimas de la unidad es 0.
(2) El producto de las raíces n-ésimas de la unidad es -1 si n es par y 1 si n es impar.

12.3.36. Considere el n-ágono regular inscrito en el círculo unitario en $\mathbb{C}$ y considere las $n-1$ diagonales obtenidas conectando un vértice fijo con todos los otros vértices. Demuestre que el producto de sus longitudes es n. (Sugerencia: suponga que los vértices están unidos al vértice fijo 1 y aplique el ejercicio 12.3.34 (1)).

12. 3.37. Determinar las raíces n-ésimas primitivas de la unidad para $n = 2, 3, 4, 5, 6$ y 12.

12.3.38. Sea $n > 0$. Probar que $\xi \in \mathbb{C}$ es una raíz n-ésima primitiva de la unidad si y sólo si $\overline{\xi}$ lo es.

12.3.39. Sea ξ una raíz n-ésima primitiva de 1. Demuestre que

(1) n es el mínimo entero positivo tal que $\xi^n = 1$.
(2) Si $m > 0$ y $\xi^m = 1$, entonces $n \mid m$.
(3) Si $(k, n) = 1$, entonces ξ^k es una raíz n-ésima primitiva de 1.

12.3.40. Sea ξ una raíz primitiva quinta de 1 y sea $\zeta = \xi + \frac{1}{\xi}$. Pruebe que $\zeta^2 + \zeta = 1$. Utilícese esto para mostrar que $\cos(72°) = \frac{-1+\sqrt{5}}{4}$.

12.3.41. Sea $n > 0$ y considere el conjunto

$$\mu_n = \left\{ z \in \mathbb{C} \mid z^n = 1 \right\}.$$

Demuestre que

(1) μ_n es cerrado bajo productos, es decir, si $z, w \in \mu_n$, entonces $zw \in \mu_n$.
(2) μ_n es cerrado bajo inversos, es decir, si $z \in \mu_n$, entonces $z^{-1} \in \mu_n$.
(3) $-1 \in \mu_n$ si y sólo si n es par.

12.3.42. Con las notaciones del ejercicio anterior, para enteros $m, n > 0$, demuestre que

(1) $\mu_m \subseteq \mu_n$ si y sólo si $m \mid n$;
(2) $\mu_m \cap \mu_n = \mu_{(m,n)}$.

12.3.43. Sean $z_0, w \in \mathbb{C}$ tales $z_0^n = w$. demuestre que las n raíces distintas n-ésimas de w están dadas por $z_0 \cdot \xi^k$ para $k = 0, 1, \ldots, n-1$ y donde ξ es una raíz n-ésima primitiva de 1.

12.3.44. Sea $\xi = \cos\left(\frac{2\pi}{n}\right) + i\,\mathrm{sen}\left(\frac{2\pi}{n}\right)$ con $n > 0$. Demuestre que
(1) $1 + \xi^k + \xi^{2k} + \cdots + \xi^{(n-1)k} = 0$, si $n \nmid k$,
(2) $1 + \xi^k + \xi^{2k} + \cdots + \xi^{(n-1)k} = n$, si $n \mid k$.

Cualquier relación entre números, funciones y operaciones se hace transparente, generalmente aplicable y completamente productiva sólo si ha sido aislada a partir de objetos particulares y formulada como conceptos universalmente válidos.

Emmy Noether
1882 - 1935

***Capítulo* 13**

El anillo de polinomios

§ 13.1. El anillo de polinomios

Definición 13.1.1*. Sea A un anillo conmutativo con 1. Un polinomio en x con coeficientes en A es una expresión del tipo*

$$\boldsymbol{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 x^0},$$

donde $n \in \mathbb{N}$ y $a_i \in A$ para todo $i = 0, 1, \ldots, n$.

Al conjunto de polinomios en x con coeficientes en A lo denotamos por $\boldsymbol{A[x]}$ y usaremos $f(x), g(x)$, etc para denotar a sus elementos. Al polinomio

$$0 \cdot x^n + 0 \cdot x^{n-1} + \cdots + 0 \cdot x + 0 \cdot x^0$$

lo llamamos el ***polinomio cero*** (sin importar el valor de n) y lo denotamos por 0. A un polinomio de la forma $\boldsymbol{a_k \cdot x^k}$ se le llama ***monomio***.

Dado un polinomio $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 x^0$, donde no todas las a_i son cero, si para alguna j, $0 \leq j \leq n$, $a_j = 0$, omitiremos el monomio $a_j \cdot x^j$ en la expresión del polinomio y el término $a_0 \cdot x^0$ lo escribiremos simplemente como a_0.

Por ejemplo, el polinomio $0 \cdot x^6 + 5 \cdot x^5 + 0 \cdot x^4 + 2 \cdot x^3 + x^2 + 0 \cdot x + 1 \cdot x^0$ se escribirá simplemente como $5 \cdot x^5 + 2 \cdot x^3 + x^2 + 1$. Por otro lado, si algún coeficiente del polinomio es de la forma $-a_j$, lo escribiremos como

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_{j-1} x^{j-1} - a_j x^j + a_{j+1} x^{j+1} + \cdots + a_1 x + a_0 x^0.$$

Por ejemplo, escribimos

$$3 \cdot x^4 - 2 \cdot x^3 - x^2 + x$$

en lugar de $3 \cdot x^4 + (-2) \cdot \cdot x^3 + (-1) \cdot x^2 + x$. A cada elemento $a \in A$ lo identificamos con el polinomio $a \cdot x^0$.

Con el fin de presentar de una manera simple la igualdad de polinomios y las operaciones entre ellos, introducimos las expresiones (series) $\sum_{\boldsymbol{i=0}}^{\boldsymbol{\infty}} \boldsymbol{a_i \cdot x^i}$ para los polinomios, en donde casi todos los coeficientes son cero, lo que significa que para algún $n \in \mathbb{N}$, $a_j = 0$ para toda $j > n$, esto es, solamente para un número finito de valores de i se tiene $a_i \neq 0$. Con estas nuevas expresiones el polinomio 0 es $\sum_{i=0}^{\infty} 0 \cdot x^i$.

Definición 13.1.2. *Dos polinomios* $\sum_{i=0}^{\infty} a_i \cdot x^i$ *y* $\sum_{i=0}^{\infty} b_i \cdot x^i$ *serán iguales si* $a_i = b_i$, *para toda* $i = 0, 1, 2, \ldots$.

Según la definición anterior un polinomio $f(x) = \sum_{i=0}^{\infty} a_i \cdot x^i$ es distinto del polinomio 0 si y sólo si $a_i \neq 0$ para alguna $i = 0, 1, 2, \ldots$.

§ 13.2. Operaciones en $A[x]$

Introduciremos ahora la suma y el producto en $A[x]$, donde A es un anillo conmutativo.

Definición 13.2.1. *Sean* $f(x) = \sum_{i=0}^{\infty} a_i \cdot x^i$ *y* $g(x) = \sum_{i=0}^{\infty} b_i \cdot x^i$ *polinomios en* $A[x]$. *La suma de* $f(x)$ *y* $g(x)$ *es el polinomio, denotado como* $\boldsymbol{f(x) + g(x)}$, *dado por*

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

Evidentemente $f(x) + g(x) \in A[x]$, ya que como para alguna $n \in \mathbb{N}$, $a_j = 0$ para toda $j > n$ y para alguna $m \in \mathbb{N}$ $b_k = 0$ para toda $k > m$, se tiene entonces que $a_j + b_j = 0$ para toda $j > \text{máx}\{n, m\}$. Además recuerde que A es un anillo y por lo tanto $a_j + b_j \in A$ para toda $j = 1, 2, \ldots$.

La suma de polinomios tiene las siguientes propiedades.

Teorema 13.2.2. *Sea* A *un anillo conmutativo y* $f(x), g(x)$ *y* $h(x)$ *polinomios en* $A[x]$. *Entonces*

(1) $(f(x) + g(x)) + h(x) = f(x) + (g(x) + h(x))$
(2) $f(x) + g(x) = g(x) + f(x)$
(3) $f(x) + 0 = f(x)$
(4) *Existe* $t(x) \in A[x]$ *tal que* $f(x) + t(x) = 0$

Demostración. Sea $f(x) = \sum_{i=0}^{\infty} a_i \cdot x^i$, $g(x) = \sum_{i=0}^{\infty} b_i \cdot x^i$ y $h(x) = \sum_{i=0}^{\infty} c_i \cdot x^i$. Demostraremos (1), (3) y (4) y dejamos como ejercicio (2).

(1)

$$\begin{aligned}
(f(x) + g(x)) + h(x) &= \left(\sum_{i=0}^{\infty} a_i \cdot x^i + \sum_{i=0}^{\infty} b_i \cdot x^i\right) + \sum_{i=0}^{\infty} c_i \cdot x^i \\
&= \sum_{i=0}^{\infty} (a_i + b_i)\, x^i + \sum_{i=0}^{\infty} c_i \cdot x^i \\
&= \sum_{i=0}^{\infty} ((a_i + b_i) + c_i)\, x^i \\
&= \sum_{i=0}^{\infty} (a_i + (b_i + c_i))\, x^i \\
&= \sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} (b_i + c_i) \cdot x^i \\
&= \sum_{i=0}^{\infty} a_i \cdot x^i + \left(\sum_{i=0}^{\infty} b_i \cdot x^i + \sum_{i=0}^{\infty} c_i \cdot x^i\right) \\
&= f(x) + (g(x) + h(x)).
\end{aligned}$$

(3) $f(x) + 0 = \sum_{i=0}^{\infty} a_i \cdot x^i + \sum_{i=0}^{\infty} 0 \cdot x^i = \sum_{i=0}^{\infty} (a_i + 0) \cdot x^i = \sum_{i=0}^{\infty} a_i \cdot x^i = f(x)$.

(4) Sea $t(x) = \sum_{i=0}^{\infty} (-a_i) \cdot x^i$. Entonces

$$f(x) + t(x) = \sum_{i=0}^{\infty} a_i \cdot x^i + \sum_{i=0}^{\infty} (-a_i) \cdot x^i = \sum_{i=0}^{\infty} (a_i - a_i) \cdot x^i = \sum_{i=0}^{\infty} 0 \cdot x^i = 0. \quad \blacksquare$$

Obsérvese que las propiedades de la suma de polinomios son consecuencia de las respectivas propiedades de la suma en A.

Definición 13.2.3. *Sean* $f(x) = \sum_{i=0}^{\infty} a_i \cdot x^i$ *y* $g(x) = \sum_{i=0}^{\infty} b_i \cdot x^i$ *polinomios en* $A[x]$. *El producto de* $f(x)$ *y* $g(x)$ *es el polinomio* $f(x) \cdot g(x) = \sum_{i=0}^{\infty} c_i \cdot x^i$, *donde* $c_i = \sum_{j+k=i} a_j \cdot b_k$ *para toda* $i = 0, 1, 2, \ldots$.

Para mostrar que la definición del producto está bien dada, basta observar que si n y m son tales que $a_j = 0$ para todo $j > n$ y $b_k = 0$ para toda $k > m$, entonces $c_i = \sum_{j+k=i} a_j \cdot b_k = 0$ debido a que $i = j + k > n + m$ implica que $j > n$ o $k > m$ (si $j \leq n$ y $k \leq m$, entonces $j + k \leq n + m$ que no es el caso) y esto a su vez implica, en cualquiera de los casos, que $a_j \cdot b_k = 0$ y así $c_i = \sum_{j+k=i} a_j \cdot b_k = 0$. Por último es claro que $c_i = \sum_{j+k=i} a_j \cdot b_k \in A$.
Las propiedades del producto son las siguientes.

Teorema 13.2.4. *Sea A un anillo conmutativo y $f(x), g(x)$ y $h(x)$ polinomios en $A[x]$. Entonces*

(1) $(f(x) \cdot g(x)) \cdot h(x) = f(x) \cdot (g(x) \cdot h(x))$
(2) $f(x) \cdot g(x) = g(x) \cdot f(x)$
(3) $f(x) \cdot 1 = f(x)$
(4) $f(x) \cdot (g(x) + h(x)) = f(x) \cdot g(x) + f(x) \cdot h(x)$

Demostración. Sea $f(x) = \sum_{i=0}^{\infty} a_i \cdot x^i$, $g(x) = \sum_{i=0}^{\infty} b_i \cdot x^i$ y $h(x) = \sum_{i=0}^{\infty} c_i \cdot x^i$. Demostraremos (2), (3) y (4) dejando como ejercicio (1).

(2) Sean $f(x) \cdot g(x) = \sum_{i=0}^{\infty} d_i \cdot x^i$, donde $d_i = \sum_{j+k=i} a_j \cdot b_k$ para toda $i = 0, 1, 2, \ldots$ y $g(x) \cdot f(x) = \sum_{i=0}^{\infty} e_i \cdot x^i$, donde $e_i = \sum_{j+k=i} b_j \cdot a_k$ para toda $i = 0, 1, 2, \ldots$. Debemos demostrar que $d_i = e_i$ para toda $i = 0, 1, 2, \ldots$.

$$d_i = \sum_{j+k=i} a_j \cdot b_k = \sum_{k+j=i} b_k \cdot a_j = e_i.$$

(3) $1 = \sum_{i=0}^{\infty} d_i \cdot x^i$, donde $d_0 = 1$ y $d_k = 0$ para toda $k > 0$. $f(x) \cdot 1 = \sum_{i=0}^{\infty} e_i \cdot x^i$, donde $e_i = \sum_{j+k=i} a_j \cdot d_k$. Considerando el valor de d_k obtenemos

$$e_i = \sum_{j+k=i} a_j \cdot d_k = \sum_{j+0=i} a_j \cdot 1 = \sum_{j=i} a_j = a_i$$

y por lo tanto $f(x) \cdot 1 = f(x)$.

(4) Sean $f(x)(g(x)+h(x)) = \left(\sum_{i=0}^{\infty} a_i \cdot x^i\right)\left(\sum_{i=0}^{\infty}(b_i+c_i)\cdot x^i\right) = \sum_{i=0}^{\infty} d_i \cdot x^i$, donde $d_i = \sum_{j+k=i} a_j(b_k+c_k)$; $f(x)\cdot g(x) = \sum_{i=0}^{\infty} u_i \cdot x^i$, donde $u_i = \sum_{j+k=i} a_j \cdot b_k$ y $f(x)\cdot h(x) = \sum_{i=0}^{\infty} e_i \cdot x^i$, donde $e_i = \sum_{j+k=i} a_j \cdot c_k$. Debemos demostrar que $d_i = u_i + e_i$ para toda $i = 0, 1, 2, \ldots$.

$$d_i = \sum_{j+k=i} a_j(b_k+c_k) = \sum_{j+k=i}\left(a_j \cdot b_k + a_j \cdot c_k\right) = \sum_{j+k=i} a_j \cdot b_k + \sum_{j+k=i} a_j \cdot c_k = u_i + e_i. \quad \blacksquare$$

De los teoremas 13.2.2 y 13.2.4 obtenemos el siguiente

Teorema 13.2.5. *Si A es un anillo conmutativo, entonces $A[x]$ es un anillo conmutativo.*

Así como las propiedades de anillo de $A[x]$ se heredan de A, sucede lo mismo cuando A es un dominio entero.

Teorema 13.2.6. *Si A es un dominio entero, entonces $A[x]$ es un dominio entero.*

Demostración. Sean $f(x) = \sum_{i=0}^{\infty} a_i \cdot x^i$ y $g(x) = \sum_{i=0}^{\infty} b_i \cdot x^i$ ambos distintos de 0. Debemos demostrar que $f(x)\cdot g(x) \neq 0$. Como $f(x)$ y $g(x)$ son distintos de 0, entonces existen $n, m \in \mathbb{N}$ tales que $a_n \neq 0$ y $a_k = 0$ para toda $k > n$ y $b_m \neq 0$ y $b_j = 0$ para toda $j > m$. Sea $f(x)\cdot g(x) = \sum_{i=0}^{\infty} c_i x^i$, donde $c_i = \sum_{j+k=i} a_k \cdot b_j$. Mostraremos que $c_{m+n} = \sum_{j+k=m+n} a_k \cdot b_j \neq 0$. Existen dos posibilidades para k y j que son ($k > n$ o $j > m$) o ($k \leq n$ y $j \leq m$). En el primer caso se tendrá que $a_k = 0$ o $b_j = 0$ y por lo tanto $a_k \cdot b_j = 0$ y en el segundo caso forzosamente $k = n$ y $j = m$, ya que si no es así, $k + j < n + m$ y por lo tanto $a_k \cdot b_j$ no aparece como sumando en c_{n+m}. Concluimos entonces que $c_{m+n} = \sum_{k+j=n+m} a_k \cdot b_j = a_n \cdot b_m \neq 0$ puesto que $a_n \neq 0$ y $b_m \neq 0$ y A es un dominio entero. Luego $f(x)\cdot g(x) \neq 0$. ∎

Uno de los conceptos importantes en el anillo de polinomios es el *grado de un polinomio*, y será mediante este concepto que podremos adaptar al anillo de polinomios resultados de los enteros como lo es el Algoritmo de la división.

Definición 13.2.7. *Sea A un anillo y $f(x) = \sum_{i=0}^{\infty} a_i \cdot x^i$ un polinomio distinto de* 0 *en $A[x]$. Al elemento $a_n \neq 0$ de A tal que $a_k = 0$ para toda $k > n$ lo llamaremos el* **coeficiente principal** *de $f(x)$ y en este caso decimos que el* **grado** *de $f(x)$ es n y lo denotamos por $\partial f(x) = n$ y cuando el coeficiente principal es 1 diremos que el polinomio es* **mónico**.

Así pues, el grado de un polinomio $f(x) = \sum_{i=0}^{\infty} a_i \cdot x^i \neq 0$ es el máximo número natural n tal que $a_n \neq 0$. Como se puede apreciar el polinomio cero no le asignamos ningún grado por obvias razones. El grado de un polinomio es entonces una función $\partial : A[x] - \{0\} \longrightarrow \mathbb{N}$ y puesto que vamos a trabajar en un dominio A, las propiedades de ∂, cuando A es un dominio entero, son las siguientes:

Teorema 13.2.8. *Sea A un dominio y sean $f(x)$ y $g(x)$ polinomios distintos de* 0 *en $A[x]$.*

(1) *Si $f(x) + g(x) \neq 0$, entonces $\partial(f(x) + g(x)) \leq \text{máx}\{\partial f(x), \partial g(x)\}$.*
(2) *Si $\partial f(x) \neq \partial g(x)$, entonces $\partial(f(x) + g(x)) = \text{máx}\{\partial f(x), \partial g(x)\}$.*
(3) *$\partial(f(x) \cdot g(x)) = \partial f(x) + \partial g(x)$.*

Demostración. Sean $f(x) = \sum_{i=0}^{\infty} a_i \cdot x^i$ y $g(x) = \sum_{i=0}^{\infty} b_i \cdot x^i$ con $a_n \neq 0$, $b_m \neq 0$, $a_k = 0$ para toda $k > n$ y $b_j = 0$ para toda $j > m$. Esto es $\partial f(x) = n$ y $\partial g(x) = m$.

(1) Supongamos $n \geq m$. $f(x) + g(x) = \sum_{i=0}^{\infty} (a_i + b_i) \cdot x^i$, donde $a_k + b_k = 0$ para toda $k > n$ y por lo tanto $\partial(f(x) + g(x)) \leq n = \text{máx}\{\partial f(x), \partial g(x)\}$.
(2) Supongamos $n > m$. Como en el inciso (1), $a_k + b_k = 0$ para toda $k > n$. Debido a que $b_n = 0$, entonces $a_n + b_n = a_n \neq 0$ y por lo tanto

$$\partial(f(x) + g(x)) = n = \text{máx}\{\partial f(x), \partial g(x)\}.$$

(3) En el caso del producto $f(x) \cdot g(x)$, como se vio en la demostración del teorema 13.2.6, si $f(x) \cdot g(x) = \sum_{i=0}^{\infty} c_i \cdot x^i$, se tiene que $c_{m+n} = a_n \cdot b_m \neq 0$ y $c_i = 0$ para toda $i > n + m$ y por lo tanto $\partial(f(x) \cdot g(x)) = n + m = \partial f(x) + \partial g(x)$. ∎

Corolario 13.2.9. *Si A es un dominio, entonces los polinomios en $A[x]$ que son invertibles son los elementos de A que lo son. En el caso particular cuando A es campo, estos elementos son $A - \{0\}$.*

Demostración. Si $f(x) \in A[x]$ es invertible, existe $g(x) \in A[x]$ tal que $f(x) \cdot g(x) = 1$ y por (3) del Teorema 13.2.8, $\partial f(x) + \partial g(x) = 0$ y por lo tanto $\partial f(x) = 0$, es decir, $f(x)$ es un elemento de A. Si A es campo los elementos invertibles de $A[x]$ son los elementos de $A - \{0\}$. ∎

Los polinomios de grado cero en $A[x]$ son justamente los elementos de $A - \{0\}$ y los llamamos polinomios constantes.

§ 13.3. Divisibilidad

A partir de esta sección estudiaremos el anillo de polinomios $K[x]$ donde K es un campo (véase definición 7.7.14). Recordamos que un campo es en particular un dominio entero y por lo tanto $K[x]$ es un dominio entero así que los resultados obtenidos en las dos secciones anteriores son válidos para $K[x]$. El desarrollo que se hará es muy similar al que se hizo para los enteros (sección 7.1 a 7.3) en donde muchos de los teoremas que veremos aquí se obtienen intercambiando $\mathbb{Z}$ por $K[x]$ y en su caso la comparación de enteros mediante el orden se sustituirá por la comparación de polinomios mediante el grado; tal es el caso por ejemplo del Algoritmo de la División.

Definición 13.3.1. *Sea K un campo y sean $f(x), g(x) \in K[x]$. Diremos que* **$f(x)$ divide a $g(x)$** *y lo denotaremos* **$f(x) \mid g(x)$**, *si existe $h(x) \in K[x]$ tal que $f(x) \cdot h(x) = g(x)$.*

Ejemplo 13.3.2.
(1) $x^2 + 1 \mid 3x^7 + 3x^5 + 2x^3 - x^2 + 2x - 1$ ya que

$$\left(x^2 + 1\right)\left(3x^5 + 2x - 1\right) = 3x^7 + 3x^5 + 2x^3 - x^2 + 2x - 1 \text{ en } \mathbb{Q}[x].$$

(2) $\sqrt{2}x^3 + \pi x^2 - \sqrt{5} \mid 2x^4 + (\pi + 1)\sqrt{2}x^3 + \pi x^2 - \sqrt{10}x - \sqrt{5}$ ya que $\left(\sqrt{2}x^3 + \pi x^2 - \sqrt{5}\right)\left(\sqrt{2}x + 1\right) = 2x^4 + (\pi + 1)\sqrt{2}x^3 + \pi x^2 - \sqrt{10}x - \sqrt{5}$ en $\mathbb{R}[x]$.
(3) $x + (i + 1) \mid x^2 + 2x + 2$ ya que $(x + (i + 1))(x - (i - 1)) = x^2 + 2x + 2$ en $\mathbb{C}[x]$.

Es muy importante tomar en cuenta el campo K con el que trabajamos ya que, por ejemplo, el polinomio $x^2 + 1$ en $\mathbb{R}[x]$ solamente es divisible por por los elementos distintos de cero de $\mathbb{R}$ y múltiplos constantes de él. Sin embargo, si consideramos a $x^2 + 1$ como polinomio en $\mathbb{C}[x]$, $x^2 + 1$ además de ser divisible por los elementos distintos de cero de $\mathbb{C}$, también lo divide por ejemplo $x + i$.
Las propiedades inmediatas de la definición (compárese con el teorema 7.1.1) son

Teorema 13.3.3. *Sean $f(x), g(x)$ y $h(x)$ polinomios en $K[x]$. Entonces*

(1) *$a \mid f(x)$ para toda $a \in K - \{0\}$.*
(2) *Si $f(x) \mid g(x)$, entonces $a \cdot f(x) \mid b \cdot g(x)$ para cualesquiera $a \in K - \{0\}$ y $b \in K$. En particular $f(x) \mid f(x)$ y $f(x) \mid 0$.*
(3) *Si $f(x) \mid g(x)$, y $g(x) \mid h(x)$, entonces $f(x) \mid h(x)$.*
(4) *Si $f(x) \mid g(x)$, y $f(x) \mid h(x)$, entonces $f(x) \mid r(x) \cdot g(x) + s(x) \cdot h(x)$ para cualesquiera $r(x), s(x) \in K[x]$. En particular $f(x) \mid g(x) + h(x)$.*
(5) *Si $0 \mid f(x)$, entonces $f(x) = 0$. Esto es, el único polinomio que es divisible por 0 es el polinomio cero.*
(6) *Si $f(x) \mid g(x)$ y $g(x) \neq 0$, entonces $f(x) \neq 0$ y $\partial f(x) \leq \partial g(x)$.*
(7) *Si $f(x) \mid g(x)$ y $g(x) \mid f(x)$, entonces $f(x) = a \cdot g(x)$ para alguna $a \in K - \{0\}$.*

Demostración. Las demostraciones son totalmente análogas a las correspondientes para los enteros, así que solamente demostraremos (6) y (7).

(6) Si $f(x) \mid g(x)$, entonces $f(x) \cdot r(x) = g(x)$ para algún polinomio $r(x) \in K[x]$ y como $g(x) \neq 0$, debe ser $f(x) \neq 0$ y $r(x) \neq 0$. Tomando grados y aplicando el teorema 13.2.8, tenemos que $\partial f(x) + \partial r(x) = \partial g(x)$ y ya que $\partial r(x) \geq 0$, entonces $\partial f(x) \leq g(x)$.
(7) Si algunos de los polinomios $f(x)$ o $g(x)$ es cero, automáticamente el otro lo es y la igualdad se cumple trivialmente, así que suponemos $g(x) \neq 0 \neq f(x)$ y sean $r(x)$ y $s(x)$ en $K[x]$ tales que $f(x) \cdot r(x) = g(x)$ y $g(x) \cdot s(x) = f(x)$. Entonces de estas dos igualdades obtenemos $g(x) \cdot s(x) \cdot r(x) = g(x)$, por lo que $\partial(r(x) \cdot s(x)) = \partial r(x) + \partial s(x) = 0$ y de aquí se debe tener $s(x)$ y $r(x)$ son polinomios constantes distintos de cero y por lo tanto $f(x) = a \cdot g(x)$, donde $a = s(x)$ es un elemento de K. ∎

Teorema 13.3.4. ***(Algoritmo de la División)***
Sean $f(x)$ y $g(x)$ polinomios en $K[x]$ tales que $g(x) \neq 0$. Entonces existen polinomios $q(x)$ y $r(x)$ en $K[x]$ únicos tales que

$$f(x) = g(x) \cdot q(x) + r(x) \quad \textit{donde } r(x) = 0 \quad \textit{o} \quad \partial r(x) < \partial g(x).$$

Demostración. Si $g(x) \mid f(x)$ entonces $f(x) = q(x) \cdot g(x)$ para alguna $q(x) \in K[x]$ y basta tomar $r(x) = 0$. Supongamos entonces $g(x) \nmid f(x)$. Sea

$$\mathfrak{A} = \{ f(x) - g(x) \cdot s(x) \mid s(x) \in K[x] \}.$$

$0 \notin \mathfrak{A}$ puesto que $g(x) \nmid f(x)$. Para demostrar el teorema mostraremos que podemos encontrar un polinomio $r(x)$ en $K[x]$ con las propiedades requeridas. Sea

$$\mathscr{A} = \{n \in \mathbb{N} \mid n = \partial h(x) \text{ para algún } h(x) \in \mathfrak{A}\}.$$

Como $\mathfrak{A} \neq \varnothing$ ($f(x) \in \mathfrak{A}$) se tiene que $\mathscr{A} \neq \varnothing$. Siendo $\varnothing \neq \mathscr{A} \subseteq \mathbb{N}$, podemos considerar la mínima $n \in \mathbb{N}$ tal que $n \in \mathscr{A}$ (Principio del Buen Orden). Sean $r(x)$ y $q(x)$ tales que $r(x) = f(x) - g(x) \cdot q(x)$ y $\partial r(x) = n$. Entonces $f(x) = g(x) \cdot q(x) + r(x)$. Ahora, supongamos que $\partial r(x) \geq \partial g(x)$ y sean a_n y b_m los coeficientes principales de $r(x)$ y $g(x)$ respectivamente. Si $r_1(x) = r(x) - a_n b_m^{-1} \cdot g(x) \cdot x^{n-m}$, entonces

$$f(x) = g(x)\left(q(x) + a_n b_m^{-1} \cdot x^{n-m}\right) + r_1(x)$$

y por lo tanto $r_1(x) \in \mathfrak{A}$. Pero como estamos en el supuesto de que $0 \notin \mathfrak{A}$, entonces $\partial r_1(x) < \partial r(x)$, lo que resulta una contradicción, por lo que debe ser $\partial r(x) < \partial g(x)$. Nos queda demostrar que $q(x)$ y $r(x)$ son únicos. Supongamos que $q_1(x)$ y $r_1(x)$ también satisfacen $f(x) = g(x) \cdot q_1(x) + r_1(x)$, donde $r_1(x) = 0$ o $\partial r_1(x) < \partial g(x)$. Entonces

$$g(x)\,(q(x) - q_1(x)) = r_1(x) - r(x).$$

Pero suponer $r_1(x) \neq r(x)$ nos lleva a una contradicción, ya que en este caso se tendría $\partial\,(r_1(x) - r(x)) \leq \text{máx}\,\{\partial r_1(x), \partial r(x)\} < \partial g(x)$ y por otro lado,

$$\partial\,(r_1(x) - r(x)) = \partial g(x) + \partial\,(q(x) - q_1(x)) \geq \partial g(x).$$

Por lo tanto debe ser $r(x) = r_1(x)$ y por ser $K[x]$ un dominio entero y $g(x) \neq 0$ se obtiene que $q(x) = q_1(x)$. ∎

El teorema anterior asegura la existencia de $q(x)$ y $r(x)$ con las propiedades requeridas, pero no nos dice cómo obtenerlos. Sin embargo se puede dar un algoritmo para encontrar esta pareja de polinomios como sigue:
Sean $f(x) = a_n x^n + \cdots + a_1 x + a_0$ y $g(x) = b_m x^m + \cdots + b_1 x + b_0$, con $b_m \neq 0$ (recuérdese que $g(x) \neq 0$). Si $f(x) = 0$ o $\partial f(x) < \partial g(x)$, en cualquiera de los dos casos basta tomar $q(x) = 0$ y $r(x) = f(x)$ así que supongamos $f(x) \neq 0$ y $n = \partial f(x) > \partial g(x) = m$. Entonces

$$f(x) = g(x) \cdot b_m^{-1} a_n \cdot x^{n-m} + f(x) - g(x) \cdot b_m^{-1} a_n \cdot x^{n-m},$$

donde

$$f(x) - g(x) \cdot b_m^{-1} a_n \cdot x^{n-m} = \left(a_{n-1} - b_{m-1} b_m^{-1} a_n\right) x^{n-1} + \cdots + \left(a_{n-m} - b_0 b_m^{-1} a_n\right) x^{n-m} + a_{n-m-1} \cdot x^{n-m-1} + \cdots + a_1 x + a_0.$$

Esto es, para $q_1(x) = b_m^{-1}a_n \cdot x^{n-m}$ y $f_1(x) = f(x) - g(x) \cdot b_m^{-1}a_n \cdot x^{n-m}$ se tiene

$$f(x) = g(x) \cdot q_1(x) + f_1(x) \quad \text{donde } \partial f_1(x) < \partial f(x).$$

Si $f_1(x) = 0$ o $\partial f_1(x) < \partial g(x)$ habremos terminado, siendo $q_1(x)$ y $f_1(x)$ los polinomios buscados. En caso contrario, es decir, si $f_1(x) \neq 0$ y $\partial f_1(x) \geq \partial g(x)$, repetimos el proceso anterior con $g(x)$ y $f_1(x)$, que es, si $\partial f_1(x) = r$ y c_r es el coeficiente principal de $f_1(x)$, entonces

$$f_1(x) = g(x) \cdot b_m^{-1}c_r \cdot x^{r-m} + f_1(x) - g(x) \cdot b_m^{-1}c_r \cdot x^{r-m}$$

donde $f_2(x) = f_1(x) - g(x) \cdot b_m^{-1}c_r \cdot x^{r-m}$ es tal que

$$\partial f_2(x) < \partial f_1(x) \, y \; f(x) = g(x)\,(q_1(x) + q_2(x)) + f_2(x).$$

Si $f_2(x) = 0$ o $\partial f_2(x) < \partial g(x)$, entonces $q(x) = q_1(x) + q_2(x)$ y $r(x) = f_2(x)$ satisfarán el teorema 13.3.4. En caso contrario $f_2(x) \neq 0$ y $\partial f_2(x) \geq \partial g(x)$ continuaremos de la misma forma. Así pues, mediante este proceso obtenemos una sucesión de parejas

$$(q_1(x), f_1(x)), \ldots, (q_s(x), f_s(x))$$

tales que, $f_i(x) \neq 0$ para $i = 1, \ldots, s$, $f(x) = g(x)q_1(x) + f_1(x)$ y $f_{i-1}(x) = g(x)q_i(x) + f_i(x)$ para $i = 2, \ldots, s$, con

$$\partial f_s(x) < \cdots < \partial f_1(x) < \partial f(x).$$

Debido a que esta sucesión es decreciente, en algún momento para alguna t, deberá ser $f_t(x) = 0$ o $\partial f_t(x) < \partial g(x)$ y entonces los polinomios buscados serán $q(x) = q_1(x) + \cdots + q_t(x)$ y $r(x) = f_t(x)$.

Ejemplo 13.3.5. Sean $f(x) = 3x^6 + x^4 - x^3 - x^2 + x + 2$ y $g(x) = 2x^2 + 1$. Entonces

$$f(x) = \left(2x^2 + 1\right) \underbrace{\left(\frac{1}{2}3 \cdot x^4\right)}_{q_1(x)} + \underbrace{\left(-\frac{1}{2} \cdot x^4 - x^3 - x^2 + x + 2\right)}_{f_1(x)}$$

Como $f_1(x) \neq 0$ y $\partial f_1(x) \geq \partial g(x)$ continuamos el proceso

$$f_1(x) = \left(2x^2 + 1\right) \underbrace{\left(\frac{1}{2}\left(\frac{-1}{2}\right) \cdot x^2\right)}_{q_2(x)} + \underbrace{\left(-x^3 - \frac{3}{4} \cdot x^2 + x + 2\right)}_{f_2(x)}$$

Nuevamente, como $\partial f_1(x) \geq \partial g(x)$ continuamos

$$f_2(x) = \left(2x^2+1\right)\underbrace{\left(\frac{1}{2}(-1)\cdot x\right)}_{q_3(x)} + \underbrace{\left(-\frac{3}{4}x^2+\frac{3}{2}\cdot x+2\right)}_{f_3(x)}$$

$\partial f_3(x) \geq \partial g(x)$, así que

$$f_3(x) = \left(2x^2+1\right)\underbrace{\left(\frac{1}{2}\left(\frac{-3}{4}\right)\right)}_{q_4(x)} + \underbrace{\left(\frac{3}{2}x+\frac{19}{8}\right)}_{f_4(x)}$$

Puesto que $\partial f_4(x) < \partial g(x)$, hemos terminado y por lo tanto para $q(x) = \frac{3}{2}\cdot x^4 - \frac{1}{4}\cdot x^2 - \frac{1}{2}\cdot x - \frac{3}{8}$, $r(x) = \frac{3}{2}\cdot x + \frac{19}{8}$ y $f(x) = g(x)\cdot q(x) + r(x)$, donde $\partial r(x) < \partial g(x)$.

§ 13.4. Máximo común divisor

En la sección 7.2, definimos el máximo común divisor de dos enteros (no ambos cero) como el máximo del conjunto de divisores comunes, lo que pudimos hacer debido a que este conjunto es finito. Para el caso de polinomios, aparte de no tener definido un orden, el conjunto de divisores comunes de dos polinomios dados es infinito en el caso en que K es un conjunto infinito y quisiéramos, de entre estos, tomar alguno que satisfaga las propiedades (*ii*) y (*iii*) mencionadas en el inciso (3) del teorema 7.2.8. Lo que veremos es que efectivamente existen polinomios en el conjunto de divisores comunes que satisfacen estas propiedades y hablamos en plural ya que, salvo el caso en que el campo es $\mathbb{Z}_2$, habrá más de uno que satisfaga ambas propiedades. En realidad esto sucede también en los enteros si no consideramos la propiedad (*i*) del inciso (3) del teorema 7.2.8 pues si d satisface las propiedades (*ii*) y (*iii*), $-d$ también, así que la unicidad del máximo común divisor será consecuencia de pedir que sea positivo (propiedad (*i*)). Veremos que en el caso de polinomios esto también será posible, que es, de entre todos los polinomios que satisfacen las propiedades (*ii*) y (*iii*) habrá uno y sólo uno que será mónico, por lo que se sustituirá la condición de ser mayor que cero en $\mathbb{Z}$ por la condición de ser mónico en $K[x]$. Muchos de los teoremas sobre el m.c.d. en los enteros se repetirán aquí, incluyendo el Algoritmo de Euclides, con los ajustes convenientes.

Definición 13.4.1. *Sean $f(x)$ y $g(x)$ polinomios no ambos cero en $K[x]$. Un polinomio $d(x)$ en $K[x]$ es el máximo común divisor de $f(x)$ y $g(x)$ si satisface*

(*a*) *$d(x)$ es mónico,*
(*b*) *$d(x) \mid f(x)$ y $d(x) \mid g(x)$,*
(*c*) *Si $h(x) \mid f(x)$ y $h(x) \mid g(x)$, entonces $h(x) \mid d(x)$.*

Antes de demostrar la existencia en $K[x]$ del máximo común divisor para cada pareja de polinomios no ambos cero, veamos que a lo más hay un único polinomio con esta propiedad.

Nota 13.4.2. Si $d(x)$ es un polinomio mónico de grado cero (constante), entonces $d(x) = 1$.

Proposición 13.4.3. *Sean $f(x)$ y $g(x)$ polinomios en $K[x]$, no ambos cero. Si $d_1(x)$ y $d_2(x)$ son polinomios que satisfacen $(a), (b)$ y (c) de la definición 13.4.1, entonces $d_1(x) = d_2(x)$.*

Demostración. Por la condición (c) y como tanto $d_1(x)$ como $d_2(x)$ son divisores comunes de $f(x)$ y $g(x)$, se tiene que $d_1(x) \mid d_2(x)$ y $d_2(x) \mid d_1(x)$, y por (7) del teorema 13.3.3, $d_1(x) = a \cdot d_2(x)$ para alguna $a \in K$. Por ser $d_1(x)$ y $d_2(x)$ ambos mónicos, entonces $a = 1$ y así $d_1(x) = d_2(x)$. ∎

Esta última proposición nos dice entonces que en caso de existir un polinomio $d(x)$ que satisfaga la definición 13.4.1, éste debe ser único. Demostraremos ahora su existencia

Nota 13.4.4. Consideremos dos polinomios $f(x)$ y $g(x)$, no ambos cero. Sea

$$\mathfrak{A} = \{h(x) \mid h(x) = f(x) \cdot a(x) + g(x) \cdot b(x), \text{ con } a(x), b(x) \in K[x] \text{ y } h(x) \neq 0\}$$

y sea m el mínimo de $\mathscr{A} = \{\partial h(x) \mid h(x) \in \mathfrak{A}\}$, cuya existencia está garantizada por el Principio del buen orden ($\varnothing \neq \mathscr{A} \subseteq \mathbb{N}$). Sea $h(x) \in \mathfrak{A}$ tal que $\partial h(x) = m$, entonces $a \cdot h(x) \in \mathfrak{A}$ para toda $a \in K - \{0\}$ y $\partial(a \cdot h(x)) = m$. En particular, si a es el coeficiente principal de $h(x)$, entonces $a^{-1} \cdot h(x) \in \mathfrak{A}$ y es mónico. En el siguiente teorema demostraremos que este polinomio es precisamente el máximo común divisor de $f(x)$ y $g(x)$.

Definición 13.4.5. *Un polinomio $h(x)$ es combinación lineal de $f(x)$ y $g(x)$ si existen polinomios $a(x)$ y $b(x)$ tales que $h(x) = f(x) \cdot a(x) + g(x) \cdot b(x)$*

Teorema 13.4.6. *Sean $f(x)$ y $g(x)$ polinomios en $K[x]$, no ambos cero y sea $d(x)$ un polinomio de grado mínimo en el conjunto de combinaciones lineales distintas de cero de $f(x)$ y $g(x)$, el cual es mónico. Entonces $d(x)$ es el máximo común divisor de $f(x)$ y $g(x)$.*

Demostración. La existencia de $d(x)$ está justificada en la Nota 13.4.4.
Consideremos este polinomio $d(x)$ y sea $d(x) = f(x) \cdot a(x) + g(x) \cdot b(x)$ y $h(x)$ un polinomio tal que $h(x) \mid f(x)$ y $h(x) \mid g(x)$. Por (4) del teorema 13.3.3, $h(x) \mid f(x) \cdot a(x) + g(x) \cdot b(x) = d(x)$ con lo que queda demostrado (c) de la definición de m.c.d., así que sólo falta demostrar que $d(x) \mid f(x)$ y $d(x) \mid g(x)$.

Aplicando el algoritmo de la división a $f(x)$ y $d(x)$ obtenemos $f(x) = d(x) \cdot q(x) + r(x)$ donde $r(x) = 0$ o $\partial r(x) < \partial d(x)$. Veamos que no puede ser $r(x) \neq 0$ y entonces se tendrá que $d(x) \mid f(x)$.

$f(x) = d(x) \cdot q(x) + r(x) = (f(x) \cdot a(x) + g(x) \cdot b(x))\, q(x) + r(x)$ y de aquí obtenemos que $r(x) = f(x)\,(1 - a(x) \cdot q(x)) - g(x) \cdot b(x) \cdot q(x)$ y por lo tanto $r(x)$ es una combinación lineal de $f(x)$ y $g(x)$, luego no puede ser que $r(x) \neq 0$ ya que $\partial r(x) < \partial d(x)$ y $d(x)$ es un polinomio distinto de cero de grado mínimo en el conjunto de combinaciones lineales distintas de cero de $f(x)$ y $g(x)$.

Concluimos entonces que $d(x) \mid f(x)$. Análogamente se muestra que $d(x) \mid g(x)$. Por lo tanto $d(x)$ es el máximo común divisor de $f(x)$ y $g(x)$. ∎

Corolario 13.4.7. *Sean $f(x)$ y $g(x)$ polinomios en $K[x]$, no ambos cero. Entonces existe el máximo común divisor de $f(x)$ y $g(x)$ y es combinación lineal en $K[x]$ de $f(x)$ y $g(x)$.*

Notación 13.4.8. *Denotaremos por $(f(x), g(x))$ al m.c.d. de los polinomios $f(x)$ y $g(x)$ (no ambos cero).*

El siguiente resultado es exactamente igual al correspondiente en $\mathbb{Z}$ y se demuestra de la misma manera (usando el Teorema 13.4.6).

Teorema 13.4.9. *Si $f(x) \mid g(x) \cdot h(x)$ y $(f(x), g(x)) = 1$, entonces $f(x) \mid h(x)$.*

Si $(f(x), g(x)) = 1$ diremos que $f(x)$ y $g(x)$ ***son primos entre sí*** o ***primos relativos***.

Los divisores positivos de un número entero $a \neq 0$ son menores o iguales a él y por lo tanto hay un número finito de ellos, así que para encontrarlos basta ver cuáles de éstos dividen a a.

Sin embargo, en el caso de polinomios no resulta nada sencillos puesto que por cada grado n, existen una infinidad de polinomios de ese grado (cuando el campo es infinito). Entonces ¿cómo encontrar el m.c.d. de dos polinomios?

Algoritmo de Euclides
Dados dos polinomios $f(x)$ y $g(x)$, no ambos cero, se tiene una sucesión de igualdades, cada una de ellas obtenida a partir del algoritmo de la división, como sigue

$$\begin{array}{rcll} f(x) &=& g(x)\cdot q_0(x)+r_0(x) & \partial r_0(x) < \partial g(x) \\ g(x) &=& r_0(x)\cdot q_1(x)+r_1(x) & \partial r_1(x) < \partial r_0(x) \\ r_0(x) &=& r_1(x)\cdot q_2(x)+r_2(x) & \partial r_2(x) < \partial r_1(x) \\ \vdots & & \vdots & \vdots \\ r_{n-3}(x) &=& r_{n-2}(x)\cdot q_{n-1}(x)+r_{n-1}(x) & \partial r_{n-1}(x) < \partial r_{n-2}(x) \\ r_{n-2}(x) &=& r_{n-1}(x)\cdot q_n(x)+0 & r_n(x) = 0 \end{array}$$

Debido a que los grados de los residuos van disminuyendo, es decir,

$$\partial r_0(x) > \partial r_1(x) > \cdots,$$

forzosamente $r_n(x) = 0$ para algún n. Entonces $a^{-1}\cdot r_{n-1}(x)$ será el m.c.d. de $f(x)$ y $g(x)$, donde a es el coeficiente principal de $r_{n-1}(x)$. La demostración de este hecho es completamente similar a la dada en los enteros, motivo por el cual lo dejamos como ejercicio. Si $r_0 = 0$, el m.c.d. de $f(x)$ y $g(x)$ será $f(x)$ si $g(x) = 0$ o $b^{-1}g(x)$ si $g(x) \neq 0$, donde b es el coeficiente principal de $g(x)$.

Ejemplo 13.4.10. Consideremos $f(x) = 2x^6 + 4x^5 - 10x^4 - 13x^3 - 2x^2 + 5x + 6$ y $g(x) = x^4 + x^3 - 5x^2 + x - 6$.
$f(x) = g(x)(2x^+2x - 2) + (-3x^3 - 2x^2 + 19x - 6)$
$g(x) = (-3x^3 - 2x^2 + 19x - 6)(-\frac{1}{3}x - \frac{1}{9}) + (\frac{10}{9}x^2 + \frac{10}{9}x - \frac{20}{3})$
$-3x^3 - 2x^2 + 19x - 6 = (\frac{10}{9}x^2 + \frac{10}{9}x - \frac{10}{3})(-\frac{27}{10}x + \frac{9}{10}) + 0$
El último residuo distinto de cero es $\frac{10}{9}x^2 + \frac{10}{9}x - \frac{10}{3}$ y por lo tanto del m.c.d. de $f(x)$ y $g(x)$ es $(f(x), g(x)) = \frac{9}{10}\left(\frac{10}{9}x^2 + \frac{10}{9}x - \frac{10}{3}\right) = x^2 + x - 6$.

§ 13.5. Polinomios irreducibles y factorización única en $K[x]$

Siguiendo con la analogía entre el anillo de polinomios sobre un campo y el anillo de los enteros, definimos polinomio irreducible de manera semejante a la de número primo en los enteros. Los polinomios irreducibles en $K[x]$ jugarán un papel completamente similar al de los primos en $\mathbb{Z}$, como se verá en el desarrollo de este tema, culminando con el teorema de factorización única que dice que todo polinomio de grado positivo es producto, de un elemento invertible y polinomios irreducibles y esta descomposición es única salvo el orden de los factores
Es importante mencionar, que en general en un anillo, irreducible y primo son conceptos distintos. Sin embargo para ciertos anillos estos conceptos coinciden.

Tales anillos son conocidos como dominios de factorización única, de los cuales ejemplos importantes de estos son precisamente $\mathbb{Z}$ y $K[x]$. Un elemento a de un anillo se llama ***primo*** si cada vez que a divide a un producto, entonces divide a uno de los factores y a se llama ***irreducible*** si $a = b \cdot c$ implica que alguno de los dos b o c es invertible.

Definición 13.5.1. *Un polinomio $p(x)$ en $K[x]$ se llama* **irreducible** *si es de grado positivo y si no puede expresarse como el producto de dos polinomios, ambos de grado menor al de $p(x)$. En caso contrario se llamará* **reducible**.

Es importante mencionar que el hecho de que un polinomio sea irreducible en $K[x]$ depende directamente de K como se puede ver en el siguiente

Ejemplo 13.5.2. El polinomio $p(x) = x^2 - 3$ es irreducible en $\mathbb{Q}[x]$ pero es reducible en $\mathbb{R}[x]$ ya que $x^2 - 3 = \left(x + \sqrt{3}\right)\left(x - \sqrt{3}\right)$. Esto es porque $x + \sqrt{3}$ y $x - \sqrt{3}$ pertenecen a $\mathbb{R}[x]$ pero no a $\mathbb{Q}[x]$. De la misma manera, x^2+1 es irreducible en $\mathbb{R}[x]$ pero no en $\mathbb{C}[x]$ puesto que $x^2 + 1 = (x + i)(x - i)$ en $\mathbb{C}[x]$.

Dado un polinomio $p(x) \neq 0$ y $f(x)$ un divisor de él, sabemos por el teorema 13.3.3 (6) que $\partial f(x) \leq \partial p(x)$. En el caso particular en que $p(x)$ es irreducible sabemos además que no puede ser que $0 < \partial f(x) < \partial p(x)$, así que la única posibilidad, en este caso, para $f(x)$ es que $\partial f(x) = 0$ o $\partial f(x) = \partial p(x)$ con lo que no es difícil saber quiénes son sus divisores.

Lema 13.5.3. *Sea $p(x)$ un polinomio de grado positivo en $K[x]$. Entonces $p(x)$ es irreducible en $K[x]$ si y sólo si sus únicos divisores son los elementos distintos de cero de K y los polinomios de la forma $a \cdot p(x)$ para cada $a \in K - \{0\}$.*

La demostración de este lema es bastante sencilla, así que la dejamos como ejercicio (véase ejercicio 13.5.1).
Veamos ahora algunas propiedades de polinomios irreducibles.

Proposición 13.5.4. *Sea $p(x)$ un polinomio irreducible en $K[x]$. Para cada polinomio*
$0 \neq f(x) \in K[x]$, $(p(x), f(x)) = 1$ o $(p(x), f(x)) = a^{-1} \cdot p(x)$, donde a es el coeficiente principal de $p(x)$. Es más, $(p(x), f(x)) = a^{-1} \cdot p(x)$ si y sólo si $p(x) \mid f(x)$.

Demostración. Sea $d(x) = (p(x), f(x))$. Entonces $d(x) \mid p(x)$ y por el lema 13.5.3, $d(x)$ es una constante distinta de cero (elemento del campo) o $d(x) = b \cdot p(x)$ para algún $0 \neq b \in K$. Ahora, por la definición de m.c.d. (éste

debe ser mónico), en el primer caso debe ser $d(x) = 1$ y en el segundo debe ser $b = a^{-1}p(x)$ donde a es el coeficiente principal de $p(x)$. La segunda afirmación del teorema es inmediata. ■

La siguiente proposición es completamente similar al resultado análogo para primos en $\mathbb{Z}$, y como se verá, su demostración es completamente similar a la de los enteros.

Proposición 13.5.5. *Si $p(x)$ un polinomio irreducible en $K[x]$ y $p(x) \mid f(x) \cdot g(x)$, entonces $p(x) \mid f(x)$ o $p(x) \mid g(x)$.*

Demostración. Supongamos que $p(x) \mid f(x) \cdot g(x)$ y supongamos que $p(x) \nmid f(x)$. Demostraremos que $p(x) \mid g(x)$. Como $p(x) \nmid f(x)$, por la proposición 13.5.4, $(p(x), f(x)) = 1$ y por lo tanto, por el teorema 13.4.9, $p(x) \mid g(x)$. ■

Corolario 13.5.6. *Si $p(x)$ es un polinomio irreducible y $p(x) \mid f_1(x) \cdot \ldots \cdot f_r(x)$, entonces $p(x) \mid f_i(x)$ para alguna $i = 1, \ldots, r$.*

Demostración. Se puede demostrar por inducción sobre r y lo dejamos como ejercicio (véase ejercicio 13.5.3). ■

Continuando con la analogía entre el anillo de polinomios y el anillo de los enteros, como anunciamos al principio de esta sección, terminaremos esta sección presentando el resultado análogo al teorema 7.4.6, en el cual número primo será sustituido por polinomio irreducible.

Teorema 13.5.7. *Cada polinomio de grado positivo en $K[x]$ se expresa como producto de un elemento invertible (elemento distinto de cero del campo) y polinomios irreducibles mónicos. La descomposición es única salvo por el orden de los factores.*

Demostración. Factorización: Por inducción sobre $\partial f(x) = n$

$1°/$ $n = 1$. $f(x) = ax + b$ con $a \neq 0$. Entonces la descomposición es

$$f(x) = a\left(x + a^{-1}b\right).$$(véase ejercicio 13.5.6)

$2°/$ Supongamos cierto el resultado para todo polinomio de grado k con $0 < k < n$ y sea $f(x)$ un polinomio tal que $\partial f(x) = n$.

Si $f(x)$ es irreducible y $f(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \cdots + a_1 \cdot x + a_0$ con $a_n \neq 0$, entonces $f(x) = a_n \left(x^n + a_n^{-1}a_{n-1} \cdot x^{n-1} + \cdots + a_n^{-1}a_1 \cdot x + a_n^{-1}a_0\right)$ es la descomposición deseada.
Si $f(x)$ no es irreducible, entonces existen polinomios $g(x)$ y $h(x)$ tales que $f(x) = g(x) \cdot h(x)$ y $0 < \partial g(x) < n$ y $0 < \partial h(x) < n$. Por hipótesis de inducción se tiene que $g(x) = a \cdot p_1(x) \cdot \ldots \cdot p_r(x)$ y $h(x) = b \cdot q_1(x) \cdot \ldots \cdot q_s(x)$ con $a, b \in K - \{0\}$ y cada $p_i(x)$ y $q_j(x)$ irreducibles mónicos para $i = 1, \ldots, r$ y $j = 1, \ldots, s$.
Por lo tanto $g(x) = ab \cdot p_1(x) \cdot \ldots \cdot p_r(x) \cdot q_1(x) \cdot \ldots \cdot q_s(x)$, siendo esta la descomposición requerida.

Unicidad: Por inducción sobre el número de factores mónicos irreducibles que ocurren en una descomposición del polinomio $f(x)$.

$1°/$ $n = 1$. Supongamos $f(x) = a \cdot g(x) = b \cdot h_1(x) \cdot \ldots \cdot h_r(x)$ donde $a, b \in K - \{0\}$ y $g(x)$ y $h_i(x)$ son irreducibles mónicos para $i = 1, \ldots, r$. Entonces $a = b$ y

$$g(x) = h_1(x) \cdot \ldots \cdot h_r(x).$$

Como $\partial h_i(x) > 0$ y $g(x)$ es irreducible, entonces debe ser $r = 1$.
$2°/$ Supongamos cierto el resultado para $n-1$ y sea $f(x) = a \cdot g_1(x) \cdot \ldots \cdot g_n(x)$ donde $a \in K - \{0\}$ y $g_1(x), \ldots, g_n(x)$ son mónicos irreducibles. Supongamos que existen $h_1(x) \cdot \ldots \cdot h_r(x)$ polinomios mónicos irreducibles y $b \in K$ tales que

$$f(x) = a \cdot g_1(x) \cdot \ldots \cdot g_n(x) = b \cdot h_1(x) \cdot \ldots \cdot h_r(x).$$

Como tanto los $g_i(x)$ y los $h_j(x)$ son mónicos, se tiene $a = b$ y por otro lado ya que $g_1(x) \mid h_1(x) \cdot \ldots \cdot h_r(x)$, por el ejercicio 13.4.11, debe ser $g_1(x) = h_i(x)$ para alguna i. No se pierde generalidad si suponemos $i = 1$. Entonces

$$g_2(x) \cdot \ldots \cdot g_n(x) = h_2(x) \cdot \ldots \cdot h_r(x)$$

y por lo tanto por hipótesis de inducción debe ser $n - 1 = r - 1$ y para alguna permutación σ de $\{2, \ldots, n\}$ se tiene que $g_i(x) = h_{\sigma(i)}(x)$ para toda $i = 2, \ldots, n$. ∎

Proposición 13.5.8. *Sean $c_1, c_2 \in K$ con $c_1 \neq c_2$. Entonces*

$$((x - c_1)^m, (x - c_2)^n) = 1$$

para cualesquiera enteros positivos m y n.

Demostración. Tanto $x - c_1$ como $x - c_2$ son polinomios irreducibles. Sea

$$d(x) = \left((x - c_1)^m, (x - c_2)^n\right)$$

y supongamos que $\partial d(x) > 0$ y sea $p(x)$ un polinomio irreducible mónico tal que $p(x) \mid d(x)$. Entonces $p(x) \mid (x - c_1)^m$ y $p(x) \mid (x - c_2)^n$. Como $p(x)$ es irreducible, por el corolario 13.5.6, $p(x) \mid x - c_1$ y por ser ambos irreducibles y mónicos, se debe tener $p(x) = x - c_1$. Entonces $x - c_1 \mid (x - c_2)^n$ y por las mismas razones que antes debe ser $x - c_1 = x - c_2$ lo que es imposible ya que $c_1 \neq c_2$. Por lo tanto $\partial d(x) = 0$ y así $((x - c_1)^m, (x - c_2)^n) = 1$. ∎

§ 13.6. Derivada de un polinomio

La definición que daremos aquí de la derivada de un polinomio coincide con la derivada de un polinomio en cálculo cuando $K = \mathbb{R}$. Sin embargo como estamos trabajando con un campo arbitrario K, introducimos este concepto desde un punto de vista completamente algebraico.

Definición 13.6.1. *Dado un polinomio*

$$f(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \cdots + a_1 \cdot x + a_0 \in K[x],$$

su derivada, denotada por $\boldsymbol{f'(x)}$*, es el polinomio*

$$f'(x) = na_n \cdot x^{n-1} + (n-1)a_{n-1} \cdot x^{n-2} + \cdots + a_1.$$

Teorema 13.6.2. *Sean* $f(x)$ *y* $g(x)$ *polinomios en* $K[x]$ *y* $n \in \mathbb{N}$. *Si*

$$h(x) = f(x) + g(x),\ t(x) = f(x) \cdot g(x) \text{ y } s(x) = f(x)^n,$$

entonces

$$h'(x) = f'(x) + g'(x),\ t'(x) = f'(x) \cdot g(x) + f(x) \cdot g'(x) \text{ y } s'(x) = n \cdot f(x)^{n-1} \cdot f'(x).$$

Demostración. Sean

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

y

$$g(x) = b_m \cdot x^m + b_{m-1} \cdot x^{m-1} + \cdots + b_1 \cdot x + b_0.$$

(1) Supongamos $m \leq n$ (el caso $n \leq m$ es totalmente análogo). Entonces

$$h(x) = a_n \cdot x^n + \cdots + a_{m+1} \cdot x^{m+1} + (a_m + b_m) \cdot x^m + \cdots + (a_1 + b_1) \cdot x + (a_0 + b_0)$$

y por la definición de la derivada tenemos que

$$h'(x) =$$
$$n \cdot a_n \cdot x^{n-1} + \cdots + (m+1) \cdot a_{m+1} \cdot x^m + m \cdot (a_m + b_m) \cdot x^{m-1} + \cdots + a_1 + b_1 =$$
$$(n \cdot a_n \cdot x^{n-1} + (n-1) \cdot a_{n-1} \cdot x^{n-2} + \cdots + a_1) + (m \cdot b_m \cdot x^{m-1} + (m-1) \cdot b_{m-1} \cdot x^{m-2} + \cdots + b_1) =$$
$$f'(x) + g'(x)\,.$$

(2) Por hipótesis

$$t(x) = f(x) \cdot g(x) =$$
$$f(x) \cdot b_m \cdot x^m + f(x) \cdot b_{m-1} \cdot x^{m-1} + \cdots + f(x) \cdot b_1 \cdot x + f(x) \cdot b_0.$$

Ahora, por el inciso (1) tenemos que

$$t'(x) = (f(x) \cdot b_m \cdot x^m)' + (f(x) \cdot b_{m-1} \cdot x^{m-1})' + \cdots + (f(x) \cdot b_1 \cdot x)' + (f(x) \cdot b_0)'.$$

Veamos ahora cómo es la derivada de $f(x) \cdot b_j \cdot x^j$:

$$(f(x) \cdot b_j \cdot x^j)' =$$
$$\left(b_j a_n \cdot x^{n+j} + b_j a_{n-1} \cdot x^{n-1+j} + \cdots + b_j a_1 \cdot x^{1+j} + b_j a_0 \cdot x^j\right)' =$$
$$(n+j) b_j a_n \cdot x^{n+j-1} + (n-1+j) b_j a_{n-1} \cdot x^{n-1+j-1} + \cdots + (1+j) b_j a_1 \cdot x^{1+j-1} + j b_j a_0 \cdot x^{j-1} =$$
$$n b_j a_n \cdot x^{n+j-1} + j b_j a_n \cdot x^{n+j-1} + (n-1) b_j a_{n-1} \cdot x^{n-1+j-1} + j b_j a_{n-1} \cdot x^{n-1+j-1} +$$
$$\cdots + b_j a_1 \cdot x^{1+j-1} + j b_j a_1 \cdot x^{1+j-1} + j b_j a_0 \cdot x^{j-1} =$$
$$(n b_j a_n \cdot x^{n+j-1} + (n-1) b_j a_{n-1} \cdot x^{n+j-2} + \cdots + b_j a_1 \cdot x^j) +$$
$$(j b_j a_n \cdot x^{n+j-1} + j b_j a_{n-1} \cdot x^{n-1+j-1} + \cdots + j b_j a_1 \cdot x^{1+j-1} + j b_j a_0 \cdot x^{j-1}) =$$
$$(n a_n \cdot x^{n-1} + (n-1) a_{n-1} \cdot x^{n-2} + \cdots + a_1) \cdot b_j \cdot x^j +$$
$$(a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \cdots + a_1 \cdot x + a_0)(j b_j \cdot x^{j-1}) =$$
$$f'(x) \cdot b_j \cdot x^j + f(x) \cdot (b_j \cdot x^j)'.$$

Finalmente tenemos

$$t'(x) =$$
$$f'(x) \cdot b_m \cdot x^m + f(x) \cdot (b_m \cdot x^m)' + f'(x) \cdot b_{m-1} \cdot x^{m-1} + f(x) \cdot (b_{m-1} \cdot x^{m-1})' +$$
$$\cdots + f'(x) \cdot b_1 \cdot x + f(x) \cdot (b_1 \cdot x)' + f'(x) \cdot b_0 + f(x) \cdot (b_0') =$$
$$f'(x) \cdot (b_m \cdot x^m + b_m \cdot x^{m-1} + \cdots + b_1 \cdot x + b_0) + f(x) \cdot (m b_m \cdot x^{m-1} + (m-1) b_{m-1} \cdot x^{m-1} + \cdots + b_1) =$$
$$f'(x) \cdot g(x) + f(x) + g'(x).$$

(3) Para $s(x) = f(x)^n$, demostraremos por inducción sobre el exponente n que $s'(x) = n \cdot f(x)^{n-1} \cdot f'(x)$.
$1^\circ/$ $n = 1$, $s(x) = f(x)$ y $s'(x) = f'(x)$ y $1 \cdot (f(x)^{1-1}) \cdot f'(x) = f'(x)$.
$2^\circ/$ Suponemos cierta la afirmación para n y sea $s(x) = f^{n+1}$. Entonces por el inciso (2), considerando $s(x) = f(x)^n \cdot f(x)$, tenemos que

$$\begin{aligned} s'(x) &= (f(x)^n)' \cdot f(x) + f(x)^n \cdot f'(x) \\ &= n \cdot f(x)^{n-1} \cdot f'(x) \cdot f(x) + f(x)^n \cdot f'(x) \quad \text{(hipótesis de inducción)} \\ &= n \cdot f(x)^n \cdot f'(x) + f(x)^n \cdot f'(x) \\ &= (n+1) \cdot f(x)^n \cdot f'(x). \end{aligned}$$

∎

§ 13.7. Las raíces de un polinomio

En esta sección estudiaremos las raíces (definición 13.7.1) de un polinomio. Veremos el hecho de que un polinomio tenga una raíz no sólo depende del polinomio mismo sino también del campo en el cual están considerados los coeficientes, lo que significa que un polinomio cuyos coeficientes pueden considerarse en dos campos distintos, el conjunto de raíces del polinomio en uno de esos campos puede ser distinto al conjunto de raíces del polinomio en el otro campo.
Dado un polinomio $f(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \cdots + a_1 \cdot x + a_0 \in K[x]$, éste determina una función $f : K \longrightarrow K$ cuya regla de correspondencia es, para $\alpha \in K$,

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

Esto es, para encontrar $f(\alpha)$ sólo debemos sustituir x por α en el polinomio $f(x)$. Se puede dar el caso en que para $\alpha \neq \beta$ en K, $f(\alpha) = f(\beta)$. En particular estaremos interesados en el conjunto de elementos de K tales que $f(\alpha) = 0$ y veremos que este conjunto tiene a lo más tantos elementos como el grado del polinomio, lo que significa que el número de elementos de K con esta propiedad está acotado por el grado del polinomio sin importar quién es el campo K.

Definición 13.7.1. *Sea $f(x) \in K[x]$ y $\alpha \in K$. α es una raíz de $f(x)$ si $f(\alpha) = 0$.*

Ejemplo 13.7.2. Sea $f(x) = x^5 + x^4 - x^3 - x^2 - 2x - 2$.
(1) Considerando $f(x) \in \mathbb{Q}[x]$, $f(x)$ tiene sólo una raíz en $\mathbb{Q}$ que es $\alpha = -1$.
(2) Considerando $f(x) \in \mathbb{R}[x]$, $f(x)$ tiene tres raíces en $\mathbb{R}$ que son $\alpha_1 = -1$, $\alpha_2 = \sqrt{2}$ y $\alpha_3 = -\sqrt{2}$.
(3) Considerando $f(x) \in \mathbb{C}[x]$, $f(x)$ tiene cinco raíces en $\mathbb{C}$ que son $\alpha_1 = -1$, $\alpha_2 = \sqrt{2}$, $\alpha_3 = -\sqrt{2}$, $\alpha_4 = i$ y $\alpha_5 = -i$.

Debido a que no existe un método general para encontrar las raíces de un polinomio de grado $n \geq 5$, hay algunos resultados que nos proporcionan información importante acerca de las raíces de un polinomio que nos puede ayudar, en algunos casos, a encontrarlas.

Teorema 13.7.3. *Sea $f(x) \in K[x]$ y $\alpha \in K$. Entonces*

$$f(x) = q(x) \cdot (x - \alpha) + f(\alpha),$$

para algún polinomio $q(x) \in K[x]$.

Demostración. Aplicando el algoritmo de la división a los polinomios $f(x)$ y $(x-\alpha)$ obtenemos $f(x) = q(x)\cdot(x-\alpha)+r(x)$, donde $r(x) = 0$ o $\partial r(x) < \partial(x-\alpha) = 1$ y por lo tanto $r(x)$ es un elemento r de K. Evaluando $f(x)$ en α tenemos que $f(\alpha) = q(\alpha) \cdot (\alpha - \alpha) + r(\alpha) = r(\alpha)$, es decir, $f(x) = q(x)(x - \alpha) + f(\alpha)$. ∎

Corolario 13.7.4. *Un elemento α de K es una raíz de un polinomio $f(x) \in K[x]$ si y sólo si $(x - \alpha) \mid f(x)$.*

Demostración. Es inmediato del teorema 13.7.3 ya que como $f(x) = q(x)(x - \alpha) + f(\alpha)$ para algún polinomio $q(x) \in K[x]$, entonces $(x - \alpha) \mid f(x)$ si y sólo si $f(\alpha) = 0$. ∎

Nota 13.7.5. Sea $f(x) = g(x) \cdot h(x)$ en $K[x]$ y $\alpha \in K$. α es raíz de $f(x)$ si y sólo si α es raíz de $g(x)$ o α es raíz de $h(x)$ (véase ejercicio 13.7.1)

Ejemplo 13.7.6. Sea $f(x)$ el polinomio del ejemplo 13.7.2. Entonces

(1) En $K = \mathbb{Q}$, $\alpha = -1$ es una raíz de $f(x)$, así que $f(x) = q(x)(x + 1)$. Para encontrar $q(x)$ sólo debemos dividir $f(x)$ entre $(x + 1)$ con lo que resulta $q(x) = x^4 - x^2 - 2$ y así $f(x) = \left(x^4 - x^2 - 2\right)(x + 1)$.

(2) En $K = \mathbb{R}$, $f(x) = \left(x^4 - x^2 - 2\right)(x + 1)$. Ahora, es evidente que cada raíz de $x^4 - x^2 - 2$ es también raíz de $f(x)$. $\sqrt{2}$ es una raíz de $x^4 - x^2 - 2$ y entonces dividiendo $x^4 - x^2 - 2$ entre $\left(x - \sqrt{2}\right)$ obtenemos

$$x^4 - x^2 - 2 = \left(x^3 + \sqrt{2}x^2 + x + \sqrt{2}\right)\left(x - \sqrt{2}\right)$$

y de aquí $f(x) = \left(x^3 + \sqrt{2}x^2 + x + \sqrt{2}\right)\left(x - \sqrt{2}\right)(x + 1)$. Nuevamente $-\sqrt{2}$ es raíz de $x^3 + \sqrt{2}x^2 + x + \sqrt{2}$ y $x^3 + \sqrt{2}x^2 + x + \sqrt{2} = \left(x^2 + 1\right)\left(x + \sqrt{2}\right)$. Finalmente $f(x) = \left(x^2 + 1\right)\left(x + \sqrt{2}\right)\left(x - \sqrt{2}\right)(x + 1)$.

Entonces $\sqrt{2}$, $-\sqrt{2}$ y -1 son las raíces en $\mathbb{R}$ de $f(x)$.
(3) En $K = \mathbb{C}$, $f(x) = \left(x^2+1\right)\left(x+\sqrt{2}\right)\left(x-\sqrt{2}\right)(x+1)$. Como i es raíz de x^2+1 en $\mathbb{C}$, entonces $x^2+1 = (x-i)(x+i)$ y así

$$f(x) = (x-i)(x+i)\left(x+\sqrt{2}\right)\left(x-\sqrt{2}\right)(x+1) \text{ en } \mathbb{C}[x].$$

Por lo tanto i, $-i$, $\sqrt{2}$, $-\sqrt{2}$ y -1 son raíces en $\mathbb{C}$ de $f(x)$.

Nota 13.7.7. Si $(x-\alpha)^r | f(x)$ y $f(x) \neq 0$, por el Teorema 13.2.8 entonces $r \leq \partial f(x)$. Luego existe una máxima m tal que $(x-\alpha)^m | f(x)$.

Como comentamos al principio de esta sección, un polinomio en $K[x]$ no puede tener más raíces distintas que su grado, sin importar quién es el campo K. Esta afirmación es consecuencia del siguiente

Teorema 13.7.8. *Sea $f(x)$ un polinomio en $K[x]$ distinto de cero y de grado n y sean $\alpha_1, \ldots, \alpha_k$ todas las raíces distintas en K de $f(x)$. Entonces*

$$f(x) = (x-\alpha_1)^{m_1} \cdot \ldots \cdot (x-\alpha_k)^{m_k} \cdot g(x),$$

donde $m_1, \ldots, m_k$ son enteros positivos y $g(x)$ es un polinomio distinto de cero que no tiene raíces en K.

Demostración. Si α_i es una raíz de $f(x)$ en K, entonces $(x-\alpha_i) | f(x)$. Sea m_i el máximo entero positivo tal que $(x-\alpha_i)^{m_i} | f(x)$ para cada $i \in \{1, \ldots, k \ldots\}$.
Por inducción sobre k,
$1°/$ $k = 1$. $f(x) = (x-\alpha_1)^{m_1} \cdot g(x)$,

Si $g(x)$ tuviera una raíz α se tendría que $(x-\alpha_1)^{m_1+1} | f(x)$ en el caso en el que $\alpha = \alpha_1$, contradiciendo la maximalidad de m y si $\alpha \neq \alpha_1$, $f(x)$ tendría más de una raíz, que contradice la hipótesis. Luego $g(x)$ no tiene raíces en K.
$2°/$ Supongamos cierto para $k \geq 1$, y sean $\alpha_1, \ldots, \alpha_{k+1}$ las raíces distintas de $f(x)$. Entonces $f(x) = (x-\alpha_1)^{m_1} \cdot h(x)$. Como $\alpha_2, \ldots, \alpha_{k+1}$ son raíces de $h(x)$ (no pueden serlo de $(x-\alpha_1)^{m_1}$) y éstas son todas, por hipótesis de inducción, $h(x) = (x-\alpha_2)^{m_2} \cdot (x-\alpha_{k+1})^{m_{k+1}} \cdot g(x)$, donde $g(x)$ no tiene raíces. Luego $f(x) = (x-\alpha_1)^{m_1} \cdots (x-\alpha_{k+1})^{m_{k+1}} \cdot g(x)$. ∎

Corolario 13.7.9. *Sea $f(x)$ un polinomio en $K[x]$ distinto de cero y de grado n. Si $\alpha_1, \ldots, \alpha_k$ son todas las raíces de $f(x)$ en K, entonces $k \leq n$.*

Demostración. Por el teorema 13.7.8, $f(x) = a \cdot (x-\alpha_1)^{m_1} \cdot \ldots \cdot (x-\alpha_k)^{m_k} \cdot g(x)$, donde $m_1, \ldots, m_k$ son enteros positivos y $g(x)$ es un polinomio distinto de cero.

Entonces, por (3) del teorema 13.2.8, $n = m_1 + \cdots + m_k + \partial g(x)$ y como $m_i \geq 1$ para toda $i = 1, \ldots, k$, evidentemente debe ser $k \leq n$. ∎

Corolario 13.7.10. *Sea $f(x)$ un polinomio en $K[x]$ de grado $n > 0$. Si $\alpha_1, \ldots, \alpha_n$ son raíces distintas de $f(x)$ en K, entonces $f(x) = a \cdot (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n)$.*

Demostración. Se obtiene inmediatamente del corolario 13.7.9, donde $k = n$ y entonces forzosamente $m_1 = \cdots = m_n = 1$ y $g(x) = a$. ∎

Definimos ahora la multiplicidad de una raíz de un polinomio.

Definición 13.7.11. *Sea α una raíz de $f(x)$ y $m \in \mathbb{N}$. α es una raíz de multiplicidad m de $f(x)$ si $(x - \alpha)^m \mid f(x)$ y $(x - \alpha)^{m+1} \nmid f(x)$.*

Esto es, la multiplicidad de una raíz α de $f(x)$ es el máximo entero positivo m tal que $f(x) = (x - \alpha)^m \cdot g(x)$ para algún polinomio $g(x) \in K[x]$.

Lema 13.7.12. *Sea $\alpha \in K$ una raíz de $f(x) \in K[x]$. La multiplicidad de α es m si y sólo si $f(x) = (x - \alpha)^m \cdot g(x)$ para algún polinomio $g(x) \in K[x]$, con $g(\alpha) \neq 0$.*

Demostración.

$\Longrightarrow$) Supongamos que α es una raíz de multiplicidad m, es decir, $(x - \alpha)^m \mid f(x)$ y $(x - \alpha)^{m+1} \nmid f(x)$. Entonces $f(x) = (x - \alpha)^m \cdot g(x)$ para algún $g(x) \in K[x]$ y supongamos que $g(\alpha) = 0$. Esto es $g(x) = (x - \alpha) \cdot h(x)$ para algún $h(x) \in K[x]$. Sustituyendo en $f(x)$ obtenemos $f(x) = (x - \alpha)^{m+1} \cdot h(x)$, lo que implica $(x - \alpha)^{m+1} \mid f(x)$ que contradice la hipótesis. Por lo tanto $g(\alpha) \neq 0$.

$\Longleftarrow$) Supongamos que $f(x) = (x - \alpha)^m \cdot g(x)$ donde $g(\alpha) \neq 0$. Entonces $(x - \alpha)^m \mid f(x)$. Supongamos ahora que $(x - \alpha)^{m+1} \mid f(x)$, es decir, $f(x) = (x - \alpha)^{m+1} \cdot h(x)$. Por lo tanto $(x - \alpha)^{m+1} \cdot h(x) = (x - \alpha)^m \cdot g(x)$ y esto implica que $(x - \alpha) \cdot h(x) = g(x)$ y de aquí se tiene que $g(\alpha) = 0$, que contradice la hipótesis. Concluimos entonces que $(x - \alpha)^m \mid f(x)$ y $(x - \alpha)^{m+1} \nmid f(x)$, lo que significa que α es raíz de multiplicidad de m de $f(x)$. ∎

Podemos usar el lema 13.7.12 para encontrar la multiplicidad de una raíz, aunque puede resultar un poco largo: Sea α una raíz de $f(x)$. Realizando la división de $f(x)$ entre $x - \alpha$ obtenemos $f(x) = (x - \alpha) \cdot f_1(x)$. Si $f_1(\alpha) \neq 0$, por el lema 13.7.12, la multiplicidad de α será 1. Si $f_1(\alpha) = 0$, dividiendo $f_1(x)$ entre $x - \alpha$ llegamos a que $f_1(x) = (x - \alpha) \cdot f_2(x)$ y así $f(x) = (x - \alpha)^2 \cdot f_2(x)$. Analizando ahora $f_2(x)$, si $f_2(\alpha) \neq 0$ la multiplicidad de α será 2 y si $f_2(\alpha) = 0$ nuevamente dividimos $f_2(x)$ por $x - \alpha$ y así llegamos a que $f(x) = (x - \alpha)^3 \cdot f_3(x)$. Continuando

con este proceso y teniendo en cuenta que $\partial f_1(x) > \partial f_2(x) > \cdots$ en algún momento se tendrá $f(x) = (x-\alpha)^m \cdot f_m(x)$ donde $f_m(\alpha) \neq 0$ y entonces la multiplicidad de α será m.

Existe otra manera de encontrar la multiplicidad de una raíz a través de la derivada del polinomio, pero antes de dar este resultado, definiremos por recursión para cada $i \in \mathbb{N}$, la i-ésima derivada, denotada $f^{(i)}(x)$, de un polinomio $f(x)$ como sigue:

(1) $f^{(0)}(x) = f(x)$
(2) $f^{(i)}(x) = \left(f^{(i-1)}(x)\right)'$ para $i > 0$

Necesitamos el siguiente lema

Lema 13.7.13. *Sea α una raíz de multiplicidad $m \geq 1$ de $f(x) \in K[x]$. Entonces α es un raíz de multiplicidad $m-1$ de $f'(x)$. En particular si $m = 1$, $f'(\alpha) \neq 0$.*

Demostración. Si α es una raíz de multiplicidad $m \geq 1$ de $f(x)$, entonces $f(x) = (x-\alpha)^m \cdot g(x)$ donde $g(\alpha) \neq 0$. Usando el teorema 13.6.2, tenemos que

$$f'(x) = m \cdot (x-\alpha)^{m-1} \cdot g(x) + (x-\alpha)^m \cdot g'(x) = (x-\alpha)^{m-1} \cdot \left(m \cdot g(x) + (x-\alpha) \cdot g'(x)\right).$$

Si $h(x) = m \cdot g(x) + (x-\alpha) \cdot g'(x)$, se tiene $f'(x) = (x-\alpha)^{m-1} \cdot h(x)$ y además $h(\alpha) = m \cdot g(\alpha) \neq 0$ y por el lema 13.7.12, α es raíz de multiplicidad $m-1$ de $f'(x)$. Si $m = 1$, $f'(x) = h(x)$ y entonces $f'(\alpha) = h(\alpha) \neq 0$. ∎

Teorema 13.7.14. *Sea $\alpha \in K$ una raíz de $f(x) \in K[x]$. α es raíz de multiplicidad m de $f(x)$ si y sólo si*

(1) $f^{(0)}(\alpha) = f^{(1)}(\alpha) = \cdots = f^{(m-1)}(\alpha) = 0$ *y*
(2) $f^{(m)}(\alpha) \neq 0$.

Demostración.

$\Longrightarrow$) Usando iteradamente el lema 13.7.13, tenemos α raíz de multiplicidad m de $f(x)$ implica α raíz de multiplicidad $m-1$ de $f^{(1)}(x)$, que a su vez implica α raíz de multiplicidad $m-2$ de $f^{(2)}(x)$, etc. hasta llegar a que α es raíz de multiplicidad $m-(m-1) = 1$ de $f^{(m-1)}(x)$ y $f^{(m)}(\alpha) \neq 0$. Resumiendo: $f^{(0)}(\alpha) = 0$, $f^{(1)}(\alpha) = 0, \ldots, f^{(m-1)}(\alpha) = 0$ y $f^{(m)}(\alpha) \neq 0$.

$\Longleftarrow$) Supongamos $f^{(0)}(\alpha) = f^{(1)}(\alpha) = \cdots = f^{(m-1)}(\alpha) = 0$ y $f^{(m)}(\alpha) \neq 0$ y sea k la multiplicidad de α. Por la parte ($\Longrightarrow$),

$$f^{(0)}(\alpha) = 0,\ f^{(1)}(\alpha) = 0,\ \ldots,\ f^{(k-1)}(\alpha) = 0 \ \ y \ \ f^{(k)}(\alpha) \neq 0,$$

lo cual evidentemente implica $k = m$. ∎

Ejemplo 13.7.15. El polinomio

$$f(x) = 3x^6 - 3(3 - \sqrt{2})x^5 + (10 - 9\sqrt{2})x^4 - 2(3 - 5\sqrt{2})x^3 + 3(1 - 2\sqrt{2})x^2 - (1 - 3\sqrt{2})x - \sqrt{2}$$

es un elemento de $\mathbb{R}[x]$ tiene como raíces a 1 y $-\sqrt{2}$. Veamos cuál es la multiplicidad de ellas.

$$f^{(1)}(x) = 18x^5 - 15(3 - \sqrt{2})x^4 + 4(10 - 9\sqrt{2})x^3 - 6(3 - 5\sqrt{2})x^2 + 6(1 - 2\sqrt{2})x - (1 - 3\sqrt{2})$$

$$f^{(1)}(1) = (18 - 45 + 40 - 18 + 6 - 1) + (15 - 36 + 30 - 12 + 3)\sqrt{2} = 0 + 0\sqrt{2} = 0$$

$$f^{(1)}(-\sqrt{2}) =$$
$$18(-4\sqrt{2}) - 15(3 - \sqrt{2})(4) + 4(10 - 9\sqrt{2})(-2\sqrt{2}) - 6(3 - 5\sqrt{2})(2) + 6(1 - 2\sqrt{2})(-\sqrt{2}) - (1 - 3\sqrt{2}) =$$
$$-72\sqrt{2} - 60(3 - \sqrt{2}) - 8(-18 + 10\sqrt{2}) - 12(3 - 5\sqrt{2}) - 6(-4 + \sqrt{2}) - (1 - 3\sqrt{2}) =$$
$$-49 - 35\sqrt{2} \neq 0.$$

$$f^{(2)}(x) = 90x^4 - 60(3 - \sqrt{2})x^3 + 12(10 - 9\sqrt{2})x^2 - 12(3 - 5\sqrt{2})x + 6(1 - 2\sqrt{2})$$

$$f^{(2)}(1) = 90 - 60(3 - \sqrt{2}) + 12(10 - 9\sqrt{2}) - 12(3 - 5\sqrt{2}) + 6(1 - 2\sqrt{2}) = 0 + 0\sqrt{2} = 0$$

$$f^{(3)}(x) = 360x^3 - 180(3 - \sqrt{2})x^2 + 24(10 - 9\sqrt{2})x - 12(3 - 5\sqrt{2})$$

$$f^{(3)}(1) = 360 - 180(3 - \sqrt{2}) + 24(10 - 9\sqrt{2}) - 12(3 - 5\sqrt{2}) = 24 + 24\sqrt{2} \neq 0$$

Para $\alpha = 1$ se tiene $f^{(0)}(1) = f^{(1)}(1) = f^{(2)}(1) = 0$ y $f^{(3)}(1) \neq 0$ y por lo tanto $\alpha = 1$ es una raíz de multiplicidad 3 de $f(x)$.
Para $\alpha = \sqrt{2}$ se tiene $f^{(0)}(-\sqrt{2}) = 0$ y $f^{(1)}(-\sqrt{2}) \neq 0$ y así $-\sqrt{2}$ es una raíz de multiplicidad 1 de $f(x)$.
Entonces $f(x) = (x-1)^3\left(x + \sqrt{2}\right)\left(3x^2 + 1\right)$.
Obsérvese que el factor $3x^2 + 1$ de $f(x)$ resulta de dividir $f(x)$ por el producto $(x-1)^3\left(x + \sqrt{2}\right)$.

§ 13.8. Polinomios sobre $\mathbb{C}$, $\mathbb{R}$ y $\mathbb{Q}$

Hemos visto que un polinomio $f(x) \in K[x]$ de grado $n > 0$ tiene a lo más n raíces en K, pero no necesariamente n. Supongamos que un polinomio $f(x) \in K[x]$ se descompone como $f(x) = (x - \alpha_1)^{m_1} \cdot \ldots \cdot (x - \alpha_k)^{m_k}$ en $K[x]$. Entonces

$$f(x) = \underbrace{(x-\alpha_1)\cdots(x-\alpha_1)}_{m_1-veces}\underbrace{(x-\alpha_2)\cdots(x-\alpha_2)}_{m_2-veces}\cdots\underbrace{(x-\alpha_k)\cdots(x-\alpha_k)}_{m_k-veces}.$$

Si consideramos a α_i raíz de $f(x)$ tantas veces como su multiplicidad, tendremos entonces que $f(x)$ tiene exactamente $n = \partial f(x)$ raíces, no necesariamente distintas. Por ejemplo $f(x) = (x-\alpha)^n$ tiene n raíces, tantas como su grado, y todas iguales a α. En general esto no es el caso para cualquier polinomio y dependerá del polinomio mismo y del campo K, lo que significa que un polinomio en $K[x]$ puede tener en K menos raíces que su grado, aun considerando la multiplicidad de cada raíz (véase el ejemplo 13.7.15) en cuyo caso el polinomio tendrá factores irreducibles de grado mayor a 1. Cabe entonces preguntarse si existirá un campo L que contenga a K donde cada polinomio en $K[x]$ tenga tantas raíces en L como su grado. La respuesta a esta pregunta es sí, siendo éste un resultado que se prueba en la Teoría de Campos y no solamente esto, se demuestra que para cualquier campo K siempre existe un campo $\overline{K}$; que contiene a K, y al que se le llama la cerradura algebraica de K, tal que; (1) cada elemento de $\overline{K}$ es raíz de algún polinomio en $K[x]$ y (2) cada polinomio en $\overline{K}[x]$ tiene todas sus raíces en $\overline{K}$. A los campos que satisfacen la propiedad (2) se les llama ***algebraicamente cerrados***. Un ejemplo de este tipo de campos es $\mathbb{C}$, el campo de los números complejos.
Así pues, comenzaremos con el estudio de $\mathbb{C}[x]$. Más concretamente, demostraremos que $\mathbb{C}$ es la cerradura algebraica de $\mathbb{R}$.
El primer y muy importante resultado que presentaremos sobre $\mathbb{C}$ es el conocido como Teorema fundamental del álgebra y aunque se conocen distintas demostraciones de este teorema (la primera la dio Gauss en 1797) no lo demostraremos aquí debido al nivel que guarda este libro. Sin embargo, los lectores interesados pueden consultar [[**2**]]

Teorema 13.8.1. *(**Teorema fundamental del álgebra**)*
Cada polinomio en $\mathbb{C}[x]$ y de grado mayor que cero tiene al menos una raíz en $\mathbb{C}$.

Teorema 13.8.2. *Dado un polinomio $f(x) \in \mathbb{C}[x]$ y de grado $n > 0$, existen $a, \alpha_1, \ldots, \alpha_n \in \mathbb{C}$ (no necesariamente distintos) tales que $f(x) = a(x-\alpha_1)\cdot\ldots\cdot(x-\alpha_n)$. Esto es, $f(x)$ tiene tantas raíces en $\mathbb{C}$ como su grado.*

Demostración. Por inducción sobre $n = \partial f(x) > 0$.

$1°/$ $n = 1$. En este caso $f(x) = ax + b$ con $a \neq 0$ y así $f(x) = a \cdot \left(x + \frac{b}{a}\right)$ y por lo tanto para $\alpha = -\frac{b}{a}$ se tiene $f(x) = a(x-\alpha)$.
$2°/$ Supongamos que el resultado es cierto para todo polinomio de grado $n > 0$ y sea $f(x) \in \mathbb{C}[x]$ de grado $n+1 > 1$. Por el teorema 13.8.1, existe $\alpha_{n+1} \in \mathbb{C}$ tal que $f(x) = g(x)\cdot(x-\alpha_{n+1})$ y donde $g(x) \in \mathbb{C}[x]$ y de grado $n > 0$. Por hipótesis de

inducción existen $a, \alpha_1, \ldots, \alpha_n \in \mathbb{C}$ tales que

$$g(x) = a \cdot (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n).$$

Obtenemos entonces que $f(x) = a \cdot (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n) \cdot (x - \alpha_{n+1})$. ∎

El teorema 13.8.1 dice que $\mathbb{C}$ es un campo algebraicamente cerrado. Nuestro objetivo inmediato será demostrar que $\mathbb{C}$ es la cerradura algebraica de $\mathbb{R}$, es decir, probaremos que

Teorema 13.8.3. *Cada $\alpha \in \mathbb{C}$ es raíz de un polinomio en $\mathbb{R}[x]$.*

Demostración. Si $\alpha \in \mathbb{C}$, entonces $\alpha + \overline{\alpha}$ y $\alpha \cdot \overline{\alpha}$ serán números reales. Luego

$$f(x) = (x - \alpha)(x - \overline{\alpha}) = x^2 - (\alpha + \overline{\alpha}) + \alpha \cdot \overline{\alpha} \in \mathbb{R}[x]$$

y α es raíz de $f(x)$. ∎

Ahora estudiamos un poco más de cerca el anillo de polinomios $\mathbb{R}[x]$.

Teorema 13.8.4. *Si $\alpha \in \mathbb{C}$ es raíz de un polinomio $f(x) \in \mathbb{R}[x]$, entonces $\overline{\alpha}$ también lo es.*

Demostración. Sea $f(x) = a_n x^n + \cdots + a_1 x + a_0$. Como α es raíz de $f(x)$, entonces

$$f(\alpha) = a_n \alpha^n + \cdots + a_1 \alpha + a_0 = 0.$$

Tomando el conjugado de $f(\alpha)$ y aplicando las propiedades de conjugación (teorema 12.2.6) obtenemos

$$\begin{aligned} 0 &= \overline{0} \\ &= \overline{f(\alpha)} \\ &= \overline{a_n \alpha^n + \cdots + a_1 \alpha + a_0} \\ &= \overline{a_n} \cdot \overline{\alpha}^n + \cdots + \overline{a_1} \cdot \overline{\alpha} + \overline{a_0} \\ &= a_n \cdot \overline{\alpha}^n + \cdots + a_1 \cdot \overline{\alpha} + a_0 \\ &= f(\overline{\alpha}). \end{aligned}$$

Por lo tanto $\overline{\alpha}$ es raíz de $f(x)$. ∎

Corolario 13.8.5. *$\alpha \in \mathbb{C}$ es raíz de multiplicidad m de $f(x) \in \mathbb{R}[x]$ si y sólo si $\overline{\alpha}$ es raíz de multiplicidad m de $f(x)$.*

Demostración. Si α es una raíz de multiplicidad m de $f(x)$ por el teorema 13.7.14 tenemos $f^{(0)}(\alpha) = f^{(1)}(\alpha) = \cdots = f^{(m-1)}(\alpha) = 0$ y $f^m(\alpha) \neq 0$. Aplicando el teorema 13.8.4 obtenemos $f^{(0)}(\overline{\alpha}) = f^{(1)}(\overline{\alpha}) = \cdots = f^{(m-1)}(\overline{\alpha}) = 0$. Ahora si

$f^m(\overline{\alpha}) = 0$, entonces $f^{(m)}\left(\overline{\overline{\alpha}}\right) = f^{(m)}(\alpha) = 0$ que no puede ser y por lo tanto $\overline{\alpha}$ es una raíz de multiplicidad m. ∎

Nota 13.8.6. Consideramos un polinomio $f(x) \in \mathbb{R}[x]$ de grado positivo y sean $\alpha_1, \ldots, \alpha_s$ todas las raíces distintas en $\mathbb{R}$ de $f(x)$ con multiplicidad $k_1, \ldots, k_s$ respectivamente. Entonces $f(x) = (x-\alpha_1)^{k_1} \cdot \ldots \cdot (x-\alpha_k)^{k_s} \cdot g(x)$, donde $g(x) \in \mathbb{R}[x]$ y $\partial g(x) \geq 0$. Como cualquier raíz de $g(x)$ lo es también de $f(x)$, $g(x)$ no puede tener raíces reales, así que, en caso de que $\partial g(x) > 0$, las raíces de $g(x)$ son todas complejos no reales. Así, por el corolario 13.8.5 las raíces de $g(x)$ están dadas en la forma $\beta_1, \overline{\beta_1}, \ldots, \beta_r, \overline{\beta_r}$ y tal que la multiplicidad de las β_i coinciden con las de las $\overline{\beta_i}$ respectivamente y de aquí $f(x)$ se descompone en $\mathbb{C}[x]$ como

$$f(x) = (x-\alpha_1)^{k_1} \cdot \ldots \cdot (x-\alpha_s)^{k_s} \cdot (x-\beta_1)^{m_1} \cdot \left(x-\overline{\beta_1}\right)^{m_1} \cdot \ldots \cdot (x-\beta_r)^{m_r} \cdot \left(x-\overline{\beta_r}\right)^{m_r}.$$

Corolario 13.8.7. *Si $f(x) \in \mathbb{R}[x]$ es de grado impar, entonces $f(x)$ tiene al menos una raíz en $\mathbb{R}$.*

Demostración. Demostraremos, equivalentemente, que cada polinomio $f(x) \in \mathbb{R}[x]$ de grado positivo que no tiene raíces en $\mathbb{R}$ debe ser de grado par. Supongamos que $f(x) \in \mathbb{R}[x]$ es de grado positivo y que no tiene raíces en $\mathbb{R}$. Por la nota 13.8.6, se tiene entonces que

$$f(x) = (x-\beta_1)^{m_1} \cdot \left(x-\overline{\beta_1}\right)^{m_1} \cdot \ldots \cdot (x-\beta_r)^{m_r} \cdot \left(x-\overline{\beta_r}\right)^{m_r}$$

y de aquí $\partial f(x) = 2(m_1 + \cdots + m_r)$, esto es, el grado de $f(x)$ es par. ∎

Gracias al teorema 13.8.4 podemos saber quiénes son exactamente los polinomios irreducibles en $\mathbb{R}[x]$.

Proposición 13.8.8. *Las raíces en $\mathbb{C}$ del polinomio $ax^2+bx+c \in \mathbb{C}[x]$, con $a \neq 0$ son $\frac{1}{2a}\left(-b \pm \sqrt{b^2-4ac}\right)$.*

Demostración. Sea $\alpha \in \mathbb{C}$ una raíz de $ax^2 + bx + c$. Entonces $a\alpha^2 + b\alpha + c = 0$. Sumado $\frac{b^2}{4a}$ a ambos lados de esta igualdad obtenemos

$$\frac{b^2}{4a} = a\alpha^2 + b\alpha + \frac{b^2}{4a} + c = a\left(\alpha^2 + \frac{b}{a}\alpha + \frac{b^2}{4a^2}\right) + c = a\left(\alpha + \frac{b}{2a}\right)^2 + c$$

y despejando α, llegamos a que los posibles valores de α son

$$\frac{1}{2a}\left(-b \pm \sqrt{b^2-4ac}\right).$$

Finalmente para cualquiera de estos dos valores de α, se tiene que $a\alpha^2 + b\alpha + c = 0$. Por lo tanto estas son las dos raíces del polinomio ∎

Nota 13.8.9. Un polinomio en $\mathbb{R}[x]$ de grado 2 es irreducible si y sólo si no tiene raíces en $\mathbb{R}$. Para todo número real a, $\sqrt{a} \in \mathbb{C} - \mathbb{R}$ si y sólo si $a < 0$.

Corolario 13.8.10. *El polinomio $p(x) = ax^2 + bx + c \in \mathbb{R}[x]$ con $a \neq 0$ es irreducible si y sólo si $b^2 - 4ac < 0$.*

Demostración. Supongamos que $p(x)$ es irreducible en $\mathbb{R}[x]$. Entonces $p(x)$ no tiene raíces reales. Así pues, por la proposición 13.8.8, las raíces en $\mathbb{C}$ de $p(x)$ son

$$\alpha = \frac{1}{2a}\left(-b \pm \sqrt{b^2 - 4ac}\right) \in \mathbb{C} - \mathbb{R}.$$

Pero para que esto suceda y debido a que $\frac{1}{2a}$ y $-b$ son números reales, concluimos que $\sqrt{b^2 - 4ac} \in \mathbb{C} - \mathbb{R}$, lo que significa que $b^2 - 4ac < 0$. Ahora, si $b^2 - 4ac < 0$ entonces $\pm\sqrt{b^2 - 4ac} = \pm\sqrt{4ac - b^2}\,i \neq 0$ y de aquí

$$-\frac{1}{2a} \pm \sqrt{b^2 - 4ac} \in \mathbb{C} - \mathbb{R},$$

no tiene raíces reales y entonces $p(x)$ es irreducible. ∎

Estamos en condiciones de determinar todos los polinomios irreducibles en $\mathbb{R}[x]$.

Teorema 13.8.11. *Los polinomios irreducibles en $\mathbb{R}[x]$ son los polinomios de grado 1 y los polinomios $ax^2 + bx + c$ que satisfacen $b^2 - 4ac < 0$.*

Demostración. Sea $p(x)$ un polinomio irreducible en $\mathbb{R}[x]$. Como todos los polinomios de grado 1 son irreducibles (véase el ejercicio 13.5.6), podemos suponer directamente que $\partial p(x) \geq 2$. Sea $\alpha \in \mathbb{C}$ una raíz de $p(x)$. Por ser $p(x)$ irreducible se debe tener $\alpha \in \mathbb{C} - \mathbb{R}$ y por el teorema 13.8.4, $\overline{\alpha}$ también es raíz de $p(x)$. El polinomio

$$h(x) = (x - \alpha)(x - \overline{\alpha}) = x^2 - (\alpha + \overline{\alpha}) + \alpha \cdot \overline{\alpha} \in \mathbb{R}[x],$$

así que bastará demostrar que $h(x) \mid p(x)$ en $\mathbb{R}[x]$. Por el algoritmo de la división se tiene que

$$p(x) = h(x) \cdot q(x) + r(x), \quad \text{donde } r(x) = 0 \text{ o } \partial r(x) \leq 1$$

Si fuera $r(x) \neq 0$, se tendría que $0 = p(\alpha) = h(\alpha) \cdot q(\alpha) + r(\alpha)$ y similarmente $r(\overline{\alpha}) = 0$. Pero esto significaría que tanto α como $\overline{\alpha}$ son raíces de $r(x)$, donde $\alpha \neq$

$\overline{\alpha}$ ya que $\alpha \in \mathbb{C} - \mathbb{R}$, lo que es imposible debido a que $r(x)$ es de grado a lo más 1 y recordemos que un polinomio no puede tener más raíces que su grado. Por lo tanto $r(x) = 0$ y $p(x) = h(x) \cdot q(x)$ y debido a que $p(x)$ es irreducible, $q(x)$ deberá ser una constante. Hemos probado que $\partial p(x) = 2$. Por último $p(x) = ax^2 + bx + c$ es irreducible si y sólo si, por el corolario 13.8.10, $b^2 - 4ac < 0$. ∎

Resumiendo, cada polinomio en $\mathbb{R}[x]$ de grado positivo se descompone en $\mathbb{R}[x]$ como producto de polinomios irreducibles siendo cada uno de ellos de grado a lo más 2. Así pues, en el caso en que conozcamos esta descomposición podemos encontrar todas las raíces del polinomio, ya que disponemos de una fórmula para encontrar las raíces de un polinomio de grado 2. La parte complicada es precisamente conocer esta descomposición en irreducibles.

En algunos casos teniendo información adicional sobre un polinomio en particular, como por ejemplo, el hecho de conocer algunas raíces o de conocer una raíz de cierta multiplicidad, podría ayudar a encontrar el resto de las raíces, pero en general este no es el caso. Para polinomios de grado 2, 3 y 4 (ya lo hicimos para grado 2), existe un método para encontrar todas sus raíces y lo veremos en la siguiente sección.

En el caso general se dispone de métodos para aproximar raíces (sección 13.)
Por último estudiaremos el caso en que $K = \mathbb{Q}$.

Sabemos exactamente quiénes son los polinomios irreducibles en $\mathbb{R}[x]$. Para el caso de polinomios en $\mathbb{Q}[x]$ esto resulta mucho más difícil, es más, saber si un polinomio en $\mathbb{Q}[x]$ es irreducible o no es algo muy complicado y no siempre se puede dar una respuesta. Así que estudiaremos la parte del problema general enfocándonos sólo a determinar las raíces en $\mathbb{Q}$ de un polinomio en $\mathbb{Q}[x]$.

Cada polinomio con coeficientes racionales determina un polinomio con coeficientes enteros de la siguiente manera: Sea $f(x) = \frac{a_n}{b_n}x^n + \cdots + \frac{a_1}{b_1}x + \frac{a_0}{b_0} \in \mathbb{Q}[x]$, donde $a_i, b_i \in \mathbb{Z}$ y $b_i \neq 0$ para $i = 0, \ldots, n$. Entonces $b = b_0 \cdot b_1 \cdot \ldots \cdot b_n \neq 0$ y $b \cdot f(x) \in \mathbb{Z}[x]$. Es claro que un número racional $\frac{r}{s}$ $(r, s \in \mathbb{Z},\ s \neq 0)$ es raíz de $f(x)$ si y sólo si es raíz de $b \cdot f(x)$, por lo que estudiar las raíces racionales de un polinomios en $\mathbb{Q}[x]$ es lo mismo que estudiar las raíces racionales de un polinomio con coeficientes enteros. La ventaja de pasar a polinomios en $\mathbb{Z}[x]$ se ve claramente en el siguiente

Teorema 13.8.12. *Sea $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ y sea $\frac{r}{s} \in \mathbb{Q}$ una raíz de $f(x)$ con $(r, s) = 1$. Entonces $s \mid a_n$ y $r \mid a_0$.*

Demostración. Como $\frac{r}{s}$ es una raíz de $f(x)$, se tiene que

$$f\left(\frac{r}{s}\right) = a_n\left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots + a_1\left(\frac{r}{s}\right) + a_0 = 0$$

y multiplicando esta igualdad por s^n obtenemos

$$a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_1 r s^{n-1} + a_0 s^n = 0$$

y de aquí $a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_1 r s^{n-1} = -a_0 s^n$. Tenemos que

$$s \mid a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_1 r s^{n-1},$$

y ya que $s \mid a_{n-i} r^{n-i} s^i$ para toda $i = 1, \ldots, n-1$, entonces $s \mid a_n r^n$. De la misma igualdad, también $r \mid a_0 s^n$. Como $(r, s) = 1$, entonces $(r, s^n) = 1$ y $(r^n, s) = 1$ y por el teorema 7.2.16, $s \mid a_n$ y $r \mid a_0$. ∎

El teorema 13.8.12 nos asegura que podemos encontrar todas las raíces en $\mathbb{Q}$ de un polinomio $f(x) \in Q[x]$ ya que para alguna $b \in \mathbb{Z} - \{0\}$, $b \cdot f(x) \in \mathbb{Z}[x]$ y este último polinomio tiene las mismas raíces que $f(x)$, las cuales deben pertenecer a un conjunto finito determinado por los divisores tanto del coeficiente principal como del término independiente de b.

Ejemplo 13.8.13. Sea $f(x) = x^6 + \frac{1}{6}x^5 - \frac{7}{6}x^4 - \frac{1}{6}x^3 - \frac{11}{6}x^2 - \frac{1}{3}x + \frac{1}{3}$. Entonces

$$6 \cdot f(x) = 6x^6 + x^5 - 7x^4 - x^3 - 11x^2 - 2x + 2 \in \mathbb{Z}[x]$$

y sus raíces racionales (si las tiene) pertenecen al conjunto

$$\left\{\pm 1, \pm\tfrac{1}{2}, \pm\tfrac{1}{3}, \pm\tfrac{2}{3}, \pm\tfrac{1}{6}, \pm 2\right\}.$$

Sustituyendo cada uno de estos valores en el polinomio $f(x)$, llegamos a que las raíces racionales de él son $\frac{1}{3}$ y $-\frac{1}{2}$ y dividiendo

$$f(x) \text{ entre } \left(x - \tfrac{1}{3}\right) \cdot \left(x + \tfrac{1}{2}\right) = x^2 + \tfrac{1}{6}x - \tfrac{1}{6}$$

llegamos a que

$$f(x) = \left(x - \tfrac{1}{3}\right) \cdot \left(x + \tfrac{1}{2}\right) \cdot \left(x^4 - x^2 - 2\right)$$

donde $x^4 - x^2 - 2$ no tiene raíces racionales.
Por otro lado no sabemos si $x^4 - x^2 - 2$ es irreducible o no en $\mathbb{Q}$. Sin embargo, para cualquier raíz α de este polinomio, α^2 es raíz de $x^2 - x - 2$ y por lo tanto

$$\alpha^2 = \tfrac{1 \pm \sqrt{1+8}}{2} = \tfrac{1 \pm 3}{2},$$

esto es, $\alpha^2 = 2$ o $\alpha^2 = -1$, por lo que α es alguno de $\sqrt{2}, -\sqrt{2}, i, -i$ y entonces

$$x^4 - x^2 - 2 = \left(x - \sqrt{2}\right) \cdot \left(x + \sqrt{2}\right) \cdot (x - i) \cdot (x + i) = \left(x^2 - 2\right) \cdot \left(x^2 + 1\right)$$

y evidentemente $x^2 - 2$ y $x^2 + 1$ son polinomios que pertenecen a $\mathbb{Q}[x]$ y son irreducibles ahí, así que la descomposición de $f(x)$ en irreducibles en $\mathbb{Q}[x]$ es

$$f(x) = \left(x - \tfrac{1}{3}\right) \cdot \left(x + \tfrac{1}{2}\right) \cdot \left(x^2 - 2\right) \cdot \left(x^2 + 1\right).$$

La descomposición en irreducibles de $f(x)$ en $\mathbb{R}[x]$ es

$$f(x) = \left(x - \tfrac{1}{3}\right) \cdot \left(x + \tfrac{1}{2}\right) \cdot \left(x - \sqrt{2}\right) \cdot \left(x + \sqrt{2}\right) \cdot \left(x^2 + 1\right)$$

y considerando $f(x)$ en $\mathbb{C}[x]$) su descomposición es

$$f(x) = \left(x - \tfrac{1}{3}\right) \cdot \left(x + \tfrac{1}{2}\right) \cdot \left(x - \sqrt{2}\right) \cdot \left(x + \sqrt{2}\right) \cdot (x + i) \cdot (x - i).$$

§ 13.9. Las raíces de polinomios de grado 3 y 4 en $\mathbb{C}[x]$

Hemos visto que para los polinomios de grado 2 existe una fórmula para encontrar las raíces, y está dada en términos de suma, diferencia, producto, cociente y raíz cuadrada de elementos obtenidos a través de los coeficientes del polinomio. En esta sección obtendremos fórmulas para encontrar las raíces de polinomios en $\mathbb{C}[x]$ de grado 3 y grado 4, las cuales estarán dadas a través de raíces cuadradas y cúbicas de elementos de $\mathbb{C}$ determinados por los coeficientes del polinomio. Para polinomios de grado 5 o más, podemos asegurar que no existen una fórmula general que se pueda obtener a través de la suma, diferencia, producto, cociente y raíces n-ésimas de elementos de $\mathbb{C}$. Este resultado se demuestra dentro de lo que se conoce como Teoría de Galois, así que cualquier esfuerzo encaminado a buscar una fórmula del tipo mencionado resultará infructuoso. Por último, teniendo en cuenta que las raíces de un polinomio $f(x)$ coinciden con las raíces del polinomio $a \cdot f(x)$, donde a es cualquier número complejo distinto de cero, será suficiente considerar polinomios mónicos.

Las raíces de polinomios de grado 3

Sea el polinomio en $\mathbb{C}[x]$

$$f(x) = x^3 + ax^2 + bx + c. \tag{1}$$

Haciendo $x = y - \frac{a}{3}$ obtenemos

$$\begin{aligned} f\left(y-\tfrac{a}{3}\right) &= \left(y-\tfrac{a}{3}\right)^3 + a\left(y-\tfrac{a}{3}\right)^2 + b\left(y-\tfrac{a}{3}\right) + c \\ &= y^3 + \left(b - \tfrac{a^2}{3}\right)y + \left(c - \tfrac{ab}{3} + 2\left(\tfrac{a}{3}\right)^3\right) \end{aligned}$$

Si $g(x) = x^3 + r \cdot x + s$, donde $r = b - \frac{a^2}{3}$ y $s = c - \frac{ab}{3} + 2\left(\frac{a}{3}\right)^3$, no es difícil ver que α es un raíz de $f(x)$ si y sólo si $\beta = \alpha + \frac{a}{3}$ es una raíz de $g(x)$ por lo que será suficiente restringir nuestra atención a polinomios del tipo

$$g(x) = x^3 + r \cdot x + s. \tag{2}$$

Podemos suponer $r \neq 0$, ya que para $r = 0$ las raíces de $g(x)$ serán las raíces cúbicas de s y sabemos cómo encontrarlas.
Consideramos $x = z - \frac{r}{3z}$. Entonces

$$g\left(z-\frac{r}{3z}\right) = \left(z-\frac{r}{3z}\right)^3 + r\left(z-\frac{r}{3z}\right) + s = z^3 - \left(\frac{r}{3z}\right)^3 + s = \frac{1}{z^3}\left(z^6 + sz^3 - \left(\frac{r}{3}\right)^3\right)$$

y de aquí $z^3 g\left(z - \frac{r}{3z}\right) = z^6 + sz^3 - \left(\frac{r}{3}\right)^3$.
Sea $h(x) = x^6 + sx^3 - \left(\frac{r}{3}\right)^3$. Teniendo en cuenta que las raíces de $h(x)$ son distintas de cero debido a que $r \neq 0$, no es difícil ver que

γ es un raíz de $h(x)$ si y sólo si $\beta = \gamma - \frac{r}{3\gamma}$ es raíz de $g(x)$.

Observación 13.9.1. Primero que $\beta = \gamma - \frac{r}{3\gamma}$ nos dice que γ es solución de $x^2 - \beta x - \frac{r}{3} = 0$ y segundo puede parecer inconsistente el hecho de que $h(x)$ tiene 6 raíces y $g(x)$ tiene 3, pero como se verá más adelante, en realidad las raíces de $h(x)$ se particionan en 3 parejas de tal manera que cada pareja produce la misma β.

Encontremos pues las raíces de $h(x)$. Consideremos γ una raíz de $h(x)$. Entonces γ^3 es raíz de $x^2 + sx - \left(\frac{r}{s}\right)^3$ y por lo tanto

$$\gamma^3 = \tfrac{1}{2}\left(-s \pm \sqrt{s^2 + 4\left(\tfrac{r}{3}\right)^3}\right) = -\tfrac{s}{2} \pm \sqrt{\left(\tfrac{s}{2}\right)^2 + \left(\tfrac{r}{3}\right)^3}.$$

$1^{\underline{er}}$ caso: $\gamma^3 = -\frac{s}{2} + \sqrt{\left(\frac{s}{2}\right)^2 + \left(\frac{r}{3}\right)^3} = A$. γ es una raíz cúbica de A y las otras raíces son $\gamma\xi$ y $\gamma\xi^2$, donde $\xi = -\frac{1}{2} + \frac{1}{2}\sqrt{3}i$ es una raíz cúbica de 1 (evidentemente la otra es $\xi^2 = -\frac{1}{2} - \frac{1}{2}\sqrt{3}i$, así que no existe problema en cuál de estos dos valores

consideramos como ξ). Por lo ya visto, entonces

$$\beta_1 = \gamma - \frac{r}{3\gamma},\ \beta_2 = \gamma\xi - \frac{r}{3\gamma\xi} = \gamma\xi - \xi^2\left(\frac{r}{3\gamma}\right)\ y\ \beta_3 = \gamma\xi^2 - \xi\left(\frac{r}{3\gamma}\right) \tag{3}$$

deben ser raíces de $g(x)$. Verifiquémoslo:

$$g(\beta_1) = g\left(\gamma - \frac{r}{3\gamma}\right) = \left(\gamma - \frac{r}{3\gamma}\right)^3 - r\left(\gamma - \frac{r}{3\gamma}\right) + s =$$

$$\gamma^3 - \left(\frac{r}{3\gamma}\right)^3 + s = \gamma^3 - \left(\frac{r}{3}\right)^3\frac{1}{\gamma^3} + s =$$

$$-\frac{s}{2} + \sqrt{\left(\frac{s}{2}\right)^2 + \left(\frac{r}{3}\right)^3} - \left(\frac{r}{3}\right)^3 \cdot \frac{1}{-\frac{s}{2} + \sqrt{\left(\frac{s}{2}\right)^2 + \left(\frac{r}{3}\right)^3}} + s =$$

$$-\frac{s}{2} + \sqrt{\left(\frac{s}{2}\right)^2 + \left(\frac{r}{3}\right)^3} - \left(\frac{r}{3}\right)^3 \cdot \frac{-\frac{s}{2} - \sqrt{\left(\frac{s}{2}\right)^2 + \left(\frac{r}{3}\right)^3}}{\left(-\frac{s}{2} + \sqrt{\left(\frac{s}{2}\right)^2 + \left(\frac{r}{3}\right)^3}\right)\left(-\frac{s}{2} - \sqrt{\left(\frac{s}{2}\right)^2 + \left(\frac{r}{3}\right)^3}\right)} + s =$$

$$-\frac{s}{2} + \sqrt{\left(\frac{s}{2}\right)^2 + \left(\frac{r}{3}\right)^3} - \left(\frac{r}{3}\right)^3 \cdot \frac{-\frac{s}{2} - \sqrt{\left(\frac{s}{2}\right)^2 + \left(\frac{r}{3}\right)^3}}{\left(\frac{s}{2}\right)^2 - \left(\left(\frac{s}{2}\right)^2 + \left(\frac{r}{3}\right)^3\right)} + s =$$

$$-\frac{s}{2} + \sqrt{\left(\frac{s}{2}\right)^2 + \left(\frac{r}{3}\right)^3} - \frac{s}{2} - \sqrt{\left(\frac{s}{2}\right)^2 + \left(\frac{r}{3}\right)^3} + s = 0$$

Para β_2, teniendo en cuenta que $\xi^3 = 1 = \left(\xi^2\right)^3$, tenemos que

$$\begin{aligned} g(\beta_2) &= g\left(\gamma\xi - \tfrac{r}{3\gamma\xi}\right) \\ &= \left(\gamma\xi - \tfrac{r}{3\gamma\xi}\right)^3 + r\left(\gamma\xi - \tfrac{r}{3\gamma\xi}\right) + s \\ &= (\gamma\xi)^3 - \left(\tfrac{r}{3\gamma\xi}\right)^3 + s \\ &= \gamma^3 - \left(\tfrac{r}{3\gamma}\right)^3 + s = 0 \end{aligned}$$

De manera análoga $g(\beta_3) = 0$.

$2^{\underline{o}}$ caso: $\gamma^3 = -\frac{s}{2} - \sqrt{\left(\frac{s}{2}\right)^2 + \left(\frac{r}{3}\right)^3} = B$

Realizando el mismo procedimiento que en el primer caso, obtenemos las mismas raíces β_1, β_2 y β_3 del caso anterior y esto se debe a que γ es una raíz cúbica de A si y sólo si $\gamma' = -\frac{r}{3\gamma}$ es una raíz cúbica de B. Veamos

$$\begin{aligned}\gamma'^3 &= \left(-\frac{r}{3\gamma}\right)^3 \\ &= -\left(\frac{r}{3}\right)^3 \cdot \frac{1}{\gamma^3} \equiv -\left(\frac{r}{3}\right)^3 \cdot \frac{-\frac{s}{2} - \sqrt{\left(\frac{s}{2}\right)^2 + \left(\frac{r}{3}\right)^3}}{-\left(\frac{r}{3}\right)^3} \\ &= -\frac{s}{2} - \sqrt{\left(\frac{s}{2}\right)^2 + \left(\frac{r}{3}\right)^3} = B\end{aligned}$$

Pero $\gamma' - \frac{r}{3\gamma'} = -\left(\frac{r}{3\gamma}\right) - \frac{r}{3\left(-\frac{r}{3\gamma}\right)} = \gamma - \left(\frac{r}{3\gamma}\right) = \beta_1$.

Ahora, $\gamma'\xi = -\left(\frac{r}{3\gamma}\right)\cdot\xi = -\frac{r}{3\gamma\xi^2}$; $\gamma'\xi^2 = -\left(\frac{r}{3\gamma}\right)\cdot\xi^2 = -\frac{r}{3\gamma\xi}$ y

$\gamma'\xi - \frac{r}{3\gamma'\xi} = -\frac{r}{3\gamma\xi^2} - \frac{r}{3\left(-\frac{r}{3\gamma\xi^2}\right)} = -\frac{r}{3\gamma\xi^2} + \gamma\xi^2 = \beta_3$

$\gamma'\xi^2 - \frac{r}{3\gamma'\xi^2} = -\frac{r}{3\gamma\xi} - \frac{r}{3\left(-\frac{r}{3\gamma\xi}\right)} = -\frac{r}{3\gamma\xi} + \gamma\xi = \beta_2$.

donde β_1, β_2 y β_3 están dadas en (3).

Por último, de la igualdad $\gamma' = -\frac{r}{3\gamma}$ obtenemos $\gamma\cdot\gamma' = -\frac{r}{3}$.

Obtenemos así el siguiente

Teorema 13.9.2. *Las raíces del polinomio $x^3 + ax^2 + bx + c$ son*

$$\alpha_1 = \gamma + \gamma' - \tfrac{a}{3},\ \alpha_2 = \gamma\xi + \gamma'\xi^2 - \tfrac{a}{3}\ y\ \alpha_3 = \gamma\xi^2 + \gamma'\xi - \tfrac{a}{3}$$

donde γ y γ' son las raíces cúbicas respectivamente de

$$-\frac{s}{2} + \sqrt{\left(\frac{s}{2}\right)^2 + \left(\frac{r}{3}\right)^3}\ y\ -\frac{s}{2} - \sqrt{\left(\frac{s}{2}\right)^2 + \left(\frac{r}{3}\right)^3}$$

y tales que $\gamma\cdot\gamma' = -\frac{r}{3}$, $\xi = -\frac{1}{2} - \frac{1}{2}\sqrt{3}i$, donde $r = b - \frac{a^2}{3}$, $s = c - \frac{ab}{3} + 2\left(\frac{a}{3}\right)$.

Demostración. Hemos hecho prácticamente todo el trabajo y sólo faltaría ver que $\beta_1 = \gamma + \gamma'$, $\beta_2 = \gamma\xi + \gamma'\xi^2$ y $\beta_3 = \gamma\xi^2 + \gamma'\xi$. Recuérdese que α_i es raíz del polinomio si y sólo si $\beta_i = \alpha_i + \frac{a}{3}$ es raíz de $g(x)$.

Teniendo en cuenta que $\gamma\cdot\gamma' = -\frac{r}{3}$ y que $\xi^3 = 1$, obtenemos

$\beta_1 = \gamma' - \frac{r}{3\gamma} = \gamma + \left(-\frac{r}{3}\right)\cdot\frac{\gamma'}{\gamma\cdot\gamma'} = \gamma + \left(-\frac{r}{3}\right)\cdot\frac{\gamma'}{\left(-\frac{r}{3}\right)} = \gamma + \gamma'$

$\beta_2 = \gamma\xi' - \frac{r}{3\gamma\xi} = \gamma\xi + \left(-\frac{r}{3}\right)\cdot\frac{\gamma'\xi^2}{\gamma\xi\gamma'\xi^2} = \gamma\xi + \left(-\frac{r}{3}\right)\cdot\frac{\gamma'\xi^2}{\left(-\frac{r}{3}\right)} = \gamma\xi + \gamma'\xi^2$

$\beta_3 = \gamma\xi^{2\prime} - \frac{r}{3\gamma\xi^2} = \gamma\xi^2 + \left(-\frac{r}{3}\right)\cdot\frac{\gamma'\xi}{\gamma\xi^2\gamma'\xi} = \gamma\xi^2 + \left(-\frac{r}{3}\right)\cdot\frac{\gamma'\xi}{\left(-\frac{r}{3}\right)} = \gamma\xi^2 + \gamma'\xi$. ∎

Ejemplo 13.9.3. Sea $f(x) = x^3 + 3x^2 + 9x + 9$. Entonces $a = 3$, $b = 9$ y $c = 9$ y los valores para r y s son $r = b - \frac{a^2}{3} = 6$ y $s = c - \frac{ab}{3} + 2\left(\frac{a}{3}\right) = 2$.

Sean $\gamma = \sqrt[3]{-\frac{s}{2} + \sqrt{\left(\frac{s}{2}\right)^2 + \left(\frac{r}{3}\right)^3}} = \sqrt[3]{-1 + \sqrt{1 + 2^3}} = \sqrt[3]{2}$

$\gamma' = \sqrt[3]{-\frac{s}{2} - \sqrt{\left(\frac{s}{2}\right)^2 + \left(\frac{r}{3}\right)^3}} = \sqrt[3]{-1 - \sqrt{1 + 2^3}} = -\sqrt[3]{4}$

y donde $\gamma \cdot \gamma' = -2 = -\frac{r}{3}$.

Entonces las raíces de $f(x)$ son

$\alpha_1 = \sqrt[3]{2} - \sqrt[3]{4} - 1$, $\alpha_2 = \sqrt[3]{2}\xi - \sqrt[3]{4}\xi^2 - 1$, y $\alpha_3 = \sqrt[3]{2}\xi^2 - \sqrt[3]{4}\xi - 1$, donde $\xi = -\frac{1}{2} + \frac{1}{2}\sqrt{3}i$ y $\xi^2 = -\frac{1}{2} - \frac{1}{2}\sqrt{3}i$.

Las raíces de polinomios de grado 4

Sea $f(x) = x^4 + ax^3 + bx^2 + cx + d$.

Haciendo un cambio de variable considerando $x = y - \frac{a}{4}$ obtenemos

$f\left(y - \frac{a}{4}\right) = y^4 + \frac{1}{4}\left(8b - 3a^2\right)y^2 + \frac{1}{8}\left(a^3 - 4ab + 8c\right)y + \frac{1}{256}\left(13a^4 - 64ac + 256d\right)$.

Entonces α es raíz de $f(x)$ si y sólo si $\beta = \alpha + \frac{a}{4}$ es raíz de

$$g(x) = x^4 + rx^2 + sx + t,$$

donde $r = \frac{1}{4}\left(8b - 3a^2\right)$, $s = \frac{1}{8}\left(a^3 - 3a^2\right)$ y $t = \frac{1}{256}\left(13a^4 - 64ac + 256d\right)$ y por esta razón, restringimos nuestro estudio a polinomios de la forma

$$g(x) = x^4 + rx^2 + sx + t.$$

Consideremos una raíz β de $g(x)$ y sea $\gamma \in \mathbb{C}$. Entonces $\beta^4 = -r\beta^2 - s\beta - t$.

$$\left(\beta^2 + \gamma\right)^2 = \beta^4 + 2\beta^2\gamma + \gamma^2 = -r\beta^2 - s\beta - t + 2\gamma\beta^2 + \gamma^2 = (2\gamma - r)\beta^2 - s\beta + \left(\gamma^2 - t\right)$$

Encontraremos γ y números complejos δ y ρ que satisfacen

$$\left(\beta^2 + \gamma\right)^2 = (\delta\beta + \rho)^2$$

que es

$$(2\gamma - r)\beta^2 - s\beta + \left(\gamma^2 - t\right) = \delta^2\beta^2 + 2\delta\rho\beta + \rho^2$$

y esta igualdad se dará si tomamos $2\gamma - r = \delta^2$, $-s = 2\delta\rho$ y $\gamma^2 - t = \rho^2$, independientemente de quién sea β.

Entonces $s^2 = 4\delta^2\rho^2 = 4(2\gamma - r)\left(\gamma^2 - t\right)$, y por lo tanto

$$8\gamma^3 - 4r\gamma^2 - 8t\gamma + 4rt - s^2 = 0,$$

lo que significa que γ es raíz del polinomio $h(x) = x^3 - \frac{1}{2}rx^2 - tx + \left(\frac{rt}{2} - \frac{s^2}{8}\right)$, el cual está dado en términos de los coeficientes de $g(x)$.
Concluyendo, para una raíz γ de $h(x)$ podemos encontrar números complejos δ y r, a saber,

$$\delta = \sqrt{2\gamma - r} \ \ y \ \ \rho = -\frac{s}{2\delta} = -\frac{s}{2\sqrt{2\gamma - r}},$$

tales que $\left(\beta^2 + \gamma\right)^2 = (\delta\beta + \rho)^2$ y de aquí obtenemos dos posibilidades

$$\beta^2 + \gamma = \delta\beta + \rho \ \text{ o } \ \beta^2 + \gamma = -\delta\beta - \rho$$

por lo que β será raíz del polinomio $x^2 - \delta x + (\gamma - \rho)$ o del polinomio $x^2 + \delta x + (\gamma + \rho)$.
Por último, considerando γ una raíz cúbica de $h(x)$, $\delta = \sqrt{2\gamma - r}$ y $\rho = -\frac{s}{2\sqrt{2\gamma - r}}$, llegamos a que cualquier raíz de $x^2 - \delta x + (\gamma - \rho)$ o de $x^2 + \delta x + (\gamma + \rho)$ deberá ser raíz de $g(x)$.
En resumen, tenemos el siguiente

Teorema 13.9.4. *Dado el polinomio $f(x) = x^4 + ax^3 + bx^2 + cx + d \in \mathbb{C}[x]$, sus raíces están dadas por*

$\alpha_1 = \frac{\delta}{2} + \sqrt{\left(\frac{\delta}{2} - (\gamma - \rho)\right)} - \frac{a}{4}$
$\alpha_2 = \frac{\delta}{2} - \sqrt{\left(\frac{\delta}{2} - (\gamma - \rho)\right)} - \frac{a}{4}$
$\alpha_3 = -\frac{\delta}{2} + \sqrt{\left(\frac{\delta}{2} - (\gamma + \rho)\right)} - \frac{a}{4}$
$\alpha_4 = -\frac{\delta}{2} - \sqrt{\left(\frac{\delta}{2} - (\gamma + \rho)\right)} - \frac{a}{4}$

donde γ es una raíz del polinomio $x^3 - \frac{1}{2}x^2 - tx + \frac{1}{8}\left(4rt - s^2\right)$ con

$$r = \frac{1}{4}\left(8b - 3a^2\right), \ \ s = \frac{1}{8}\left(a^3 - 4ab + 8c\right), \ \ t = \frac{1}{256}\left(13a^2 - 64ac + 256d\right)$$

y donde $\delta = \sqrt{2\gamma - r}$ y $\rho = -\frac{s}{2\sqrt{2\gamma - r}}$.

Observemos que para encontrar las raíces de un polinomio de grado 4, será suficiente dar una raíz de un polinomio de grado 3 cuyos coeficientes están determinados por los coeficientes del polinomio en cuestión y cuyas soluciones sabemos encontrar (teorema 13.9.2).

§ 13.10. Método de Strum

Como no existe un método general para obtener las raíces de un polinomio en $\mathbb{C}[x]$ (por supuesto de grado 5 en adelante), en el caso de polinomios con coeficientes reales podríamos al menos intentar aproximarnos a las raíces reales, siempre y cuando las tengan, para acercarnos a ellas tanto como uno quiera, en el sentido de encontrar un número real que difiera de una raíz en menos de un número real positivo ε dado de antemano (mientras más pequeño sea ε estaremos más cerca de la raíz).

¿Será posible encontrar un mecanismo de este tipo? La respuesta es sí y la idea es la siguiente.

Desde el punto de vista del análisis, un polinomio $f(x)$ con coeficientes reales es una función continua de $\mathbb{R}$ en $\mathbb{R}$, lo que intuitivamente significa que su gráfica $\{(x, f(x)) \mid x \in \mathbb{R}\}$ no se rompe en ningún momento. Si la gráfica de esta curva toca algún punto x_0 del eje X, ese punto x_0 será una raíz de $f(x)$ y en este caso existen dos tipos de posibilidades mostrados en las figura 1 y 2.

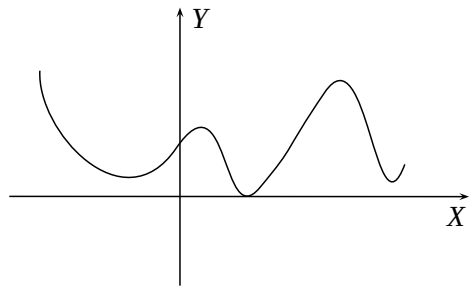


Figura 1. Gráfica de $f(x)$ tangente al eje X

En la figura 1, la gráfica toca al eje X pero no lo atraviesa y en la figura 2 la gráfica atraviesa el eje X. En el segundo caso se tendrá que para ciertos números reales $x_1 < x_2$, $f(x_1) < 0$ y $f(x_2) > 0$ o $f(x_1) > 0$ y $f(x_2) < 0$. Por otro lado, si $x_1, x_2 \in \mathbb{R}$, son tales que ($f(x_1) < 0$ y $f(x_2) > 0$) o ($f(x_1) > 0$ y $f(x_2) < 0$), el *Teorema del Valor Intermedio* nos asegura que para algún x entre x_0 y x_1, $f(x) = 0$, esto es, habrá una raíz de $f(x)$. El *método de Strum* nos permite saber cuántas raíces existen entre dos números reales x_1 y x_2 tales que $f(x_1) \neq 0$ y $f(x_2) \neq 0$, de tal manera que este método es útil en el caso (2) y en el caso (1) nos permite

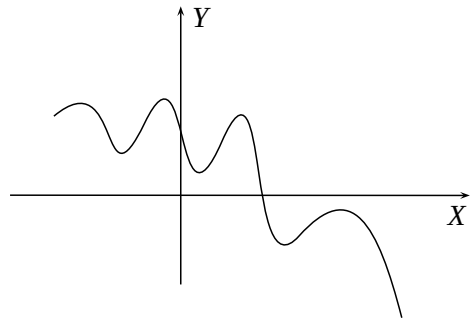


Figura 2. Gráfica de $f(x)$ que corta al eje X

saber el número de raíces que existen en un intervalo donde el valor de $f(x)$ en los extremos tiene signo distinto.

Método de Strum

Sea $f(x) \in \mathbb{R}[x]$ y aplicando el algoritmo de Euclides a los polinomios $f(x)$ y $f'(x)$:

$$\begin{array}{rcl@{\qquad}rcl@{\qquad}l}
f(x) & = & f'(x)\cdot q_1(x) + r_1(x) & \partial r_1(x) & < & \partial f'(x) & t_1(x) = -r_1(x) \\
f'(x) & = & t_1(x)\cdot q_2(x) + r_2(x) & \partial r_2(x) & < & \partial r_1(x) & t_2(x) = -r_2(x) \\
\vdots & & \vdots & \vdots & & & \vdots \\
r_{n-3}(x) & = & t_{n-2}(x)\cdot q_{n-1}(x) + r_{n-1}(x) & \partial r_{n-1}(x) & < & \partial r_{n-2}(x) & t_{n-1}(x) = -r_{n-1}(x) \\
r_{n-2}(x) & = & t_{n-1}(x)\cdot q_n(x) + r_n(x) & \partial r_n(x) & < & \partial r_{n-1}(x) & t_n(x) = -r_n(x) \\
r_{n-1}(x) & = & t_n(x)\cdot q_{n+1}(x) + 0 & & & &
\end{array}$$

$f(x), f'(x), t_1(x), \ldots, t_n(x)$ se llama la sucesión de Strum de $f(x)$.

Dado un polinomio $f(x) \in \mathbb{R}[x]$ y $a \in \mathbb{R}$, $V_f(a)$ denotará el número de variaciones de signo en la sucesión $f(a), f_1(a), \ldots, f_{n+1}(a)$, donde si algún $f_i(a) = 0$, la omitiremos de la sucesión. por ejemplo si los valores de la sucesión son $-7, -2, 1, 0, -1, 0, -2, 1, 1, -5$, quitamos los cero, la sucesión resultante será -7, -2, 1, -1, -2, 1, 1, -5 y entonces $V_f(a) = 4$.
Una variación de signo en la sucesión se dará cuando el sucesor distinto de cero de un elemento de la sucesión sea de signo contrario a su antecesor.

Teorema 13.10.1. ***Teorema de Strum***. *Sea $f(x)$ un polinomio con coeficientes reales y $a, b \in \mathbb{R}$ tales que $a < b$, $f(a) \neq 0$ y $f(b) \neq 0$. Entonces el número de raíces reales entre a y b es $V_f(a) - V_f(a)$.*

Ejemplo 13.10.2. Sea $f(x) = x^3 + x^2 + 8x + 6$. Entonces $f(-1) = (-1)^3 + (-1)^2 + 8(-1) + 6 = -2$ y $f(0) = 6$, así que $f(x)$ tiene al menos una raíz entre -1 y 0. Veamos cuántas tiene.

$f'(x) = 3x^2 + 2x + 8$

$$x^3 + x^2 + 8x + 6 = (3x^2 + 2x + 8)(\tfrac{1}{3}x + \tfrac{1}{9}) + (\tfrac{46}{9}x + \tfrac{46}{9})$$
$$3x^2 + 2x + 8 = (\tfrac{46}{9}x + \tfrac{46}{9})(\tfrac{27}{46}x - \tfrac{27}{46}) + 11$$

La sucesión de Strum es $f(x) = x^3 + x^2 + 8x + 6$, $f_1(x) = 3x^2 + 2x + 8$, $f_2(x) = -\frac{46}{9}x - \frac{46}{9}$, $f_3(x) = -11$.

Para $a = -1$, la sucesión obtenida es -2, 9, 0, -11 y así $V_f(-1) = 2$.

Para $a = 0$, la sucesión obtenida es 6, 8, $-\frac{46}{9}$, -11 y entonces $V_f(0) = 1$.

Por el teorema de Strum habrá una sola raíz entre -1 y 0. Como ya hemos dicho al inicio de la sección podemos aproximar a esta raíz, que denotaremos por α, tanto como queramos:

Dividiendo el intervalo $(-1, 0)$ en 10 partes iguales, se tiene que $f\left(\frac{-8}{10}\right) < 0$ y $f\left(\frac{-7}{10}\right) > 0$, así que $\frac{-8}{10} < \alpha < \frac{-7}{10}$. Nuevamente dividiendo este intervalo $\left(\frac{-8}{10}, \frac{-7}{10}\right)$ en 10 partes iguales, llegaremos a que $f\left(\frac{-8}{10} + \frac{4}{10^2}\right) = f\left(\frac{-76}{10^2}\right) < 0$ y $f\left(\frac{-8}{10} + \frac{5}{10^2}\right) = f\left(\frac{-75}{10^2}\right) > 0$ y entonces $\frac{-76}{10^2} < \alpha < \frac{-75}{10^2}$, lo que significa que $0 < \alpha - \frac{-76}{10^2} < \frac{1}{10^2}$. Ahora dividiremos el intervalo $\left(\frac{-76}{10^2}, \frac{-75}{10^2}\right)$ en 10 partes iguales y ubicamos a α en el intervalo correspondiente procediendo de la misma manera, etc. Por último si queremos aproximar a α en menos de $\varepsilon > 0$, basta escoger n tal que $\frac{1}{10^n} < \varepsilon$, es decir, es suficiente tomar $n > -\frac{\ln \varepsilon}{\ln 10}$.

§§ Ejercicios sección 13.1.

13.1.1. Sean $a, b, c, d, e \in \mathbb{Q}$, y suponga que $f(x) = 2ax^3 - 3x^2 - b^2x - 7$ y $g(x) = cx^4 + 10x^3 - (d + 1)x^2 - 4x + e$. Encuentra los valores de a, b, c, d, e si se tiene que $f(x) = g(x)$.

§ § Ejercicios sección 13.2.

13.2.1. [1] Sea A un a anillo y $f(x), g(x) \in A[x]$. Demuestre que

$$f(x) + g(x) = g(x) + f(x).$$

13.2.2. [2] Sea A un a anillo conmutativo y $f(x), g(x), h(x) \in A[x]$. Demuestre que $(f(x) \cdot g(x)) \cdot h(x) = f(x) \cdot (g(x) \cdot h(x))$.

13.2.3. Sea A un anillo conmutativo. Demuestre

(1) La conmutatividad de la suma en $A[x]$.
(2) La asociatividad del producto en $A[x]$.

13.2.4. Considérese los siguientes polinomios en $\mathbb{Q}[x]$:

$$a(x) = -x^2 - 5x + 7, \quad b(x) = 2x^3 - 5x^2 + \tfrac{3}{2}x - 1, \quad c(x) = x^4 + \tfrac{1}{7}x^3 - x,$$
$$d(x) = -x^3 + 5, \qquad e(x) = 2x + 6.$$

Efectúe las siguientes operaciones y determine el grado grado en cada caso.

(1) $a(x) + c(x)$ (2) $b(x) + 2d(x)$ (3) $a(x) + b(x) - e(x)$
(4) $b(x) \cdot c(x)$ (5) $a(x) \cdot d(x) + \frac{1}{2}b(x) \cdot e(x)$ (6) $(a(x))^2 - (e(x))^3$

13.2.5. Determinar $a, b, c \in \mathbb{R}$, de modo que

(1) $9x^2 - 16x + 4 = a(x-1)(x-2) + bx(x-2) + cx(x-1)$;
(2) $x + 2 = a(x^2 + x + 1) + (bx + c)(x - 1)$.

13. 2.6. Determinar los coeficientes de x y de x^3 en el polinomio $3(x-1)(x-2)(x-4)(x-5)$.

13.2.7. Considera el anillo conmutativo $\mathbb{Z}_6$.

(a) Liste todos los polinomios de grado 3 en $\mathbb{Z}_6[x]$;
(b) Sabemos que $\mathbb{Z}_6$ es finito, ¿el anillo $\mathbb{Z}_6[x]$ es finito?;
(c) Dé un ejemplo de dos polinomios $f(x)$ y $g(x)$ en $\mathbb{Z}_6[x]$ de grado positivo cuyo producto sea un polinomio de grado menor que $\partial f(x) + \partial g(x)$.

13.2.8 itemindent=5.7mm, leftmargin=0.8mm. Si $f(x) \in \mathbb{Z}_2[x]$ y en la expresión de $f(x)$ omitimos los coeficientes iguales a 0. ¿Cómo es la expresión de $f(x)$?

13.2.9. ¿Podemos decir cuál es el grado de un polinomio de la forma $ax^3 + bx^2 + cx + d$?

---

[1] Parte del teorema 13.2.2 pág. 424.
[2] Parte del teorema 13.2.4 pág. 426.

13.2.10. Sea $f(x) \neq 0$ en $K[x]$. Demuestre que si $a \in K - \{0\}$, entonces $\partial(af(x)) = \partial f(x)$.

13.2.11. Sea $f(x) \in K[x]$ un polinomio de grado 5 con

$$f(x) = f_1(x) \cdot f_2(x) \cdot f_3(x) \cdot f_4(x)$$

donde los polinomios $f_i(x)$ tienen grado positivo para $i = 1, 2, 3, 4$. Demuestre que al menos dos de los $f_i(x)$ tienen el mismo grado.

§ § Ejercicios sección 13.3.

13.3.1. [3] Sean $f(x), g(x)$ y $h(x)$ polinomios en $K[x]$. Demuestre que

(1) $a \mid f(x)$ para toda $a \in K - \{0\}$.
(2) Si $f(x) \mid g(x)$, entonces $a \cdot f(x) \mid b \cdot g(x)$ para cualesquiera $a \in K - \{0\}$ y $b \in K$. En particular $f(x) \mid f(x)$ y $f(x) \mid 0$.
(3) Si $f(x) \mid g(x)$, y $g(x) \mid h(x)$, entonces $f(x) \mid h(x)$.
(4) Si $f(x) \mid g(x)$, y $f(x) \mid h(x)$, entonces $f(x) \mid r(x) \cdot g(x) + s(x) \cdot h(x)$ para cualesquiera $r(x), s(x) \in K[x]$. En particular $f(x) \mid g(x) + h(x)$.
(5) Si $0 \mid f(x)$, entonces $f(x) = 0$. Esto es, el único polinomio que es divisible por 0 es el polinomio cero.

13.3.2. Sean $f(x), g(x), h(x) \in K[x]$. Demuestre que:

(1) $a \mid f(x)$, para toda $a \in K - \{0\}$.
(2) Si $f(x) \mid g(x)$, entonces $af(x) \mid bg(x)$ para cualesquiera $a \in K - \{0\}$ y $b \in K$. En particular $f(x) \mid f(x)$ y $f(x) \mid 0$.
(3) Si $f(x) \mid g(x)$ y $g(x) \mid h(x)$, entonces $f(x) \mid h(x)$.
(4) Si $f(x) \mid g(x)$ y $f(x) \mid h(x)$, entonces $f(x) \mid r(x) \cdot g(x) + s(x) \cdot h(x)$ para cualesquiera $r(x), s(x) \in K[x]$. En particular $f(x) \mid g(x) \pm h(x)$.
(5) Si $0 \mid f(x)$, entonces $f(x) = 0$. Esto es, el único polinomio que es divisible por 0 es el polinomio cero.

13.3.3. Sea $f(x) \in K[x]$. Demuestre que $f(x) \mid 1$ si y sólo si $f(x) = a \neq 0$ con $a \in K$.

13.3.4. Sean $a, b \in K$. Demuestre que $(x - a) \mid (x - b)$ si y sólo si $a = b$.

13.3.5. Sean $f(x), g(x) \in K[x]$ con $g(x) \neq 0$ y $f(x) = g(x) \cdot q(x) + r(x)$ donde $r(x) = 0$ o $\partial r(x) < \partial g(x)$. Demuestre que $g(x) \mid f(x)$ si y sólo si $r(x) = 0$.

[3] Parte del teorema 13.3.3 pág. 430.

13.3.6. Sean $f(x), g(x) \in K[x]$ y $a \in K$. Demuestre que si $x-a \mid f(x)$ y $x-a \nmid g(x)$, entonces $x - a \nmid f(x) + g(x)$.

13. 3.7. Encontrar el cociente y el residuo al hacer la división de $a(x)$ entre $b(x)$ para los siguientes polinomios:

(1) $a(x) = x^5 + 2$,	$b(x) = 2x^3 - 3x^2 + x - 2$,	en $\mathbb{Q}[x]$;
(2) $a(x) = x^3 - 3x^2 - x - 1$,	$b(x) = 3x^2 - 2x + 1$,	en $\mathbb{Q}[x]$;
(3) $a(x) = \frac{1}{2}x^6 + 2x^5 - 3x^3 - 5x^2 - 2x + \frac{3}{2}$,	$b(x) = x^4 - x^2 - 2x - 1$,	en $\mathbb{Q}[x]$;
(4) $a(x) = x^6 + (\pi + 2)x^5 + 2\pi x^4 - \pi x + \pi$,	$b(x) = x^4 + 2x^3 - 1$,	en $\mathbb{R}[x]$;
(5) $a(x) = x^3 + ix^2 + x + i$,	$b(x) = x^2 + i$,	en $\mathbb{C}[x]$;
(6) $a(x) = x^6 - 3x^5 + 4x^2 - 3x + 2$,	$b(x) = x^2 + 2x - 3$,	en $\mathbb{Z}_7[x]$.

13.3.8. Para qué valores de $a \in \mathbb{R}$ se cumple que

$$(x^2 + ax - a^2) \mid \left(x^3 + ax^2 - 4x - a + 2\right)$$

en $\mathbb{R}[x]$.

13. 3.9. Determina los coeficientes de a y b en $\mathbb{Q}$ para que el polinomio $x^3 + ax^2 + bx + 5$ sea divisible por $x^2 + x + 1$ en $\mathbb{Q}[x]$.

13.3.10. En $\mathbb{R}[x]$, ¿bajo qué condición el polinomio

(1) $x^3 + px + q$ es divisible por un polinomio de la forma $x^2 + mx - 1$;
(2) $x^4 + px^2 + q$ es divisible por un polinomio de la forma $x^2 + mx + 1$?

13.3.11. Si $f(x) \in K[x]$ es un polinomio de grado n y $\alpha \in K$ es un elemento dado, demuestre que $f(x)$ se puede escribir de la forma

$$f(x) = \sum_{r=0}^{n} a_r (x - \alpha)^r, \quad \text{con} \quad a_r \in K.$$

13.3.12. En cada caso, exprésese $f(x) \in \mathbb{C}[x]$ en la forma $f(x) = \sum a_r (x - \alpha)^r$.

(1) $f(x) = x^3 + x^2 + x + 1$,	$\alpha = 1$;
(2) $f(x) = x^4 + 2x^3 - 3x^2 - 4x + 1$,	$\alpha = -1$;
(3) $f(x) = x^5$,	$\alpha = 1$;
(4) $f(x) = x^4 - 8x^3 + 24x^2 - 50x + 90$,	$\alpha = 2$;
(5) $f(x) = x^4 + 2ix^3 - (1 + i)x^2 - 3x + 7 + i$,	$\alpha = -i$;
(6) $f(x) = x^4 + (3 - 8i)x^3 - (21 + 18i)x^2 - (33 - 20i)x + 7 + 18i$,	$\alpha = -1 + 2i$.

§§ Ejercicios sección 13.4.

13.4.1. Demuestre el algoritmo de Euclides en $K[x]$ para hallar el máximo común divisor de $f(x)$ y $g(x)$ en $K[x]$. Sugerencia: vea el algoritmo de Euclides en $\mathbb{Z}$.

13.4.2. Sean $f(x)$ y $g(x)$ polinomios en $\mathbb{Q}[x]$. Demuestre que el máximo común divisor de $f(x)$ y $g(x)$ en $\mathbb{Q}[x]$ es igual al máximo común divisor de $f(x)$ y $g(x)$ en $\mathbb{R}[x]$.

13.4.3. Sean $f(x)$ y $g(x)$ polinomios en $K[x]$ tales que

$$f(x) \cdot a(x) + g(x) \cdot b(x) = d(x),$$

donde $d(x)$ es el máximo común divisor de $f(x)$ y $g(x)$. ¿Cuál es el máximo común divisor de $a(x)$ y $b(x)$?

13.4.4. Sean $a(x)$, $b(x)$ y $c(x)$ polinomios en $K[x]$, con $a(x) \neq 0$, $b(x) \neq 0$ y $a(x)$ mónico. Muestre que

$$(a(x) \cdot b(x), a(x) \cdot c(x)) = a(x) \cdot (b(x), c(x)).$$

13.4.5. Demuestre el teorema 13.4.9.

13.4.6. Sean $a(x)$ y $b(x)$ polinomios en $K[x]$, no ambos cero, con máximo común divisor $d(x) = (a(x), b(x))$. Para $c(x) \in K[x]$, demuestre que existen polinomios $f(x), g(x) \in K[x]$ que satisfacen la ecuación $a(x)f(x) + b(x)g(x) = c(x)$ si y sólo si $d(x) \mid c(x)$.

13.4.7. Sean $f(x), g(x), h(x) \in K[x]$ con $(f(x), g(x)) = 1$. Demuestre que si $f(x) \mid h(x)$ y $g(x) \mid h(x)$, entonces $f(x) \cdot g(x) \mid h(x)$.

13.4.8. Sean $f(x), g_1(x), \ldots, g_r(x)$ polinomios en $K[x]$ tales que $(f(x), g_i(x)) = 1$ para toda $i = 1, \ldots, r$. Demuestre que

$$(f(x), g_1(x) \cdot \cdots \cdot g_r(x)) = 1.$$

13.4.9. Encuentre el máximo común divisor en $\mathbb{Q}[x]$ de las siguientes parejas de polinomios $f(x)$ y $g(x)$ y escríbalo como combinación lineal de la pareja de polinomios.

(1) $f(x) = x^4 - x^3 + 3x^2 - 2x + 2$, $g(x) = x^3 + x^2 + 2x + 2$;
(2) $f(x) = -x^4 + 3x^3 - 4x^2 + 12x$, $g(x) = x^3 - 4x^2 + 4x - 3$;
(3) $f(x) = x^4 + 5x^3 - 4x^2 - 2x$, $g(x) = -3x^4 - x^3 + 4x^2$;
(4) $f(x) = x^6 - 5x^5 + 2x^4 - 3x^3 + x^2 - 2x + 2$, $g(x) = x^5 - x^3 + x^2 + 1$;
(5) $f(x) = x^6 - 4x^4 + 2x^3 + 4x^2 - 4x + 1$, $g(x) = 2x^3 + 5x^2 + x - 3$;
(6) $f(x) = 2x^6 + 4x^5 + 3x^4 + 2x^3 - 5x^2 - 12x - 6$, $g(x) = x^4 - 2x^3 + 3x^2 - 4x + 2$;
(7) $f(x) = x^5 + x^4 - 3x^3 + 4x^2 + 2x$, $g(x) = x^4 + 3x^3 - x^2 - 6x - 2$.

13.4.10. Encuentre el máximo común divisor de $f(x)$ y $g(x)$:

(1) $f(x) = 2x^4 + 10x^3 + 2\sqrt{2}x^2 + 10\sqrt{2}x$, $g(x) = x^4 + 2x^3 + (\sqrt{2}+1)x^2 + 2\sqrt{2}x + \sqrt{2}$, en $\mathbb{R}[x]$;
(2) $f(x) = x^4 - 4ix + 3$, $g(x) = x^3 - i$, en $\mathbb{C}[x]$;
(3) $f(x) = x^2 - x + 4$, $g(x) = x^3 + 2x^2 + 3x + 2$, en $\mathbb{Z}_3[x]$.

13.4.11. Sean $f(x), g_1(x), \ldots, g_r(x) \in K[x]$ mónicos irreducibles. Demuestre que si $f(x) \mid g_1(x) \cdots g_r(x)$, entonces $f(x) = g_i(x)$ para alguna $i \in \{1, \ldots, r\}$.

13.4.12. Determinar la constante c si el máximo común divisor de $f(x)$ y $g(x)$ sobre el campo de los números racionales es un polinomio de grado 1. Para cada valor de c obtenido, ¿cuál es el máximo común divisor?
(1) $f(x) = x^3 + cx^2 - x + 2c$, $g(x) = x^2 + cx - 2$;
(2) $f(x) = x^2 + (c-6)x + 2c - 1$, $g(x) = x^2 + (c+2)x + 2c$.

13.4.13. Sean $f(x), g(x) \in \mathbb{R}[x]$ con $f(x) = x^3 + 2x^2 + ax - b$ y $g(x) = x^3 + 2x^2 - bx + a$. Determine los valores de a y b de modo que el máximo común divisor de $f(x)$ y $g(x)$ sea un polinomio de grado 2.

13.4.14. El **mínimo común múltiplo** de dos polinomios distintos de cero $a(x)$ y $b(x)$ en $K[x]$ es un polinomio $m(x)$ en $K[x]$ que satisface:

(a) $m(x)$ es mónico;
(b) $a(x) \mid m(x)$ y $b(x) \mid m(x)$;
(c) Si $m'(x) \in K[x]$ cumple que $a(x) \mid m'(x)$ y $b(x) \mid m'(x)$, entonces $m(x) \mid m'(x)$.

Demuestre que

(1) $m(x)$ es único. Denotaremos a $m(x)$ por $[a(x), b(x)]$.
(2) Si $a(x)$ y $b(x)$ son polinomios mónicos, entonces

$$[a(x), b(x)] \cdot (a(x), b(x)) = a(x) \cdot b(x).$$

13.4.15. Para cada inciso del ejercicio 4.10, encuentre el mínimo común múltiplo de los polinomios $f(x)$ y $g(x)$.

§§ Ejercicios sección 13.5.

13.5.1. Demuestre el lema 13.5.3

13.5.2. Sea $p(x)$ un polinomio distinto de cero en $K[x]$. Demuestre que $p(x)$ es irreducible en $K[x]$ si y sólo si sus únicos divisores son los elementos distintos de cero en K y los polinomios de la forma $a \cdot p(x)$ para cada $a \in K - \{0\}$.

13.5.3. Demuestre el corolario 13.5.6

13.5.4. Demuestre que si $p(x)$ es un polinomio irreducible y $p(x) \mid f_1(x) \cdot \ldots \cdot f_r(x)$, entonces $p(x) \mid f_i(x)$ para alguna $i = 1, \ldots, r$.

13.5.5. Sea $p(x) \in K[x]$. Demuestre que $p(x)$ es irreducible si y sólo si, para cada $f(x), g(x) \in K[x]$, $p(x) \mid f(x) \cdot g(x)$ implica que $p(x) \mid f(x)$ o $p(x) \mid g(x)$.

13.5.6. Demuestre que cada polinomio de grado 1 en $K[x]$ es irreducible

13.5.7. Demuestre que, si $g(x)$ y $h_1(x), \ldots, h_r(x)$ son mónicos e irreducibles en $K[x]$ y cumplen que $g(x) \mid h_1(x) \cdot \ldots \cdot h_r(x)$, entonces $g(x) = h_i(x)$ para alguna $i = 1, \ldots, r$.

13.5.8. Demuestre que todo polinomio de grado 1 en $K[x]$ es irreducible.

13.5.9. Demuestre que si $p(x)$ es irreducible en $K[x]$, entonces $ap(x)$ es irreducible en $K[x]$, para todo $a \in K - \{0\}$.

13.5.10. Sean $f(x), g(x) \in K[x]$, no nulos, y $\partial g(x) < \partial f(x)$. Si $f(x)$ es irreducible en $K[x]$, ¿por qué esto implica que 1 es el m.c.d de $f(x)$ y $g(x)$?

13.5.11. Sea $f(x) = a \cdot p_1(x)^{k_1} p_2(x)^{k_2} \cdots p_n(x)^{k_n}$ un polinomio en $K[x]$, donde los $p_i(x)$ son irreducibles mónicos en $K[x]$ y $a \in K - \{0\}$, $p_i(x) \neq p_j(x)$ para $i \neq j$, y los exponentes k_i son números naturales. Demuestre que $g(x) \in K[x]$ divide a $f(x)$ si y sólo si $g(x) = a \cdot p_1(x)^{r_1} p_2(x)^{k_2} \cdots p_n(x)^{r_n}$, donde $b \in K - \{0\}$ y $0 \leq r_i \leq k_i$ para $i = 1, \ldots, n$.

13.5.12. Sean $f(x), g(x) \in K[x]$. Si

$$f(x) = a \cdot p_1(x)^{k_1} p_2(x)^{k_2} \cdots p_n(x)^{k_n}$$

y

$$g(x) = b \cdot p_1(x)^{r_1} p_2(x)^{r_2} \ldots p_n(x)^{r_n},$$

donde $a, b \in K - \{0\}$, los $p_i(x)$ son irreducibles mónicos en $K[x]$ distintos entre sí, y los exponentes k_i y r_i son números naturales.

(1) Demuestre que el m.c.d de $f(x)$ y $g(x)$ es

$$(f(x), g(x)) = p_1(x)^{t_1} p_2(x)^{t_2} \cdots p_n(x)^{t_n},$$

donde $t_i = \min\{k_i, r_i\}$.

(2) Demuestre que el m.c.m de $f(x)$ y $g(x)$ es

$$[f(x), g(x)] = p_1(x)^{\ell_1} p_2(x)^{\ell_2} \cdots p_n(x)^{\ell_n},$$

donde $\ell_i = \max\{k_i, r_i\}$.

13.5.13. Sea K un campo.

(1) Si K es infinito, pruebe que hay una infinidad de polinomios irreducibles en $K[x]$.
(2) Si K es finito, demuéstrese que $K[x]$ contiene polinomios irreducibles de grado arbitrariamente alto. (Sugerencia: Trátese de imitar la demostración de Euclides de que existe una infinidad de números primos.)

13.5.14. Muestre que en $\mathbb{Q}[x]$ los polinomios $f(x) = x^2 - p$, con $p \in \mathbb{Z}$ primo, son irreducibles.

13.5.15. Hacer una lista de los polinomios mónicos de segundo grado sobre $\mathbb{Z}_3$. ¿Cuáles son irreducibles? Encontrar la descomposición de los polinomios reducibles.

13.5.16. El polinomio $x^4 + 4$ puede descomponerse en factores lineales en $\mathbb{Z}_5[x]$. Encuéntrese esta descomposición.

§§ Ejercicios sección 13.6.

13.6.1. Encuentre la derivada de los siguientes polinomios:

(1) $f(x) = 5x^5 + \frac{1}{2}x^4 + \frac{2}{3}x^2 - x + 6$ en $\mathbb{Q}[x]$
(2) $f(x) = (x+1)^2(x-2)$ en $\mathbb{Q}[x]$
(3) $f(x) = x^{2n+1} - (2n+1)x^n - 1$ en $\mathbb{Q}[x]$, con $n \geq 1$
(4) $f(x) = (x - \sqrt{2})^2 - (x-1)^3$ en $\mathbb{R}[x]$
(5) $f(x) = ix\left(3x^2 - (5+i)x - i\right)^2$ en $\mathbb{C}[x]$
(6) $f(x) = x^3 + x + 1$ en $\mathbb{Z}_3[x]$

13.6.2. Demuestre que la derivada de $f(g(x))$ es $f'(g(x)) \cdot g'(x)$.

13.6.3. Sea $f(x) \in K[x]$, donde $K = \mathbb{Q}, \mathbb{R}$ o $\mathbb{C}$.

(1) Demuestre que si $\partial f(x) > 0$, entonces $f'(x) \neq 0$ y $\partial f'(x) = (\partial f(x)) - 1$.
(2) Probar que $f'(x) = 0$ si y sólo si $f(x)$ es una constante.

13.6.4. Sea $p(x) \in K[x]$ un polinomio irreducible, donde $K = \mathbb{Q}, \mathbb{R}$ o $\mathbb{C}$. Demuestre que $(p(x), p'(x)) = 1$.

13.6.5. Considere $f(x) = a \cdot p_1(x)^{m_1} \cdot \ldots \cdot p_k(x)^{m_k}$ en $K[x]$, donde $a \in K$; $p_1(x), \ldots, p_k(x)$ son polinomios no contantes en $K[x]$ y $m_1, \ldots, m_k$ son números naturales. Demuestre que

$$f'(x) = \sum_{j=1}^{k} \frac{f(x)}{p_j(x)} \cdot m_j \cdot p_j'(x)$$

13.6.6. Sea $K = \mathbb{Q}, \mathbb{R}$ o $\mathbb{C}$. Considere $f(x) = a \cdot p_1(x)^{m_1} \cdot \ldots \cdot p_r(x)^{m_r}$ en $K[x]$, donde

(1) $r \geq 1$ y $a \in K - \{0\}$;
(2) $p_1(x), \ldots, p_r(x)$ son polinomios mónicos, irreducibles y distintos entre sí en $K[x]$; y
(3) $m_1 \geq 1, \ldots, m_r \geq 1$.

Demuestre que

$$\big(f(x), f'(x)\big) = p_1(x)^{m_1-1} \cdot \ldots \cdot p_r(x)^{m_r-1}.$$

§ § Ejercicios sección 13.7.

13.7.1. Demostrar

(1) Si $f(x) = g(x) + h(x)$ en $K[x]$ y $\alpha \in K$, entonces $f(\alpha) = g(\alpha) + h(\alpha)$.
(2) Si $f(x) = g(x) \cdot h(x)$, entonces $f(\alpha) = g(\alpha) \cdot h(\alpha)$.

Definición 13.7.2*. Sea α una raíz de multiplicidad $m \geq 1$ de $f(x) \in K[x]$. Si $m = 1$, diremos que α es una raíz* ***simple****. Si $m > 1$, diremos que α es una raíz* ***múltiple****.*

13.7.3. Sean $f(x), g(x), h(x) \in K[x]$, y sea $\alpha \in K$. Demostrar que

(1) Si $f(x) = g(x) + h(x)$, entonces $f(\alpha) = g(\alpha) + h(\alpha)$.
(2) Si $f(x) = g(x) \cdot h(x)$, entonces $f(\alpha) = g(\alpha) \cdot h(\alpha)$.

13.7.4. Sea $f(x) = (x+2)^2 \left(x^2 - 2x - 2\right) \left(x^3 - 1\right)$.

(1) Considerando $f(x) \in \mathbb{Q}[x]$, ¿cuántas raíces tiene en $\mathbb{Q}$?;
(2) Considerando $f(x) \in \mathbb{R}[x]$, ¿cuántas raíces tiene en $\mathbb{R}$?;
(3) Considerando $f(x) \in \mathbb{C}[x]$, ¿cuántas raíces tiene en $\mathbb{C}$?.

13.7.5. Sea $f(x) = g(x) \cdot h(x)$ en $K[x]$, y sean $\alpha \in K$. Demuestre que α es raíz de $f(x)$ si y sólo si α es raíz de $g(x)$ o α es raíz de $h(x)$.

13.7.6. Si $f(x) \mid g(x)$ en $K[x]$, demuestre que toda raíz de $f(x)$ es raíz de $g(x)$.

13.7.7. Sea $f(x) \in K[x]$; y sean $a, b \in K$, con $b \neq 0$. Demuestre que a es raíz de $f(x)$ si y sólo si a es raíz de $b \cdot f(x)$.

13.7.8. Si $f(x) \in K[x]$ y $\alpha \in K$, demuestre que $(x - \alpha) \mid (f(x) - f(\alpha))$.

13.7.9. El polinomio $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ tiene las raíces $\alpha_1, \ldots, \alpha_n$. ¿Qué raíces tiene el polinomio

$$a_n x^n + a_{n-1} b x^{n-1} + a_{n-2} b^2 x^{n-2} + \ldots + a_1 x + a_0 b^n?$$

13. 7.10. Demuestre que si α es una raíz de $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, entonces $a_n\alpha$ es raíz del polinomio mónico

$$x^n + a_{n-1}x^{n-1} + a_n a_{n-2}x^{n-2} + \ldots + a_n^{n-2}a_1 x + a_n^{n-1}a_0.$$

13.7.11. Si K es un campo y $\alpha \neq 0$ es una raíz de de $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ en $K[x]$, demuestre que α^{-1} es raíz de $a_n + a_{n-1}x + \ldots + a_0 x^n$.

13.7.12. Sea $f(x) \in K[x]$ un polinomio de grado 3 cuyas raíces son $\alpha_1, \alpha_2, \alpha_3$ son elementos de K. Describa el polinomio $f(x)$ dando explícitamente sus coeficientes.

13. 7.13. Sean $f(x)$ y $g(x)$ polinomios en $\mathbb{Q}[x]$ tales que $f(x)$ es irreducible en $\mathbb{Q}[x]$ y $g(x) \neq 0$. Si existe $\alpha \in \mathbb{R}$ tal que $f(\alpha) = g(\alpha) = 0$, es decir, $f(x)$ y $g(x)$ tienen una raíz en común en $\mathbb{R}$, demuestre que $f(x) \mid g(x)$ en $\mathbb{Q}[x]$.

13.7.14.

(*a*) Dé un ejemplo de un polinomio $f(x)$ en $\mathbb{R}[x]$ tal que $\partial f(x) = 6$, sea reducible en $\mathbb{R}[x]$, pero que no tenga raíces reales.
(*b*) Sea $f(x) \in K[x]$ con grado 2 ó 3. Demuestre que $f(x)$ es irreducible en $K[x]$ si y sólo si $f(x)$ no tiene raíces en $K[x]$.

13. 7.15. Tomamos $K = \mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$. Sean $f(x) \in K[x]$ y $\alpha \in K$. Si el polinomio $f(x) = \sum_{r=0}^{n} a_r(x-\alpha)^r$, con $a_r \in K$, demuestre que los coeficientes a_r son

$$a_r = \frac{f^{(r)}(\alpha)}{r!}.$$

13.7.16. ¿Cuál es el residuo que deja:

(1) $\frac{1}{9}x^4 + \frac{1}{3}x^2 - \frac{1}{6}x - 2$ al ser dividido por $x + 3$ en $\mathbb{Q}[x]$;
(2) $x^6 - 4x^4 + x^2 - 1$ al ser dividido por $x - \sqrt{2}$ en $\mathbb{R}[x]$;
(3) $x^{15} - 4x^8 + 5x^3 - 2ix + 2$ al ser dividido por $x + i$ en $\mathbb{C}[x]$;
(4) $\pi x^4 - ex^2 + i$ al ser dividido por $x + 1$ en $\mathbb{C}[x]$?

13. 7.17. Hallar los valores de a tales que a es el residuo cuando el polinomio $x^3 - ax^2 - 14x + 15a$ es dividido por $x - 5$.

13. 7.18. Hallar los valores de b tales que b^2 es el residuo cuando el polinomio $2x^3 - x^2 + (b + 1)x + 10$ es dividido por $x + 1$.

13.7.19. Hallar a y b para que el polinomio $x^5 - ax + b$ sea divisible por $x^2 - 4$.

13.7.20. Considere el polinomio $f(x) = x^3 - 4x^2 + ax - 3$ en $\mathbb{Q}[x]$. Si al dividir $f(x)$ entre $x + 1$ su residuo es -12, ¿cuál debe ser el valor de a?

13.7.21. Calcular el valor de a para que el polinomio $x^3 - ax + 8 \in \mathbb{R}[x]$ tenga la raíz $\alpha = -2$, y calcular las otras raíces.

13.7.22. Encuentra el polinomio $f(x) \in \mathbb{R}[x]$ de grado 2 para el que $f(0) = 1$, $f(2) = 1$ y $f(-3) = 0$.

13.7.23. ¿Existe un polinomio no cero $f(x) = ax^2 + bx + c$ en $\mathbb{R}[x]$ tal que $f(0) = f(1) = f(-1) = 0$?

13.7.24. Demuestre que si un polinomio tiene una infinidad de raíces, entonces es el polinomio 0.

13.7.25. Recuerde que, en general, dos polinomios $f(x), g(x) \in K[x]$ son iguales si y sólo si sus coeficientes correspondientes son iguales.

(1) Sean $f(x) = a_2x^2+a_1x+a_0$ y $g(x) = b_2x^2+b_1x+b_0$ dos polinomios cuadráticos en $\mathbb{C}[x]$. Suponga que para todo $\alpha \in \mathbb{C}$ se tiene que $f(\alpha) = g(\alpha)$. Demuestre que $f(x) = g(x)$.
(2) En general, si $f(x), g(x) \in \mathbb{C}[x]$ son tales que para todo $\alpha \in \mathbb{C}$ se tiene que $f(\alpha) = g(\alpha)$, demuestre que $f(x) = g(x)$.
(3) Lo anterior, no es cierto en todos los campos. Encuentre dos polinomios $f(x), g(x) \in \mathbb{Z}_2[x]$ tales que para todo $\alpha \in \mathbb{Z}_2$ se tiene que $f(\alpha) = g(\alpha)$, pero $f(x) \neq g(x)$.

13.7.26. Sea $n \in \mathbb{N}$; sean $f(x)$ y $g(x)$ polinomios en $K[x]$, distintos de cero, con $\partial f(x) \leq n$ y $\partial g(x) \leq n$; y sean $\alpha_1, \alpha_2, \ldots, \alpha_{n+1}$ en K con $\alpha_i \neq \alpha_j$ para $i \neq j$. Demuestre que si $f(\alpha_i) = g(\alpha_i)$ para $i = 1, \ldots, n + 1$, entonces $f(x) = g(x)$.

13.7.27. Sean $f_1(x)$, $f_2(x) \in K[x]$. Supongamos que α es una raíz de multiplicidad m_1 en $f_1(x)$ y de multiplicidad m_2 en $f_2(x)$.

(1) Demuestre que para cualesquiera $g_1(x), g_2(x) \in K[x]$, α es una raíz de multiplicidad mayor o igual que mín$\{m_1, m_2\}$ en el polinomio $f_1(x)g_1(x) + f_2(x)g_2(x)$.
(2) Demuestre que α también es raíz del polinomio $f_1(x)+ f_2(x)$ y su multiplicidad es mín$\{m_1, m_2\}$.

13.7.28. Sea $f(x) = g(x)h(x)$ en $K[x]$ y $\alpha \in K$. Supóngase que α es una raíz de $g(x)$ y $h(x)$, con multiplicidades m_1 y m_2, respectivamente. Demuestre que α es una raíz de multiplicidad $m_1 + m_2$ de $f(x)$.

13.7.29. Sean $f(x), h(x) \in K[x]$, y sea $\alpha \in K$. Si α es una raíz de $f(x)$ y $h(x)$, con multiplicidades m_1 y m_2, respectivamente, demuestre que α es una raíz de multiplicidad mín $\{m_1, m_2\}$ de $(f(x), g(x))$.

13.7.30. Sean $f_1(x), f_2(x) \in K[x]$. Demostrar que si α es una raíz de multiplicidad $m \geq 1$ del polinomio $f_1(x)f_2'(x) - f_2(x)f_1'(x)$, entonces α es una raíz de multiplicidad $m+1$ del polinomio $f_1(x)f_2(\alpha) - f_2(x)f_1(\alpha)$.

13.7.31. Sea $f(x) \in K[x]$. Demuestre que si $(f(x), f'(x)) = 1$, entonces $f(x)$ no tiene raíces múltiples en K.

13.7.32. Sean $\alpha_1, \alpha_2, \ldots, \alpha_n$ en K, y sea $f(x) = (x-\alpha_1)\cdot\ldots\cdot(x-\alpha_n)$ en $K[x]$. Demuestre que $(f(x), f'(x)) = 1$ si y sólo si $\alpha_i \neq \alpha_j$, para todo $i \neq j$.

13.7.33. Determine la multiplicidad de la raíz $\alpha = 1$ en cada uno de los siguientes polinomios con coeficientes en $\mathbb{C}$:

(1) $f(x) = x^4 - 2x^3 + 2x^2 - 2x + 1$;
(2) $g(x) = x^4 - (2-2i)x^3 - 4ix^2 + (2+2i)x - 1$;
(3) $h(x) = x^5 - 3x^4 + 5x^3 - 4x^2 + 3x - 2$;
(4) $p(x) = x^5 - 3x^4 + \left(3 + \sqrt{2}\right)x^3 - \left(1 + 3\sqrt{2}\right)x^2 + 3\sqrt{2}x - \sqrt{2}$;
(5) $q(x) = x^{2n} - nx^{n+1} + nx^{n-1} - 1$, con $n \geq 4$;
(6) $r(x) = x^{2n+1} - (2n+1)x^{n+1} + (2n+1)x^n - 1$, con $n \geq 3$.

13.7.34. Determine la multiplicidad de la raíz $\alpha = 1$ en cada uno de los siguientes polinomios con coeficientes en $\mathbb{C}$:

(1) $f(x) = x^4 - 2x^3 + 2x^2 - 2x + 1$;
(2) $g(x) = x^4 - (2-2i)x^3 - 4ix^2 + (2+2i)x - 1$;
(3) $h(x) = x^5 - 3x^4 + 5x^3 - 4x^2 + 3x - 2$;
(4) $p(x) = x^5 - 3x^4 + \left(3 + \sqrt{2}\right)x^3 - \left(1 + 3\sqrt{2}\right)x^2 + 3\sqrt{2}x - \sqrt{2}$;
(5) $q(x) = x^{2n} - nx^{n+1} + nx^{n-1} - 1$, con $n \geq 4$;
(6) $r(x) = x^{2n+1} - (2n+1)x^{n+1} + (2n+1)x^n - 1$, con $n \geq 3$.

13.7.35. El polinomio $f(x) = x^n - nx + n - 1 \in \mathbb{C}[x]$, con $n \geq 2$, tiene como raíz a $\alpha = 1$.

(1) Muestre que α es una raíz de multiplicidad 2 de $f(x)$.
(2) ¿Puede alguna otra raíz de $f(x)$ ser una raíz múltiple?

13.7.36. El polinomio $f(x) = x^5 - 3\sqrt{2}x^4 + 4x^3 + 4\sqrt{2}x^2 - 12x + 4\sqrt{2}$ en $\mathbb{R}[x]$ tiene una raíz cuádruple en $\mathbb{R}$. ¿Cuál es?

13.7.37. Considere el polinomio $f(x) = x^5 - ax^2 - ax + 1$ en $\mathbb{R}[x]$. Determinar el número a de tal modo que $\alpha = -1$ sea una raíz de multiplicidad mayor que 2.

13.7.38. Sea $f(x) = ax^{n+1} + bx^n + 1 \in \mathbb{Q}[x]$. Determine a y b de tal modo que $\alpha = 1$ sea una raíz de multiplicidad mayor que 2.

13.7.39. Demuestre que los siguientes polinomios no tienen raíces múltiples en $\mathbb{R}$.

(1) $f(x) = x^5 + 5x + 1$;
(2) $g(x) = x^7 + x^3 + 1$.
(3) $h(x) = x^{2n+1} + ax + b$; $a, b \in \mathbb{R}$ con $a > 0$.

13.7.40. Demostrar que el polinomio

$$1 + \frac{x}{1} + \frac{x^2}{1 \cdot 2} + \ldots + \frac{x^n}{n!} \quad \text{en } \mathbb{R}[x]$$

no tiene raíces múltiples.

§ § Ejercicios sección 13.8.

13.8.1. Demuestre que las dos afirmaciones siguientes son equivalentes:

(1) Todo $f(x) \in \mathbb{C}[x]$ no constante tiene *todas* sus raíces en $\mathbb{C}$.
(2) Todo $f(x) \in \mathbb{C}[x]$ no constante tiene *alguna* de sus raíces en $\mathbb{C}$.

13.8.2. Construir un polinomio en $\mathbb{C}[x]$ de grado mínimo que tenga:

(1) la raíz doble 1 y las raíces simples 2, 3 y $1 + i$.
(2) la raíz triple -1 y las raíces simples 2, 3 y $1 + i$.
(3) la raíz doble i y las raíz simple $-1 - i$.

13.8.3. Si $f(x) \in \mathbb{C}[x]$, donde $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, entonces definimos $\overline{f}(x) = \overline{a_0} + \overline{a_1} x + \cdots + \overline{a_n} x^n$. Sean $f(x), g(x), h(x) \in \mathbb{C}[x]$. Demuestre que

(1) Si $h(x) = f(x) + g(x)$, entonces $\overline{h}(x) = \overline{f}(x) + \overline{g}(x)$.
(2) Si $h(x) = f(x) \cdot g(x)$, entonces $\overline{h}(x) = \overline{f}(x) \cdot \overline{g}(x)$.
(3) $f(x) \mid g(x)$ si y sólo si $\overline{f}(x) \mid \overline{g}(x)$.
(4) $f(x) \in \mathbb{R}[x]$ si y sólo si $\overline{f}(x) = f(x)$.

13.8.4. Sea

$$p(x) = x^6 + (-3 - 2i)x^5 + (-2 + 6i)x^4 + (14 + 4i)x^3 + (-3 - 28i)x^2 + (-15 + 6i)x + a.$$

Determina $a \in \mathbb{C}$ de modo que $2i$ sea raíz de $p(x)$ y descomponga este polinomio en factores de primer grado en $\mathbb{C}[x]$ si sabemos que $\left(x - \sqrt{3}\right)$ es uno de sus factores.

13.8.5. Construir un polinomio en $\mathbb{R}[x]$ de grado mínimo que tenga:

(1) la raíz doble 1 y las raíces simples 2, 3 y $1 + i$.
(2) la raíz triple $2 - 3i$.
(3) la raíz doble i y las raíz simple $-1 - i$.

13.8.6. Sea $p(x) = x^4 - 4x^3 + 3x^2 + 11x + 26$. Si $3 + 2i$ es raíz de $p(x)$, descomponga a $p(x)$ como producto de polinomios irreducibles en $\mathbb{R}[x]$.

13.8.7. El polinomio $f(x) = x^4 + 6x^3 + 13x^2 + 12x + 4$ tiene dos raíces dobles. Encuentre estas raíces y descomponga este polinomio en factores de primer grado en $\mathbb{C}[x]$.

13.8.8. Encontrar todas las raíces de los siguientes polinomios usando los datos que se proporcionan.

(1) $x^3 + 6x^2 - 24x + 160$ si una de las raíces es $2 - 2\sqrt{3}i$.
(2) $x^5 - 2x^4 + 2x^3 - 4x^2 + x - 2$ si $-i$ es una raíz.
(3) $x^5 - 3x^4 + 4x^3 - 4x + 4$ si $1 + i$ es una raíz doble.
(4) $2x^4 - 5\sqrt{3}x^3 + 9x^2 + 3\sqrt{3}x - 9$ tiene una raíz de multiplicidad 3.
(5) $x^5 + (2 - 3i)x^4 - (2 + 6i)x^3 - (6 + 2i)x^2 - (3 - 2i)x + i$ si i es una raíz.
(6) $x^6 - x^5 - 8x^4 + 2x^3 + 21x^2 - 9x - 54$ si $\sqrt{2} + i$ es una raíz.

13.8.9. Sea $f(x)$ un polinomio no constante en $\mathbb{C}[x]$. Demuestre que $f(x)$ es divisible por su derivada si y sólo si $f(x) = a(x - \beta)^n$, con $a, \beta \in \mathbb{C}$ y $n \geq 1$.

13.8.10. Sea $f(x)$ un polinomio mónico irreducible en $\mathbb{R}[x]$ con $\partial f(x) = 2$. Demuestre que existen números reales a y $b \neq 0$ tales que $f(x) = (x - a)^2 + b^2$. Inversamente, demuestre que cualquier polinomio de la forma $f(x) = (x - a)^2 + b^2$ con $a, b \in \mathbb{R}$, $b \neq 0$, es irreducible en $\mathbb{R}[x]$.

13.8.11. Encontrar la descomposición (como producto de polinomios irreducibles) de los siguientes polinomios sobre el campo de los números reales y sobre el campo de los números complejos:

(1) $x^3 + 1$ (2) $x^4 + 1$ (3) $x^4 - 5x^2 + 6$
(4) $x^5 - x$ (5) $x^6 + x$ (6) $x^8 - 3^8$

13.8.12. Sea $f(x) = ax^2 + bx + c$ un polinomio con coeficientes racionales, donde $a \neq 0$. Demuestre que $f(x)$ es irreducible si y sólo si $b^2 - 4ac$ no es el cuadrado de un número racional.

13.8.13. Determine cuáles de los siguientes polinomios son irreducibles en $\mathbb{Q}[x]$.

(1) $x^2 - 3$ (2) $x^3 - 2$ (3) $x^3 + 2x^2 + 2x + 1$
(4) $x^4 + 1$ (5) $x^4 - x^2 - 1$ (6) $x^2 - 2x + 4$
(7) $x^6 + 2x^3 + 1$ (8) $x^4 + 4$

13.8.14. Si $\alpha \in \mathbb{Q}$ es una raíz de algún polinomio mónico en $\mathbb{Z}[x]$, pruebe que $\alpha \in \mathbb{Z}$.

13.8.15. ¿Para cuántos enteros n tales que $1 \leq n \leq 1000$, podemos descomponer $f(x) = x^2 + x - n$ como producto de dos polinomios de primer grado en $\mathbb{Z}[x]$?

13.8.16. Sea $f(x) \in \mathbb{Z}[x]$ y sea $\frac{r}{s} \in \mathbb{Q}$ una raíz de $f(x)$ con $(r, s) = 1$. Demuestre que $r - ms$ es un divisor de $f(m)$ para cualquier entero m. (Sugerencia: Escriba $f(x)$ en la forma $\sum a_r(x-m)^r$. Demuestre que cada a_r es un entero. Luego, evalúe $f(x)$ en $\frac{r}{s}$)

13.8.17. Sea $f(x) \in \mathbb{Z}[x]$. Demuestre que $f(x)$ no tiene raíces enteras, si $f(0)$ y $f(1)$ son números impares.

13.8.18. Encuentre las raíces racionales, si existen, de los siguientes polinomios en $\mathbb{Q}[x]$.

(1) $2x^3 - 7x^2 + 10x - 6$;
(2) $x^3 - \frac{2}{3}x + 3x - 2$;
(3) $4x^3 - 12x + 10x - 4$;
(4) $x^3 - \frac{1}{4}x^2 - \frac{1}{4}x + \frac{1}{16}$;
(5) $24x^5 - +10x^4 - x^3 - 19x^2 - 5x + 6$;
(6) $2x^7 - 3x^5 - 2x^4 - x^3 + 7x - 2$;
(7) $x^8 + \frac{8}{3}x^7 + \frac{1}{3}x^6 - \frac{14}{3}x^5 - \frac{14}{3}x^4 - \frac{4}{3}x^3$.

13.8.19. Sea $K = \mathbb{Q}$ o $\mathbb{R}$. Si $p(x)$ es un polinomio irreducible de grado n en $K[x]$, pruebe que $p(x)$ tiene n raíces distintas en $\mathbb{C}$.

13.8.20. Sea $f(x) \in \mathbb{Q}[x]$, y suponga $a + b\sqrt{c}$ es una raíz de $f(x)$, donde $a, b, c \in \mathbb{Q}$ y $\sqrt{c} \notin \mathbb{Q}$. Completa los siguientes pasos para probar que $a - b\sqrt{c}$ es también una raíz de $f(x)$.

(*a*) Si $b = 0$ el resultado es cierto. ¿Por qué?

(*b*) Supóngase que $b \neq 0$. Sea $g(x) = \left[x - \left(a + b\sqrt{c}\right)\right]\left[x - \left(a - b\sqrt{c}\right)\right]$. Verifica que $g(x) = (x-a)^2 - b^2c$, es decir, $g(x) \in \mathbb{Q}[x]$.
(*c*) Por el algoritmo de la división en $\mathbb{Q}[x]$ existen $q(x), r(x) \in \mathbb{Q}[x]$ tales que

$$f(x) = g(x)q(x) + r(x), \text{ donde } r(x) = 0 \text{ o } \partial r(x) < \partial g(x).$$

Como $\partial g(x) = 2$, entonces $r(x) = 0$ o $\partial r(x) < 2$, por lo que $r(x) = dx + e$, con $d, e \in \mathbb{Q}$. Demuestre que $d = e = 0$, es decir, $r(x) = 0$.
(*d*) Utilizando el inciso (*c*) concluya que $a - b\sqrt{c}$ es raíz de $f(x)$.

13.8.21. Determine cuáles de las siguientes afirmaciones son verdaderas. Justifique su respuesta.
(1) Si $1 - i$ es raíz de $f(x) = x^2 - 2x + 1 + 2i$, entonces $1 + i$ es también una raíz.
(2) $x^4 - 2x^3 - 6x^2 + 4x + 8$ tiene raíces racionales.
(3) $x^{11} - \sqrt{3}x^4 + 2x + \sqrt{13}$ no tiene raíces reales.
(4) Si $p(x) \in \mathbb{R}[x]$ es irreducible en $\mathbb{R}[x]$, entonces es también irreducible en $\mathbb{C}[x]$.
(5) Si $f(x) \in \mathbb{R}[x]$ es irreducible en $\mathbb{C}[x]$, entonces es también irreducible en $\mathbb{R}[x]$.

§ § Ejercicios sección 13.9.

13.9.1. Encontrar las raíces de $f(x) = x^3 + 6x^2 - 6x - 58$.

13.9.2. Usando el teorema 13.9.2 encuentre las raíces de los siguientes polinomios.
(1) $x^3 + 6x^2 - 6x - 58$;
(2) $x^3 + 9x - 6$;
(3) $x^3 + 3x^2 + 9x + 14$;
(4) $3x^3 - 6x^2 - 2$;
(5) $x^3 + 9x - 2$;
(6) $x^3 - 3ix + (1 - i)$;
(7) $x^3 - 4ix^2 - 10x + 12i$;
(8) $8x^3 + 12x^2 + 102x - 47$.

13.9.3. Usando el teorema 13.9.4 encuentre las raíces de los siguientes polinomios.
(1) $x^4 - 4x^3 + 5x^2 - 2x - 6$;
(2) $x^4 + 2x^3 + 2x^2 + 10x + 25$;
(3) $x^4 + 4x - 1$;
(4) $x^4 + 2x^3 + 3x^2 + 2x - 3$;
(5) $x^4 - 8x^2 - 4x + 3$;
(6) $x^4 + 5x^3 - 10x^2 - 2x + 4$;
(7) $x^4 + 5x^2 + 2x + 8$;
(8) $x^4 + x^3 + 5x^2 + 5x + 12$;
(9) $x^4 - x^2 - 2ix + 6$.

§ § Ejercicios sección 13.10.

13.10.1. Encuentre la sucesión de Sturm de los siguientes polinomios.
(1) $x^3 - x + 1$

(2) $x^3 + 3x - 5$
(3) $x^4 - 3x^2 - 10x - 6$
(4) $x^4 - x - 1$
(5) $x^5 - 5x - 2$

13.10.2. Utilice el teorema de Sturm para localizar (entre enteros consecutivos) todas las raíces reales de los polinomios del ejercicio 5.

13.10.3. Para los polinomios siguientes, aproximar hasta las centésimas la raíz que se indica.

(1) La raíz de $f(x) = x^3 - 2x - 5$ que está entre 2 y 3.
(2) La raíz de $g(x) = x^5 - 4x - 2000$ que está entre 4 y 5.
(3) La raíz de $h(x) = x^3 - 17x^2 + 54x - 350$ que está entre 14 y 15.

13.10.4. Sea $f(x) = x^3 - 7x + 7$ en $\mathbb{R}[x]$.

(1) Encuentre la sucesión de Sturm de $f(x)$.
(2) Use el teorema de Sturm para determinar el número de raíces reales de $f(x)$ entre:
(a) -4 y -3; (b) -1 y 0; (c) 1 y 2.
(3) Aproximar hasta las centésimas la raíces de $f(x)$.

13.10.5. Sea $f(x) = x^4 - 2x^3 + x^2 - 2x + 1$ en $\mathbb{R}[x]$.

(1) Encuentre la sucesión de Sturm de $f(x)$.
(2) Use el teorema de Sturm para localizar (entre enteros consecutivos) todas las raíces reales de $f(x)$.
(3) Aproximar hasta las milésimas la raíces de $f(x)$.

13.10.6. Sea $f(x) = ax^2 + bx + c$, donde a, b y c son números reales, con $a \neq 0$.

(1) Encontrar la sucesión de Sturm del polinomio $f(x)$.
(2) Use el teorema de Sturm para probar que $f(x)$ tiene raíces reales si y sólo si $b^2 > 4ac$.

13.10.7. Sean p y q números reales, con $p \neq 0$, y sea $f(x) = x^3 + px + q$.

(a) Demuestre que la sucesión de Sturm del polinomio $f(x)$ es

$$x^3 + px + q, \quad 3x^2 + p, \quad -\left(\tfrac{2}{3}px + q\right), \quad -\left[\tfrac{27}{4}\left(\tfrac{q^2}{p^2}\right) + p\right].$$

(b) Use el teorema de Sturm para probar que:
(1) Si $27q^2 + 4p^3 < 0$, entonces $f(x)$ tiene 3 raíces reales.
(2) Si $27q^2 + 4p^3 > 0$, entonces $f(x)$ tiene 1 raíz real.

(3) Si $27q^2 + 4p^3 = 0$, entonces $f(x)$ tiene una raíz doble $(-\frac{3q}{2p})$ y otra raíz real.
(Sugerencia: Para el inciso (1) observe que $27q^2 + 4p^3 < 0$ implica que $p > 0$. Para el inciso (2) considere los casos $p < 0$ y $p > 0$ por separado.)

13. 10.8. Usando el ejercicio 10.7 determine el número de raíces reales de los siguientes polinomios.
(1) $x^3 + 2x - 1$; (2) $x^3 - \sqrt[3]{10}x - 1$; (3) $2x^3 - x + 1$.

13. 10.9. Sea $f(x) = x^5 - ax - b$, donde a y b son números reales positivos y $4^4a^5 > 5^5b^4$. Determine el número de raíces reales de $f(x)$.

13. 10.10. Sea n un entero par positivo, y sean p y q números reales con $p \neq 0$. Determinar el número de raíces reales de $f(x) = x^n + px + q$. (Sugerencia: Considere $\Delta = -(n-1)^{n-1}p^n - n^nq^{n-1}$; y analice los casos $\Delta > 0$ y $\Delta < 0$.)

Las matemáticas son el alfabeto con el cual Dios ha escrito el Universo.
Galileo Galilei
1564 - 1642

***Capítulo* 14**

Una introducción al algebra lineal

§ 14.1. Sistemas de ecuaciones lineales

Sea D un dominio entero. Una ***ecuación lineal en las*** n ***indeterminadas*** $x_1, \ldots, x_n$ con coeficientes ene D es una ecuación de la forma

$$a_1 x_1 + \cdots + a_n x_n = b,$$

donde $a_i, b \in D$ para $i = 1, \ldots, n$. En este capítulo estudiaremos sistemas de m ecuaciones en n indeterminadas con coeficientes en el campo $\mathbb{R}$ de los números reales y posteriormente presentaremos una generalización considerando cualquier campo K.

No siempre existe una solución simultánea a un sistema de ecuaciones lineales, ni siquiera cuando se trata de una sola ecuación como muestra de esto es claro que la ecuación $0x_1 + \cdots + 0x_n = b$, con $b \neq 0$ no puede tener ninguna solución, así que nuestra tarea inmediata consistirá en dar una condición necesaria y suficiente para que un sistema tenga solución, en cuyo caso se verá cómo encontrar no sólo una solución sino todas las soluciones del sistema.

Introduciremos además la teoría que se desarrollará a través de este estudio, la que resulta por demás interesante. Es importante mencionar que parte de los resultados que aquí se dan son válidos cuando consideramos un dominio entero en lugar de un campo. Por último cabe mencionar que sistemas de ecuaciones lineales

aparecen en muchos temas de la matemática, motivo por el cual es importante su estudio.

Consideramos el sistema de m ecuaciones lineales en n indeterminadas con coeficientes en $\mathbb{R}$

$$\text{(1)} \qquad \begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + \cdots + a_{2n}x_n = b_2 \\ \vdots \quad \vdots \quad \vdots \quad \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{cases}$$

donde, $a_{ij}, b_i \in \mathbb{R}$ para todo $i = 1, \ldots, m$ y $j = 1, \ldots, n$.
A los elementos $b_1, \ldots, b_m$ se les llama los términos independientes del sistema.

Definición 14.1.1. *Una* **solución** *del sistema (1) es un elemento*

$$(s_1, \ldots, s_n) \in \mathbb{R}^n = \underbrace{\mathbb{R} \times \cdots \times \mathbb{R}}_{n-veces}$$

que satisface cada una de las ecuaciones, es decir, para toda $i = 1, \ldots, m$

$$a_{i1}s_1 + \cdots + a_{in}s_n = b_i.$$

Observación 14.1.2. En los ejemplos concretos, si el coeficiente de una indeterminada x_i es cero, este sumando puede ser omitido sin que haya ninguna confusión, pues la ausencia de x_i en la ecuación significará precisamente eso, que su coeficiente es cero. Por ejemplo la ecuación en 4 indeterminadas $2x_1 + 0x_2 + 6x_3 - x_4 = -1$ puede ser escrita como

$$2x_1 + 6x_3 - x_4 = -1.$$

Cuando un sistema de ecuaciones no tiene solución diremos que el sistema es inconsistente. Si un sistema tiene solución no necesariamente es única y es por ese motivo que nos referiremos al ***conjunto de soluciones***. En cualquier caso este conjunto será vacío cuando es inconsistente y si es no vacío, podrá tener un único elemento o más de uno. Es más cuando el campo es infinito (como es nuestro caso al trabajar con $\mathbb{R}$) si la tercera posibilidad se da, el conjunto de soluciones será infinito.
Puede ser que distintos sistemas de ecuaciones en las mismas indeterminadas tengan al mismo conjunto de soluciones, aún cuando el número de ecuaciones de cada sistema sea diferente. Si tuviéramos un mecanismo para sustituir un sistema

de ecuaciones por otro más sencillo (por ejemplo que tenga más coeficientes cero) sin que cambie el conjunto de soluciones (incluyendo cuando el conjunto es vacío) se podría facilitar nuestro trabajo para encontrar dicha solución. Así pues éste es el camino que seguiremos.

Definición 14.1.3. *Dados dos sistemas de ecuaciones en n indeterminadas con coeficientes en* $\mathbb{R}$

$$(*)\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + \cdots + a_{2n}x_n = b_2 \\ \vdots \quad \vdots\vdots\vdots \quad \vdots \quad \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{cases} \quad y \ (**)\begin{cases} a'_{11}x_1 + \cdots + a'_{1n}x_n = b'_1 \\ a'_{21}x_1 + \cdots + a'_{2n}x_n = b'_2 \\ \vdots \quad \vdots\vdots\vdots \quad \vdots \quad \vdots \\ a'_{r1}x_1 + \cdots + a'_{rn}x_n = b'_r \end{cases}$$

diremos que los sistemas son equivalentes si el conjunto de soluciones de cada uno de ellos es el mismo.

Ejemplo 14.1.4. Los sistemas

$$\begin{cases} x_1 + x_2 + x_3 = -5 \\ 2x_3 = 2 \\ 3x_1 + 3x_2 + 3x_3 = -15 \end{cases} \text{ y } \begin{cases} x_3 = 1 \\ x_1 + x_2 + x_3 = -5 \end{cases}$$

son equivalentes.

Proposición 14.1.5. *La relación dada en la definición 14.1.3 entre sistemas de ecuaciones es de equivalencia.*

Veamos cómo podemos obtener un sistema de ecuaciones equivalente a uno dado de antemano.
Serán tres las "operaciones" que realizaremos sobre un sistema de ecuaciones lineales para obtener otro con el mismo conjunto de soluciones y son las siguientes.

(I) Intercambiar cualesquiera dos ecuaciones del sistema.
Es claro que el orden en que están dadas las ecuaciones de un sistema no modifica el conjunto de soluciones.

(II) Multiplicar una ecuación del sistema por un número $\alpha \neq 0$.
Si $\alpha \in \mathbb{R} - \{0\}$ y $(s_1, \ldots, s_n) \in \mathbb{R}^n$, $(s_1, \ldots, s_n)$ es una solución de

$$a_{i1}x_1 + \cdots + a_{in}x_n = b_i$$

si y sólo si es solución de

$$\alpha a_{i1}x_1 + \cdots + \alpha a_{in}x_n = \alpha b_i.$$

Como las restantes ecuaciones permanecen iguales esta "operación" no altera el conjunto de soluciones.

(III) Sumar a una ecuación otra ecuación del mismo sistema de ecuaciones lineales y sólo sustituir la ecuación i por la ecuación

$$(a_{i1} + a_{k1})x_1 + \cdots + (a_{in} + a_{kn})x_n = b_i + b_k$$

dejando las restante ecuaciones iguales, el sistema resultante tendrá el mismo conjunto de soluciones que el original ya que si $(s_1, \ldots, s_n)$ es una solución del sistema inicial, entonces $a_{i1}s_1 + \cdots + a_{in}s_n = b_i$ y $a_{k1}s_1 + \cdots + a_{kn}s_n = b_k$ y sumando estas dos igualdades obtenemos que

$$(a_{i1} + a_{k1})x_1 + \cdots + (a_{in} + a_{kn})x_n = b_i + b_k$$

y en las restantes ecuaciones no hay problema pues las ecuaciones son las mismas. Inversamente si $(s_1, \ldots, s_n)$ es una solución del nuevo sistema, entonces

$$(a_{i1} + a_{k1})s_1 + \cdots + (a_{in} + b_{kn})s_n = b_i + b_k$$

y

$$a_{k1}s_1 + \cdots + a_{kn}s_n = b_k$$

y restando estas dos igualdades obtenemos $a_{i1}s_1 + \cdots + a_{in}s_n = b_i$ y dejando todas las demás igual llegamos a que $(s_1, \ldots, s_n)$ es solución del sistema original.

Teorema 14.1.6*. Si en el sistema de ecuaciones lineales*

$$\left\{\begin{array}{rcccl} a_{11}x_1 + & \cdots & + a_{1n}x_n & = & b_1 \\ a_{21}x_1 + & \cdots & + a_{2n}x_n & = & b_2 \\ \vdots & \vdots\vdots\vdots & \vdots & & \vdots \\ a_{m1}x_1 + & \cdots & + a_{mn}x_n & = & b_m \end{array}\right.$$

se realiza cualquiera de las tres "operaciones" (I), (II) o (III) el sistema de ecuaciones que resulta es equivalente al original.

Corolario 14.1.7*. Si un sistema de ecuaciones lineales se obtiene de otro aplicando un número finito de "operaciones" del tipo (I), (II) o (III), entonces los dos sistemas son equivalentes.*

Demostración. Como al realizar cualquier "operación" del tipo (I), (II) o (III) el sistema resultante es equivalente al anterior y teniendo en cuenta que esta relación es de equivalencia se obtiene el resultado. ∎

Ejemplo 14.1.8. En cada uno de los siguientes pasos indicamos el tipo de "operación" que se realiza

$$\left\{\begin{array}{rrrrl} 6x_1 & -4x_2 & +2x_3 & -2x_4 & = 14 \\ x_1 & +x_2 & -x_3 & +2x_4 & = -3 \\ 2x_1 & +3x_2 & -2x_3 & +x_4 & = -4 \end{array}\right. \overset{(I)}{\sim} \quad \left\{\begin{array}{rrrrl} x_1 & +x_2 & -x_3 & +2x_4 & = -3 \\ 6x_1 & -4x_2 & +2x_3 & -2x_4 & = 14 \\ 2x_1 & +3x_2 & -2x_3 & +x_4 & = -4 \end{array}\right. \overset{(II)}{\sim}$$

$$\left\{\begin{array}{rrrrl} x_1 & +x_2 & -x_3 & +2x_4 & = -3 \\ 3x_1 & -2x_2 & +x_3 & -x_4 & = 7 \\ 2x_1 & +3x_2 & -2x_3 & +x_4 & = -4 \end{array}\right. \overset{(III)}{\sim} \quad \left\{\begin{array}{rrrrl} x_1 & +x_2 & -x_3 & +2x_4 & = -3 \\ & -5x_2 & +4x_3 & -7x_4 & = 16 \\ 2x_1 & +3x_2 & -2x_3 & +x_4 & = -4 \end{array}\right. \overset{(III)}{\sim}$$

$$\left\{\begin{array}{rrrrl} x_1 & +x_2 & -x_3 & +2x_4 & = -3 \\ & -5x_2 & +4x_3 & -7x_4 & = 16 \\ & x_2 & & -3x_4 & = 2 \end{array}\right. \overset{(I)}{\sim} \quad \left\{\begin{array}{rrrrl} x_1 & +x_2 & -x_3 & +2x_4 & = -3 \\ & x_2 & & -3x_4 & = 2 \\ & -5x_2 & +4x_3 & -7x_4 & = 16 \end{array}\right. \overset{(III)}{\sim}$$

$$\left\{\begin{array}{rrrrl} x_1 & & -x_3 & +5x_4 & = -5 \\ & x_2 & & -3x_4 & = 2 \\ & -5x_2 & +4x_3 & -7x_4 & = 16 \end{array}\right. \overset{(III)}{\sim} \quad \left\{\begin{array}{rrrrl} x_1 & & -x_3 & +5x_4 & = -5 \\ & x_2 & & -3x_4 & = 2 \\ & & & 4x_3 & -22x_4 = 26 \end{array}\right. \overset{(II)}{\sim}$$

$$\left\{\begin{array}{rrrrl} x_1 & & -x_3 & +5x_4 & = -5 \\ & x_2 & & -3x_4 & = 2 \\ & & x_3 & -\frac{11}{2}x_4 & = \frac{13}{2} \end{array}\right. \overset{(III)}{\sim} \quad \left\{\begin{array}{rrrrl} x_1 & & & -\frac{1}{2}x_4 & = \frac{3}{2} \\ & x_2 & & -3x_4 & = 2 \\ & & x_3 & -\frac{11}{2}x_4 & = \frac{13}{2} \end{array}\right.$$

Aquí podemos observar que si damos a x_4 cualquier valor en $\mathbb{R}$, x_1, x_2 y x_3 quedan completamente determinados, es decir, los elementos en $\mathbb{R}^4$ de la forma

$$\left(\frac{3}{2} + \frac{1}{2}s, 2 + 3s, \frac{13}{2} + \frac{11}{2}s, s\right)$$

donde s es cualquier número real, son soluciones del sistema de ecuaciones original. Esto muestra la idea de lo que deseamos hacer: pasar de un sistema de ecuaciones a otro equivalente donde es fácil no sólo decidir si el sistema tiene o no solución sino que en caso de que la tenga, poder describir todas las soluciones.

Antes de continuar introducimos el concepto de matriz de manera natural a partir de nuestro estudio de sistemas de ecuaciones lineales. Consideramos el sistema de ecuaciones lineales dado como en (1) de la página 482, es decir,

$$(*) \left\{\begin{array}{rcccl} a_{11}x_1 + & \cdots & + a_{1n}x_n & = & b_1 \\ a_{21}x_1 + & \cdots & + a_{2n}x_n & = & b_2 \\ \vdots & \vdots\vdots\vdots & \vdots & & \vdots \\ a_{m1}x_1 + & \cdots & + a_{mn}x_n & = & b_m \end{array}\right.$$

Es claro que este sistema de ecuaciones está determinado por los coeficientes de las indeterminadas y los términos independientes, así que si escribimos estos en el mismo orden en que aparecen en el sistema obtendremos un arreglo de $m \times (n+1)$

elementos de $\mathbb{R}$ como sigue

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & \vdots\vdots\vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{pmatrix}$$

en el entendido de que a_{ij} es el coeficiente de x_j en la ecuación i, para $i = 1, \ldots, m$, $j = 1, \ldots, n$ y el último elemento de cada renglón es el término independiente de la ecuación correspondiente. Como se verá será más cómodo trabajar con estos arreglos que con el sistema de ecuaciones.

Definición 14.1.9. *Una* **matriz de orden $m \times n$ con coeficientes en** $\mathbb{R}$ *es un arreglo de $m \cdot n$ números reales de la siguiente forma*

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots\vdots\vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \longleftarrow \textit{renglón}$$

$$\uparrow$$

$$\textit{columna}$$

donde $a_{ij} \in \mathbb{R}$ para $i = 1, \ldots, m$ y $j = 1, \ldots, n$. Para cada $i = 1, \ldots, m$, $a_{i1}\, a_{i2} \cdots a_{im}$ se llama el i-ésimo renglón de la matriz y para cada $j = 1, \ldots, n$, $\begin{matrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{matrix}$ se llama la j-ésima columna de la matriz. Dos matrices serán iguales si son del mismo orden y los coeficientes correspondientes son iguales.

Así pues una matriz de orden $m \times n$ está compuesta por m renglones y n columnas y la colocación de cada elemento de la matriz está determinada por el renglón y la columna donde se encuentra.
Las "operaciones" que hemos definido para los sistemas de ecuaciones lineales los podemos, sin ningún problema, heredar a las matrices , como operaciones sobre los renglones de la matriz.

Operaciones elementales sobre renglones en matrices

(I) Intercambiar dos renglones.

(II) Multiplicar un renglón por un número real distinto de cero.
(III) Sumar a un renglón otro renglón.

Es claro que el realizar una operación elemental sobre renglones en una matriz, el orden de la matriz resultante es el mismo.
Siguiendo con la idea de lo que se hizo para sistemas de ecuaciones lineales, podemos definir cuándo dos matrices son equivalentes.

Definición 14.1.10. *Una matriz A es equivalente a una matriz B si B se obtiene de A mediante un número finito de operaciones elementales sobre los renglones.*

Ésta relación definida sobre matrices, como en el caso de sistemas de ecuaciones, es de equivalencia (véase ejercicio 14.1.1).
El desarrollo de la teoría de matrices es un tema de primera importancia en el álgebra lineal, es mucho más rica de lo que aquí veremos ya que nos limitaremos a trabajar con ellas sólo en lo que se concierne a nuestro objetivo que son los sistemas de ecuaciones lineales, aunque en el capítulo 16 veremos algo más.
Existen dos tipos de sistemas de ecuaciones lineales, uno es aquellos cuyos términos independientes son todos cero y el otro cuando al menos uno de los términos independientes es distinto de cero. Daremos un nombre a cada uno de ellos.

Definición 14.1.11. *El sistema de ecuaciones lineales (*) se llama homogéneo si* $b_i = 0$ *para toda* $i = 1, \ldots, m$. *En caso contrario se dirá que el sistema es no-homogéneo.*

Un sistema homogéneo de ecuaciones siempre tiene al menos una solución que es $(0, \ldots, 0)$ y a la que llamaremos la ***solución trivial***.
Formalicemos la correspondencia entre sistemas de m ecuaciones lineales en n indeterminadas y las matrices de $m \times n$ y también de orden $m \times (n+1)$.
A cada sistema de ecuaciones lineales $(*)$ le asociamos dos matrices, una de orden $m \times n$ y otra de orden $m \times (n+1)$ que son respectivamente

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots\vdots\vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

llamada ***matriz de coeficientes*** del sistema $(*)$ y

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & \vdots\vdots\vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{pmatrix}$$ llamada ***matriz aumentada*** del sistema $(*)$

Cuando el sistema sea homogéneo trabajaremos únicamente con la matriz de coeficientes puesto que cualquier operación elemental que realicemos sobre los renglones no altera el valor de los términos independientes que son todos cero.
Continuaremos nuestro trabajo utilizando las matrices.

Definición 14.1.12. *Una matriz A de orden $m \times n$ se llama* **escalonada** *si satisface*

(1) *Si $a_{(i-1)k}$ es el primer elemento distinto de cero del renglón $i-1$ y a_{ij} es el primer elemento distinto de cero del renglón i, entonces $k < j$.*
(2) *Si a_{ik} es el primer elemento distinto de cero de un renglón i, entonces $a_{jk} = 0$ para todo $j = 1, \ldots, m$ con $j \neq i$.*
La matriz A se llama **escalonada reducida** *por renglones si es escalonada y*
(3) *El primer elemento distinto de cero de cada renglón es 1.*
(4) *Si un renglón de A consta únicamente de ceros, entonces cualquier renglón por debajo de él también tiene todos sus elementos cero.*

La idea es mostrar que cada matriz A se puede llevar a una matriz escalonada reducida mediante operaciones elementales sobre renglones.

Ejemplo 14.1.13. Considerando el sistema de ecuaciones lineales inicial dado en el ejemplo 14.1.8 la matriz aumentada asociada es

$$\begin{pmatrix} 6 & -4 & 2 & -2 & 14 \\ 1 & 1 & -1 & 2 & -3 \\ 2 & 3 & -2 & 1 & -4 \end{pmatrix}$$

y como es de esperarse, si aplicamos las mismas operaciones elementales sobre los renglones en esta matriz que realizamos en el sistema de ecuaciones lineales, la matriz será la matriz aumentada del sistema de ecuaciones resultante la cual es además escalonada reducida:

$$\begin{pmatrix} 1 & 0 & 0 & -\frac{1}{2} & \frac{3}{2} \\ 0 & 1 & 0 & -3 & 2 \\ 0 & 0 & 1 & -\frac{11}{2} & \frac{13}{2} \end{pmatrix}$$

Veamos un ejemplo más y para que el proceso no resulte tan largo de describir, pasaremos de una matriz a otra posiblemente realizando más de una operación elemental lo que indicaremos poniendo las operaciones que se realizaran: $R_i \longleftrightarrow R_j$ significará que se intercambian los renglones i y j; αR_i significa que el renglón i se multiplica por α; $R_i + \alpha R_j$ significa que el renglón i se le suma α veces el renglón j.

Ejemplo 14.1.14. Consideramos el sistema de ecuaciones lineales

$$\begin{cases} 2x_1 + 2x_2 + 3x_4 + x_5 + 6x_6 = 1 \\ -2x_1 - 2x_2 + 2x_3 - x_4 + 3x_5 + 2x_6 = -1 \\ x_1 + x_2 - x_3 + x_6 = -1 \\ 4x_1 + 4x_2 + 5x_3 + 7x_4 - x_5 = 1 \end{cases}$$

Entonces su matriz aumentada asociada es

$$\begin{pmatrix} 2 & 2 & 0 & 3 & 1 & 6 & 1 \\ -2 & -2 & 2 & -1 & 3 & 2 & -1 \\ 1 & 1 & -1 & 0 & 0 & 1 & -1 \\ 4 & 4 & 5 & 7 & -1 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 2 & 0 & 3 & 1 & 6 & 1 \\ -2 & -2 & 2 & -1 & 3 & 2 & -1 \\ 1 & 1 & -1 & 0 & 0 & 1 & -1 \\ 4 & 4 & 5 & 7 & -1 & 0 & 1 \end{pmatrix} \overset{R_1 \longleftrightarrow R_3}{\sim} \begin{pmatrix} 1 & 1 & -1 & 0 & 0 & 1 & -1 \\ -2 & -2 & 2 & -1 & 3 & 2 & -1 \\ 2 & 2 & 0 & 3 & 1 & 6 & 1 \\ 4 & 4 & 5 & 7 & -1 & 0 & 1 \end{pmatrix} \overset{\substack{R_2+2R_1 \\ R_3-2R_1 \\ R_4-4R_1}}{\sim}$$

$$\begin{pmatrix} 1 & 1 & -1 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & -1 & 3 & 4 & -3 \\ 0 & 0 & 2 & 3 & 1 & 4 & 3 \\ 0 & 0 & 9 & 7 & -1 & -4 & 5 \end{pmatrix} \overset{R_2 \longleftrightarrow R_3}{\sim} \begin{pmatrix} 1 & 1 & -1 & 0 & 0 & 1 & -1 \\ 0 & 0 & 2 & 3 & 1 & 4 & 3 \\ 0 & 0 & 0 & -1 & 3 & 4 & -3 \\ 0 & 0 & 9 & 7 & -1 & -4 & 5 \end{pmatrix} \overset{\frac{1}{2}R_2}{\sim}$$

$$\begin{pmatrix} 1 & 1 & -1 & 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & \frac{3}{2} & \frac{1}{2} & 2 & \frac{3}{2} \\ 0 & 0 & 0 & -1 & 3 & 4 & -3 \\ 0 & 0 & 9 & 7 & -1 & -4 & 5 \end{pmatrix} \overset{\substack{R_1+R_2 \\ R_4-9R_2}}{\sim} \begin{pmatrix} 1 & 1 & 0 & \frac{3}{2} & \frac{1}{2} & 3 & \frac{1}{2} \\ 0 & 0 & 1 & \frac{3}{2} & \frac{1}{2} & 2 & \frac{3}{2} \\ 0 & 0 & 0 & -1 & 3 & 4 & -3 \\ 0 & 0 & 0 & -\frac{13}{2} & -\frac{11}{2} & -22 & -\frac{17}{2} \end{pmatrix} \overset{(-1)R_3}{\sim}$$

$$\begin{pmatrix} 1 & 1 & 0 & \frac{3}{2} & \frac{1}{2} & 3 & \frac{1}{2} \\ 0 & 0 & 1 & \frac{3}{2} & \frac{1}{2} & 2 & \frac{3}{2} \\ 0 & 0 & 0 & 1 & -3 & -4 & 3 \\ 0 & 0 & 0 & -\frac{13}{2} & -\frac{11}{2} & -22 & -\frac{17}{2} \end{pmatrix} \overset{\substack{R_1-\frac{3}{2}R_3 \\ R_2-\frac{3}{2}R_3 \\ R_4+\frac{13}{2}R_3}}{\sim} \begin{pmatrix} 1 & 1 & 0 & 0 & 5 & 9 & -4 \\ 0 & 0 & 1 & 0 & 5 & 8 & -3 \\ 0 & 0 & 0 & 1 & -3 & -4 & 3 \\ 0 & 0 & 0 & 0 & -25 & -48 & 11 \end{pmatrix} \overset{\left(-\frac{1}{25}\right)R_3}{\sim}$$

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 5 & 9 & -4 \\ 0 & 0 & 1 & 0 & 5 & 8 & -3 \\ 0 & 0 & 0 & 1 & -3 & -4 & 3 \\ 0 & 0 & 0 & 0 & 1 & \frac{48}{25} & -\frac{11}{25} \end{pmatrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{matrix} \sim \\ R_1-5R_4 \\ R_2-5R_4 \\ R_3+3R_4 \end{matrix} \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & -\frac{3}{5} & -\frac{9}{5} \\ 0 & 0 & 1 & 0 & 0 & -\frac{8}{5} & -\frac{4}{5} \\ 0 & 0 & 0 & 1 & 0 & \frac{44}{25} & \frac{42}{25} \\ 0 & 0 & 0 & 0 & 1 & \frac{48}{25} & -\frac{11}{25} \end{pmatrix}$$ matriz escalonada reducida

Esta última matriz corresponde a la matriz aumentada del sistema

$$\begin{cases} x_1 + x_2 - \frac{3}{5}x_6 = -\frac{9}{5} \\ x_3 - \frac{8}{5}x_6 = -\frac{4}{5} \\ x_4 + \frac{44}{25}x_6 = \frac{42}{25} \\ x_5 + \frac{48}{25}x_6 = -\frac{11}{25} \end{cases}$$

Entonces, si consideramos

$$\begin{aligned} x_1 &= -\frac{9}{5} - x_2 + \frac{3}{5}x_6 \\ x_3 &= -\frac{4}{5} + \frac{8}{5}x_6 \\ x_4 &= \frac{42}{25} - \frac{44}{25}x_6 \\ x_5 &= -\frac{11}{25} - \frac{48}{25}x_6 \end{aligned}$$

por cada valor real que le damos a x_2 y x_6 (indeterminadas independientes) obtenemos valores reales para x_1, x_3, x_4 y x_5 (es por esto que a estas últimas se les llama indeterminadas dependientes) y tendremos entonces que, para cualesquiera $r, s \in \mathbb{R}$,

$$\left(-\frac{9}{5} - s + \frac{3}{5}t, s, -\frac{4}{5} + \frac{8}{5}t, \frac{42}{25} - \frac{44}{25}t, -\frac{11}{25} - \frac{48}{25}t, t\right)$$

es una solución del sistema. Esto lo podemos comprobar sustituyendo en cada ecuación del sistema y verificando que efectivamente se cumple la igualdad.

Ejemplo 14.1.15. Consideramos el sistema de ecuaciones

$$\begin{cases} 3x_1 + 6x_3 - 3x_4 + 9x_5 = 6 \\ -6x_1 + x_2 - 12x_3 + 6x_4 - 19x_5 = -11 \\ 12x_1 + 24x_3 - 11x_4 + 37x_5 = 27 \\ x_2 + x_4 = 14 \end{cases}$$

Su matriz aumentada asociada es

$$\begin{pmatrix} 3 & 0 & 6 & -3 & 9 & 6 \\ -6 & 1 & -12 & 6 & -19 & -11 \\ 12 & 0 & 24 & -11 & 37 & 27 \\ 0 & 1 & 0 & 1 & 0 & 14 \end{pmatrix}$$

Trataremos de encontrar sus soluciones llevando a esta matriz a su forma escalonada reducida.

$$\begin{pmatrix} 3 & 0 & 6 & -3 & 9 & 6 \\ -6 & 1 & -12 & 6 & -19 & -11 \\ 12 & 0 & 24 & -11 & 37 & 27 \\ 0 & 1 & 0 & 1 & 0 & 14 \end{pmatrix} \xrightarrow{\frac{1}{3}R_1} \begin{pmatrix} 1 & 0 & 2 & -1 & 3 & 2 \\ -6 & 1 & -12 & 6 & -19 & -11 \\ 12 & 0 & 24 & -11 & 37 & 27 \\ 0 & 1 & 0 & 1 & 0 & 14 \end{pmatrix} \xrightarrow[R_3-12R_1]{R_2+6R_1} \begin{pmatrix} 1 & 0 & 2 & -1 & 3 & 2 \\ 0 & 1 & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 3 \\ 0 & 1 & 0 & 1 & 0 & 14 \end{pmatrix} \xrightarrow{R_4-R_2}$$

$$\begin{pmatrix} 1 & 0 & 2 & -1 & 3 & 2 \\ 0 & 1 & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 3 \\ 0 & 0 & 0 & 1 & 1 & 13 \end{pmatrix} \xrightarrow[R_4-R_3]{R_1+R_3} \begin{pmatrix} 1 & 0 & 2 & 0 & 4 & 5 \\ 0 & 1 & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 3 \\ 0 & 0 & 0 & 0 & 0 & 10 \end{pmatrix} \xrightarrow{\frac{1}{10}R_4} \begin{pmatrix} 1 & 0 & 2 & 0 & 4 & 5 \\ 0 & 1 & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 3 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

matriz escalonada reducida

Esta última matriz es la matriz aumentada del sistema de ecuaciones

$$\begin{cases} x_1 + 2x_3 + 4x_5 = 5 \\ x_2 - x_5 = 1 \\ x_4 + x_5 = 3 \\ 0x_1 + 0x_2 + 0x_3 + 0x_4 + 0x_5 = 1 \end{cases}$$

Es evidente que este sistema no puede tener soluciones puesto que no importa qué valores pueden tener x_1, x_2, x_3, x_4 y x_5 en la última ecuación obtendríamos $0 = 1$ lo cual es un absurdo.

Los ejemplos 14.1.14 y 14.1.15 sirven para ilustrar cómo una matriz puede ser llevada a una matriz escalonada reducida y a partir de esta última decidir si el sistema tiene o no solución. En caso de que tenga solución el ejemplo 14.1.14 nos muestra cómo se pueden encontrar todas las soluciones.

Teorema 14.1.16. *Toda matriz de orden $m \times n$ puede llevarse a una matriz escalonada reducida de orden $m \times n$ mediante un número finito de operaciones elementales sobre renglones.*

Demostración. Lo primero que haremos es ubicar todos los renglones que consten únicamente de ceros, mediante intercambio de renglones, en los renglones finales, así que podemos suponer que los primeros r renglones son distintos de cero y los restantes constan todos de ceros. Nuevamente haciendo un intercambio de renglones podemos colocar en el primer renglón a uno con la propiedad de que el primer elemento distinto de cero de cualquier otro renglón no esté más a la izquierda que el primer elemento $a \neq 0$ del primer renglón y multiplicando este

primer renglón por a^{-1} obtenemos una matriz del tipo.

$$\begin{pmatrix} 1 & * & * & \cdots \\ * & * & * & \cdots \\ \vdots & \vdots & \vdots & \vdots\vdots\vdots \\ * & * & * & \cdots \end{pmatrix}$$

donde $*$ es un número real no necesariamente distinto de cero. Ahora, en esta última matriz podemos convertir en ceros los elementos que están por debajo de 1 con lo cual llegamos a una matriz

$$\begin{pmatrix} 1 & * & * & \cdots \\ 0 & * & * & \cdots \\ \vdots & \vdots & \vdots & \vdots\vdots\vdots \\ 0 & * & * & \cdots \end{pmatrix}$$

Considerando ahora los renglones del segundo en adelante volvemos a hacer lo mismo que hicimos antes, mediante intercambio de renglones (sin modificar el primero por supuesto) ponemos en el segundo renglón uno que tenga la propiedad de que el primer elemento distinto de cero de cada renglón debajo de él no esté más a la izquierda que el primer elemento distinto de cero de éste. Acto seguido multiplicamos este renglón por el inverso multiplicativo de su primer elemento distinto de cero y a partir de ahí hacemos cero todos los elementos que están colocados en su misma columna. Debemos hacer la aclaración de que si en algún momento alguno de los renglones se convierte en algún renglón de ceros, entonces podemos intercambiarlo por el último renglón distinto de cero de la matriz. También hay que aclarar que en el proceso, las operaciones elementales que se van aplicando no modifica los ceros que van quedando a la izquierda. Por último, continuando de esta manera llegamos a una matriz escalonada reducida. ∎

Teorema 14.1.17. *En el siguiente sistema homogéneo de ecuaciones lineales*

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = 0 \\ a_{21}x_1 + \cdots + a_{2n}x_n = 0 \\ \vdots \quad \vdots\vdots\vdots \quad \vdots \quad \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = 0 \end{cases}$$

si $m < n$ (esto es el número de ecuaciones es menor que el número de indeterminadas), entonces el sistema tiene una solución no trivial.

Demostración. Sea A la matriz de coeficientes del sistema y B una matriz escalonada reducida equivalente a A. Entonces el sistema homogéneo determinado por B tiene el mismo conjunto de soluciones que el sistema original.
Sean $x_{k_1}, \ldots, x_{k_s}$ las indeterminadas correspondientes al primer elemento distinto de cero que es 1, de cada uno de los renglones distintos de cero de B y sean $x_{\ell_1}, \ldots, x_{\ell_t}$ las restantes indeterminadas de las cuales hay por lo menos una, puesto que $s + t = n$ (el número total de indeterminadas) y como $s < n$ ya que $s \leq m$ y $m < n$, entonces $t \geq 1$.
Luego el sistema homogéneo de ecuaciones lineales correspondientes a B es como sigue

$$\begin{cases} x_{k_1} + \sum_{j=1}^{t} b_{1\ell_j} x_{\ell_j} = 0 \\ \vdots \qquad\qquad \vdots \qquad\quad \vdots \\ x_{k_s} + \sum_{j=1}^{t} b_{s\ell_j} x_{\ell_j} = 0 \end{cases}$$

Si damos valores arbitrarios a $x_{\ell_1}, \ldots, x_{\ell_t}$ quedan determinados automáticamente los valores de $x_{k_1}, \ldots, x_{k_s}$, así que bastará dar un valor distinto de cero a alguna de las x_{ℓ_i} para obtener una solución no trivial del sistema de ecuaciones. ∎

Hemos considerado a las soluciones de un sistema de m ecuaciones en n indeterminadas como elementos de $\mathbb{R}^n$, así que podemos aprovechar la estructura de $\mathbb{R}^n$ (la cual introduciremos más adelante) que es sumamente conocida y lo cual nos permitirá describir de una manera más completa al conjunto de soluciones de un sistema. Antes de trabajar con esta estructura motivémosla discutiendo un poco sobre el conjunto de soluciones de un sistema homogéneo de ecuaciones lineales. Consideramos el sistema homogéneo de ecuaciones lineales

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = 0 \\ a_{21}x_1 + \cdots + a_{2n}x_n = 0 \\ \vdots \quad \vdots\vdots\vdots \quad \vdots \quad \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = 0 \end{cases}$$

Ya hemos visto que el conjunto de soluciones de este sistema es no vacío puesto que $(0, \ldots, 0) \in \mathbb{R}^n$ es solución de él. Ahora si $(s_1, \ldots, s_n)$ y $(s'_1, \ldots, s'_n)$ y $\alpha \in \mathbb{R}$, entonces $(s_1 + s'_1, \ldots, s_n + s'_n)$ y $(\alpha s_1, \ldots, \alpha s_n)$ también serán soluciones pues para cada $i = 1, \ldots, m$

$$a_{i1}(s_1 + s'_1) + \cdots + a_{in}(s_n + s'_n) = (a_{i1}s_1 + \cdots + a_{in}s_n) + (a_{i1}s'_1 + \cdots + a_{in}s'_n) = 0 + 0 = 0$$

y

$$a_{i1}(\alpha s_1) + \cdots + a_{in}(\alpha s_n) = \alpha(a_{i1}s_1 + \cdots + a_{in}s_n) = \alpha \cdot 0 = 0.$$

De aquí podemos observar que si el sistema tiene una solución distinta de cero, entonces tendrá una infinidad de soluciones. Sería interesante descubrir cuándo $(0, \ldots, 0)$ es la única solución. Esto lo veremos en la próxima sección.

§ 14.2. El espacio vectorial $\mathbb{R}^n$

En esta sección daremos una estructura a $\mathbb{R}^n$ que es la de espacio vectorial y la cual nos proporcionará resultados muy importantes para nuestro estudio de sistemas de ecuaciones lineales. Como ya adelantamos en la sección anterior, el conjunto de soluciones de un sistema homogéneo de ecuaciones lineales tiene propiedades muy interesantes y son este tipo de subconjuntos de $\mathbb{R}^n$ los que estudiaremos aquí y a las que llamaremos subespacios vectoriales de $\mathbb{R}^n$. Comenzamos presentando esta estructura de espacio vectorial para $\mathbb{R}^n$ y para esto necesitaremos antes definir la suma de los elementos de $\mathbb{R}^n$ y el producto por números reales de elementos de $\mathbb{R}^n$. En estas definiciones introduciremos también la notación que usaremos a lo largo de este capítulo.

Definición 14.2.1. *Sean* $\overline{s} = (s_1, \ldots, s_n)$ *y* $\overline{t} = (t_1, \ldots, t_n)$ *en* $\mathbb{R}^n$ *y* $\alpha \in \mathbb{R}$.

(*a*) *la suma* $\overline{s} + \overline{t}$ *de* $\overline{s}$ *y* $\overline{t}$ *es* $\overline{s} + \overline{t} = (s_1 + t_1, \ldots, s_n + t_n)$.
(*b*) *el producto* $\alpha \cdot \overline{s}$ *de* α *y* $\overline{s}$ *es* $\alpha \cdot \overline{s} = (\alpha s_1, \ldots, \alpha s_n)$.

Es evidente que $\overline{s} + \overline{t} \in \mathbb{R}^n$ y $\alpha \cdot \overline{s} \in \mathbb{R}^n$.
Con respecto a la suma y producto por números reales, también llamado ***producto por escalares*** (esta última denominación es porque en general se trabaja con un campo K y a sus elementos los llamaremos escalares) $\mathbb{R}^n$ tiene las siguientes propiedades.

Teorema 14.2.2. *Sean* $\overline{s}, \overline{t}, \overline{v} \in \mathbb{R}^n$ *y* $\alpha, \beta \in \mathbb{R}$. *Entonces*

(1) $(\overline{s} + \overline{t}) + \overline{v} = \overline{s} + (\overline{t} + \overline{v})$.
(2) $\overline{s} + \overline{t} = \overline{t} + \overline{s}$
(3) $\overline{s} + \overline{0} = \overline{0} + \overline{s} = \overline{s}$, *donde* $\overline{0} = (0, \ldots, 0)$
(4) *Existe* $\overline{s}' \in \mathbb{R}^n$ *tal que* $\overline{s} + \overline{s}' = \overline{0}$
(5) $\alpha \cdot (\overline{s} + \overline{t}) = \alpha \cdot \overline{s} + \alpha \cdot \overline{t}$
(6) $(\alpha + \beta) \cdot \overline{s} = \alpha \cdot \overline{s} + \beta \cdot \overline{s}$
(7) $(\alpha\beta) \cdot \overline{s} = \alpha \cdot (\beta \cdot \overline{s})$
(8) $1 \cdot \overline{s} = \overline{s}$

La demostración de estas propiedades es bastante sencilla, así que las dejamos como ejercicio (véase ejercicio 14.2.1)
En el ejercicio 14.2.3 se da la definición en general de un espacio vectorial sobre un campo K. Teniendo en cuenta esta definición se tiene entonces, a partir del teorema 14.2.2, que $\mathbb{R}^n$ es un espacio vectorial sobre $\mathbb{R}$.
A los elementos de un espacio vectorial se les llama ***vectores***.

Nota 14.2.3. En el ejercicio 14.2.2 se pide demostrar que el vector $\overline{s}'$ del inciso (4) del teorema 14.2.2 es único. Denotaremos por $\boldsymbol{-\overline{s}}$ a este vector, es decir, $-\overline{s}$ denota al vector en $\mathbb{R}^n$ tal que $\overline{s} + (-\overline{s}) = \overline{0}$.

En general escribiremos $\overline{s} - \overline{s}'$ en lugar de $\overline{s} + (-\overline{s}')$

Ejemplo 14.2.4. Sean $\overline{s} = \left(-\frac{1}{2}, \sqrt{2}, 1\right)$ y $\overline{t} = \left(\frac{3}{2}, \sqrt{5}, -3\right)$. Entonces
$\overline{s} + \overline{t} = \left(-\frac{1}{2} + \frac{3}{2}, \sqrt{2} + \sqrt{5}, -2\right)$
$\sqrt{2} \cdot \overline{s} = \left(-\frac{1}{2}\sqrt{2}, \sqrt{2}\sqrt{2}, 1\sqrt{2}\right) = \left(-\frac{\sqrt{2}}{2}, 2, \sqrt{2}\right)$
$-\overline{s} = \left(\frac{1}{2}, -\sqrt{2}, -1\right)$

Introduciremos ahora el concepto de subespacio vectorial.

Definición 14.2.5. *Un subconjunto S de $\mathbb{R}^n$ es un* **subespacio vectorial** *de $\mathbb{R}^n$ si*

(*i*) $\overline{0} \in S$.
(*ii*) *Si* $\overline{s}, \overline{t} \in S$, *entonces* $\overline{s} + \overline{t} \in S$.
(*iii*) *Si* $\overline{s} \in S$ *y* $\alpha \in \mathbb{R}$, *entonces* $\alpha \cdot \overline{s} \in S$.

Ejemplo 14.2.6. $\mathbb{R}^n$ y $\{\overline{0}\}$ son subespacios de $\mathbb{R}^n$.

Ejemplo 14.2.7. Sea $S = \{(a, b, a + b) \mid a, b \in \mathbb{R}\} \subseteq \mathbb{R}^3$. S es un subespacio de $\mathbb{R}^3$:

(*i*) $\overline{0} \in S$ es evidente.
(*ii*) Sean $\overline{s}, \overline{t} \in S$. Entonces $\overline{s} = (a, b, a + b)$, $\overline{t} = (a', b', a' + b')$ y

$$\overline{s} + \overline{t} = (a + a', b + b', a + b + a' + b') = (a + a', b + b', a + a' + b + b') \in S.$$

(*iii*) Si $\overline{s} \in S$ y $\alpha \in \mathbb{R}$ donde $\overline{s} = (a, b, a + b)$, entonces

$$\alpha \cdot \overline{s} = (\alpha a, \alpha b, \alpha(a + b)) = (\alpha a, \alpha b, \alpha a + \alpha b) \in S.$$

Ejemplo 14.2.8. Sea $S = \{(a, a, 2a, 0) \mid a \in \mathbb{R}\} \subseteq \mathbb{R}^4$. S es un subespacio de $\mathbb{R}^4$:

(*i*) $\overline{0} = (0, 0, 2 \cdot 0, 0) \in S$.

(*ii*) Sean $\overline{s} = (a, a, 2a, 0)$ y $\overline{t} = (b, b, 2b, 0) \in S$. Entonces

$$\overline{s} + \overline{t} = (a + b, a + b, 2(a + b), 0) \in S.$$

(*iii*) Si $\overline{s} = (a, a, 2a, 0)$ y $\alpha \in \mathbb{R}$, entonces $\alpha \cdot \overline{s} = (\alpha a, \alpha a, \alpha(2a), 0) \in S$

Ejemplo 14.2.9. Sea $S = \{(a, b, c, 1) \mid a, b, c \in \mathbb{R}\} \subseteq \mathbb{R}^4$. S no es subespacio de $\mathbb{R}^4$ puesto que $\overline{0} \notin S$.

Aunque podríamos dar el siguiente como un ejemplo de subespacio de $\mathbb{R}^n$, por la importancia que tiene para nuestro estudio de sistemas de ecuaciones lo presentamos como proposición.

Proposición 14.2.10. *Consideremos el sistema homogéneo de ecuaciones lineales*

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = 0 \\ a_{21}x_1 + \cdots + a_{2n}x_n = 0 \\ \vdots \quad \vdots\vdots\vdots \quad \vdots \quad \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = 0 \end{cases}$$

Entonces el conjunto S de soluciones del sistema es un subespacio de $\mathbb{R}^n$.

Demostración.

(*i*) $\overline{0} = (0, \ldots, 0) \in S$ ya que para toda $i = 1, \ldots, m$, $a_{i1}0 + \cdots + a_{in}0 = 0$.

(*ii*) Sean $\overline{s} = (s_1, \ldots, s_n), \overline{t} = (t_1, \ldots, t_n) \in S$. Entonces para toda $i = 1, \ldots, m$,

$$a_{i1}s_1 + \cdots + a_{in}s_n = 0$$

y

$$a_{i1}t_1 + \cdots + a_{in}t_n = 0.$$

Sumando estas igualdades obtenemos

$$0 = (a_{i1}s_1 + \cdots + a_{in}s_n) + (a_{i1}t_1 + \cdots + a_{in}t_n) = a_{i1}(s_1 + t_1) + \cdots + a_{in}(s_n + t_n)$$

para toda $i = 1, \ldots, m$. Por lo tanto $\overline{s} + \overline{t} = (s_1 + t_1, \ldots, s_n + t_n) \in S$.

(*iii*) Sean $\overline{s} = (s_1, \ldots, s_n) \in S$ y $\alpha \in \mathbb{R}$. Entonces para cada $i = 1, \ldots, m$,

$$a_{i1}s_1 + \cdots + a_{in}s_n = 0$$

y multiplicando por α,

$$0 = \alpha \cdot (a_{i1}s_1 + \cdots + a_{in}s_n) = a_{i1}(\alpha s_1) + \cdots + a_{in}(\alpha s_n)$$

y por lo tanto $\alpha \cdot \overline{s} = (\alpha s_1, \ldots, \alpha s_n) \in S$. ■

Nuestro objetivo ahora será mostrar cómo un subespacio de $\mathbb{R}^n$, cualquiera que sea éste, se puede describir a través de cierto subconjunto finito de él.

Definición 14.2.11. *Sean* $\overline{s}_1, \ldots, \overline{s}_m \in \mathbb{R}^n$. *Una* **combinación lineal** *de* $\overline{s}_1, \ldots, \overline{s}_m$ *es una expresión* $\alpha_1 \cdot \overline{s}_1 + \cdots + \alpha_m \cdot \overline{s}_m$, *donde* $\alpha_1, \ldots, \alpha_m \in \mathbb{R}$.

Expresado de otra manera, $\overline{s} \in \mathbb{R}^n$ es combinación lineal de $\overline{s}_1, \ldots, \overline{s}_m$ si y sólo si existen $\alpha_1, \ldots, \alpha_m \in \mathbb{R}$ tales que $\overline{s} = \alpha_1 \cdot \overline{s}_1 + \cdots + \alpha_m \cdot \overline{s}_m$.

Ejemplo 14.2.12. $(5, 10, 1, 4) \in \mathbb{R}^4$ es combinación lineal de $(3, 4, -1, 0)$, $(1, 1, 0, -1)$ y $(0, 1, 1, 1)$ ya que

$$(5, 10, 1, 4) = 2 \cdot (3, 4, -1, 0) + (-1) \cdot (1, 1, 0, -1) + 3 \cdot (0, 1, 1, 1).$$

Ejemplo 14.2.13. Es claro que $(1, -1, 1) \in \mathbb{R}^3$ no puede ser combinación lineal de $(3, -2, 0)$ y $(-1, -1, 0)$ ya que cualquier combinación lineal de $(3, -2, 0)$ y $(-1, -1, 0)$ siempre tendrá su tercera coordenada 0.

Ejemplo 14.2.14. Para cualesquiera $\overline{s}_1, \ldots, \overline{s}_m \in \mathbb{R}^n$, $\overline{0}$ es combinación lineal de de ellos ya que $\overline{0} = 0 \cdot \overline{s}_1 + \cdots + 0 \cdot \overline{s}_m$ (véase el ejercicio 14.2.3 (*iv*)).

Proposición 14.2.15. *Sean* $\overline{s}_1, \ldots, \overline{s}_m \in \mathbb{R}^n$ *y* $S = \{\alpha_1 \cdot \overline{s}_1 + \cdots + \alpha_m \cdot \overline{s}_m \mid \alpha_i \in \mathbb{R}$ *para toda* $i = 1, \ldots, m$. *Entonces* S *es un subespacio de* $\mathbb{R}^n$ *que contiene a* $\{\overline{s}_1, \ldots, \overline{s}_m\}$.

Demostración. $\overline{s}_i \in \mathbb{R}^n$ para toda $i = 1, \ldots, m$ ya que

$$\overline{s}_i = 0 \cdot \overline{s}_1 + \cdots + 0 \cdot \overline{s}_{i-1} + 1 \cdot \overline{s}_i + 0 \cdot \overline{s}_{i+1} + \cdots + 0 \cdot \overline{s}_m.$$

Ahora veamos que S es un subespacio de $\mathbb{R}^n$.

(*i*) $\overline{0} = 0 \cdot \overline{s}_1 + \cdots + 0 \cdot \overline{s}_m \in S$.

(*ii*) Si $\overline{s}, \overline{t} \in S$, entonces $\overline{s} = \alpha_1 \cdot \overline{s}_1 + \cdots + \alpha_m \cdot \overline{s}_m$ y $\overline{t} = \beta_1 \cdot \overline{s}_1 + \cdots + \beta_m \cdot \overline{s}_m$, donde $\alpha_i, \beta_i \in \mathbb{R}$ para $i = 1, \ldots, m$. Luego

$$\overline{s} + \overline{t} = (\alpha_1 \cdot \overline{s}_1 + \cdots + \alpha_m \cdot \overline{s}_m) + (\beta_1 \cdot \overline{s}_1 + \cdots + \beta_m \cdot \overline{s}_m) = (\alpha_1 + \beta_1) \cdot \overline{s}_1 + \cdots + (\alpha_m + \beta_m) \cdot \overline{s}_m$$

y por lo tanto $\overline{s} + \overline{t} \in S$.

(*iii*) Si $\overline{s} \in S$, $\alpha \in \mathbb{R}$ y $\overline{s} = \alpha_1 \cdot \overline{s}_1 + \cdots + \alpha_m \cdot \overline{s}_m$, entonces

$$\alpha \cdot \overline{s} = \alpha \cdot (\alpha_1 \cdot \overline{s}_1 + \cdots + \alpha_m \cdot \overline{s}_m) = \overline{s} = (\alpha\alpha_1) \cdot \overline{s}_1 + \cdots + (\alpha\alpha_m) \cdot \overline{s}_m \in S. \blacksquare$$

Definición 14.2.16. *Sea* S *un subespacio de* $\mathbb{R}^n$ *y* $\overline{s}_1, \ldots, \overline{s}_m \in \mathbb{R}^n$. *Diremos que* $\overline{s}_1, \ldots, \overline{s}_m$ ***generan*** *a* S *o* S *es el* ***subespacio generado*** *por* $\overline{s}_1, \ldots, \overline{s}_m$ *si*

$$S = \{\alpha_1 \cdot \overline{s}_1 + \cdots + \alpha_m \cdot \overline{s}_m \mid \alpha_i \in \mathbb{R} \text{ para toda } i = 1, \ldots, m\}.$$

A $\{\overline{s}_1, \ldots, \overline{s}_m\}$ *se le llama un conjunto de generadores de* S*.*

Entonces S es el subespacio generado por $\overline{s}_1, \ldots, \overline{s}_m$ si y sólo si cada $\overline{s} \in S$ se escribe como combinación lineal de $\overline{s}_1, \ldots, \overline{s}_m$.

Notación 14.2.17*. Al subespacio generado por* $\overline{s}_1, \ldots, \overline{s}_m$ *lo denotaremos por* $\langle \overline{s}_1, \ldots, \overline{s}_m \rangle$*. Convenimos en que el subespacio generado por el conjunto vacío* $\varnothing$ *es* $\{\overline{0}\}$*. Es decir,* $\langle \varnothing \rangle = \{0\}$*.*

Ejemplo 14.2.18. Sea $S = \{(a, 0, 0) \mid a \in \mathbb{R}\} \subseteq \mathbb{R}^3$. Entonces S es el subespacio generado por $(1, 0, 0)$ ya que si $\overline{s} \in S$ y $\overline{s} = (a, 0, 0)$, entonces $\overline{s} = a \cdot (1, 0, 0)$. También $(2, 0, 0)$ genera a S: $\overline{s} = (a, 0, 0) = \left(\frac{a}{2}\right) \cdot (2, 0, 0)$. Esto muestra que puede haber distintos subconjuntos de S que lo generen y no sólo eso, el número de elementos en dos conjuntos de generadores no necesariamente es el mismo: $(2, 0, 0)$ y $(3, 0, 0)$ generan a S puesto que

$$\overline{s} = (a, 0, 0) = a \cdot (3, 0, 0) + (-a) \cdot (2, 0, 0).$$

Ejemplo 14.2.19. $\mathbb{R}^3$ está generado por $(1, 0, 0), (0, 1, 0), (0, 0, 1)$. Sea $(a, b, c) \in \mathbb{R}^3$. Entonces $(a, b, c) = a \cdot (1, 0, 0) + b \cdot (0, 1, 0) + c \cdot (0, 0, 1)$. Veamos que $\mathbb{R}^3$ también está generado por $(1, 0, 0), (1, 1, 0), (1, 1, 1)$ y para esto encontraremos $x_1, x_2, x_3 \in \mathbb{R}$ tales que

$$(a, b, c) = x_1 \cdot (1, 0, 0) + x_2 \cdot (1, 1, 0) + x_3 \cdot (1, 1, 1).$$

Multiplicando y sumando en el lado derecho de la igualdad obtenemos $(a, b, c) = (x_1 + x_2 + x_3, x_2 + x_3, x_3)$ y ésta da lugar a un sistema de 3 ecuaciones lineales en 3 indeterminadas:

$$\begin{cases} x_1 + x_2 + x_3 = a \\ \qquad x_2 + x_3 = b \\ \qquad\qquad x_3 = c \end{cases}$$

Por lo tanto debe ser

$$x_3 = c, \quad x_2 = b - x_3 = b - c \ \ y \ \ x_1 = a - x_2 - x_3 = a - (b - c) - c = a - b.$$

Entonces $(a, b, c) = (a - b) \cdot (1, 0, 0) + (b - c) \cdot (1, 1, 0) + c \cdot (1, 1, 1)$.

§ §14.2.1. Dependencia e independencia lineal

Definición 14.2.20*. Sean* $\overline{s}_1, \ldots, \overline{s}_m \in \mathbb{R}^n$*. Decimos que* $\overline{s}_1, \ldots, \overline{s}_m$ *son* **linealmente dependientes** *o* $\{\overline{s}_1, \ldots, \overline{s}_m\}$ *es un* **conjunto linealmente dependiente** *si existen* $\alpha_1, \ldots, \alpha_m \in \mathbb{R}$ *no todos cero tales que* $\alpha_1 \cdot \overline{s}_1 + \cdots + \alpha_m \cdot \overline{s}_m = \overline{0}$*. En caso*

contrario se dirá que $\overline{s}_1, \ldots, \overline{s}_m$ *son* **linealmente independientes** *o* $\{\overline{s}_1, \ldots, \overline{s}_m\}$ *es un* **conjunto linealmente independiente**.

Entonces, según la definición, $\overline{s}_1, \ldots, \overline{s}_m$ son linealmente independientes si la única manera de expresar a $\overline{0}$ como combinación lineal de ellos es considerando 0 todos los coeficientes, esto es, si $\alpha_1 \cdot \overline{s}_1 + \cdots + \alpha_m \cdot \overline{s}_m = \overline{0}$, entonces $\alpha_1 = \cdots = \alpha_m = 0$.

Ejemplo 14.2.21. (*a*) Si alguno de los vectores $\overline{s}_1, \ldots, \overline{s}_m \in \mathbb{R}^n$ es el vector $\overline{0}$, entonces $\overline{s}_1, \ldots, \overline{s}_m$ son linealmente dependientes. Sin perder generalidad podemos suponer $\overline{s}_1 = \overline{0}$. Entonces $1 \cdot \overline{0} + 0 \cdot \overline{s_2} + \cdots + 0 \cdot \overline{s}_m = \overline{0}$ (véase ejercicio 14.2.3 (*v*)). En particular $\overline{0}$ es linealmente dependiente.
(*b*) Cualquier $\overline{s} \in \mathbb{R}^n$, $\overline{s} \neq \overline{0}$ es linealmente independiente ya que $\alpha \cdot \overline{s} = \overline{0}$ implica $\alpha = 0$ (véase el ejercicio 14.2.3 (*vi*)).

Proposición 14.2.22. $\{\overline{s}_1, \ldots, \overline{s}_m\} \subseteq \mathbb{R}^n$ *es linealmente dependiente si y sólo si uno de ellos es una combinación lineal de los restantes.*

Demostración.

$\Longrightarrow$) Supongamos que $\overline{s}_1, \ldots, \overline{s}_m$ son linealmente dependientes. Luego existen $\alpha_1, \ldots, \alpha_m$ no todos cero tales que $\alpha_1 \overline{s}_1 + \cdots + \alpha_m \overline{s}_m = \overline{0}$. Podemos suponer $\alpha_1 \neq 0$. Entonces $\overline{s}_1 = \left(\frac{-\alpha_2}{\alpha_1}\right) \overline{s}_2 + \cdots + \left(\frac{-\alpha_m}{\alpha_1}\right) \overline{s}_m$.
$\Longleftarrow$) Si $\overline{s}_1$ es combinación lineal de $\overline{s}_2, \ldots, \overline{s}_m$, existen $\alpha_2, \ldots, \alpha_m \in \mathbb{R}$ tales que $\overline{s}_1 = \alpha_2 \overline{s}_2 + \cdots + \alpha_m \overline{s}_m$ y por lo tanto $(-1)\overline{s}_1 + \alpha_2 \overline{s}_2 + \cdots + \alpha_m \overline{s}_m = \overline{0}$, esto es, $\overline{s}_1, \ldots, \overline{s}_m$ son linealmente dependientes. ∎

Ejemplo 14.2.23. Los vectores $(1,0,0), (1,1,0), (1,1,1)$ son linealmente independientes en $\mathbb{R}^3$ puesto que si

$$\alpha_1 \cdot (1,0,0) + \alpha_2 \cdot (1,1,0) + \alpha_3 \cdot (1,1,1) = (0,0,0),$$

entonces

$$(\alpha_1 + \alpha_2 + \alpha_3, \alpha_2 + \alpha_3, \alpha_3) = (0,0,0)$$

y esto último implica que

$$\begin{cases} \alpha_1 + \alpha_2 + \alpha_3 = 0 \\ \alpha_2 + \alpha_3 = 0 \\ \alpha_3 = 0 \end{cases}$$

y por lo tanto $\alpha_1 = \alpha_2 = \alpha_3 = 0$

Ejemplo 14.2.24. $(1,2,3,4)$ y $(-1,1,1,2)$ son linealmente independientes en $\mathbb{R}^4$. Supongamos que $\alpha_1 \cdot (1,2,3,4) + \alpha_2 \cdot (-1,1,1,2) = (0,0,0,0)$. Entonces

$$(\alpha_1 - \alpha_2, 2\alpha_1 - \alpha_2, 3\alpha_1 - \alpha_2, 4\alpha_1 + 2\alpha_2) = (0,0,0,0),$$

por lo que

$$\begin{cases} \alpha_1 - \alpha_2 = 0 \\ 2\alpha_1 + \alpha_2 = 0 \\ 3\alpha_1 + \alpha_2 = 0 \\ 4\alpha_1 + 2\alpha_2 = 0 \end{cases}$$

De la primera igualdad obtenemos $\alpha_1 = \alpha_2$ y entonces $2\alpha_1 + \alpha_2 = 3\alpha_1 = 0$, así que $\alpha_1 = \alpha_2 = 0$ y por lo tanto los vectores son linealmente independientes.

Ejemplo 14.2.25. Para cada $n \geq 1$,

$$\overline{e}_1 = (1,0,0,\ldots,0),\ \overline{e}_2 = (0,1,0,\ldots,0),\ldots,\ \overline{e}_n = (0,0,0,\ldots,1),$$

$\overline{e}_1, \ldots, \overline{e}_n$ son linealmente independientes.

Proposición 14.2.26. *Si $\overline{s}_1, \ldots, \overline{s}_m \in \mathbb{R}^m$ son linealmente dependientes, entonces para cualesquiera $\overline{s}_{m+1}, \ldots, \overline{s}_{m+k} \in \mathbb{R}^m$, $\overline{s}_1, \ldots, \overline{s}_m, \overline{s}_{m+1}, \ldots, \overline{s}_{m+k}$ es linealmente dependiente. Es decir, cualquier conjunto finito que contenga a un conjunto linealmente dependiente es también linealmente dependiente.*

Demostración. Supongamos que $\overline{s}_1, \ldots, \overline{s}_m$ son linealmente dependientes. Luego existen $\alpha_1, \ldots, \alpha_m \in \mathbb{R}$ no todos cero tales que

$$\alpha_1 \cdot \overline{s}_1 + \cdots + \alpha_m \cdot \overline{s}_m = \overline{0}.$$

Teniendo en cuenta que $0 \cdot \overline{s} = \overline{0}$ para todo $\overline{s} \in \mathbb{R}^n$, entonces

$$\alpha_1 \cdot \overline{s}_1 + \cdots + \alpha_m \cdot \overline{s}_m + 0 \cdot \overline{s}_{m+1} + \cdots + 0 \cdot \overline{s}_{m+k} = \overline{0},$$

donde algún $\alpha_i \neq 0$ y por lo tanto $\overline{s}_1 + \cdots + \overline{s}_{m+k}$ son linealmente dependientes. ∎

Corolario 14.2.27. *Si $v_1, \ldots, v_n$ son linealmente independientes y*

$$\{v_{i_1}, \ldots, v_{i_m}\} \subseteq \{v_1, \ldots, v_n\},$$

donde cada $v_{i_j} \neq v_{i_k}$ si $j \neq k$ para $1 \leq j,k \leq m$, entonces $v_{i_1}, \ldots, v_{i_m}$ son linealmente independientes.

Demostración. Si $v_{i_1}, \ldots, v_{i_m}$ fueran linealmente dependientes, por la proposición 14.2.26 $\{v_1, \ldots, v_n\}$ también lo sería. ∎

§ §14.2.2. Base de un espacio.

Introducimos el concepto de base y esto nos permitirá describir un subespacio a través de un número finito de vectores en el espacio $\mathbb{R}^n$.

Definición 14.2.28. *Sean S un subespacio de $\mathbb{R}^n$ y $\overline{s}_1, \ldots, \overline{s}_m \in S$. Diremos que $\{\overline{s}_1, \ldots, \overline{s}_m\}$ es una* **base** *de S si*

(1) $\overline{s}_1, \ldots, \overline{s}_m$ *generan a S.*
(2) $\overline{s}_1, \ldots, \overline{s}_m$ *son linealmente independientes.*

Nota 14.2.29. Si $S = \left\{\overline{0}\right\}$ convenimos en que $\varnothing$ es una base de él.

Ejemplo 14.2.30. (a) Sea $S = \{(a, 0, 0) \mid a \in \mathbb{R}\} \subseteq \mathbb{R}^3$. En el ejemplo 14.2.18 se demostró que $(1, 0, 0)$ genera a S. Además $(1, 0, 0)$ es linealmente independiente ya que si $\alpha \cdot (1, 0, 0) = (0, 0, 0)$, entonces $(\alpha, 0, 0) = (0, 0, 0)$ y de aquí debe ser $\alpha = 0$. Por lo tanto $\{(1, 0, 0)\}$ es una base de S. Ahí mismo se vio también que $(2, 0, 0)$ y $(3, 0, 0)$ generan a S. Sin embargo no es difícil ver que estos vectores son linealmente dependientes: $\frac{3}{2} \cdot (2, 0, 0) - (3, 0, 0) = (0, 0, 0)$, así que $\{(2, 0, 0), (3, 0, 0)\}$ no es base de S.

(b) $\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$ es una base para $\mathbb{R}^3$. En el ejemplo 14.2.19 se demostró que genera a $\mathbb{R}^3$ y son linealmente independientes puesto que

$$\alpha_1 \cdot (1, 0, 0) + \alpha_2 \cdot (1, 0, 0) + \alpha_3 \cdot (0, 0, 1) = (0, 0, 0)$$

implica $\alpha_1 = \alpha_2 = \alpha_3 = 0$. En ese mismo ejemplo vimos que también

$$(1, 0, 0), (1, 1, 0), (1, 1, 1)$$

generan a $\mathbb{R}^3$ y en el ejemplo 14.2.19 se demostró que son linealmente independientes y por lo tanto forman una base para $\mathbb{R}^3$.

Vale la pena mencionar que no es casualidad el hecho de que ambos conjuntos tienen el mismo número de elementos. Es cierto en general que cualesquiera dos bases de una espacio vectorial tienen la misma cardinalidad.

Teorema 14.2.31. *Sea S un subespacio vectorial de $\mathbb{R}^n$. Un subconjunto $\{s_1, \ldots, s_m\}$ de S es una base de S si y sólo si cada vector $s \in S$ se expresa de manera única como combinación lineal de $s_1, \ldots, s_m$.*

Demostración.

$\Longrightarrow$) Si $\{s_1, \ldots, s_m\}$ es una base de S, sabemos por definición que cada vector de S es combinación lineal de ellos, así que sólo nos falta demostrar que esta combinación lineal es única: suponemos que

$$s = \alpha_1 s_1 + \cdots + \alpha_m s_m = \beta_1 s_1 + \cdots + \beta_m s_m$$

donde $\alpha_i, \beta_i \in K$ para $i = 1, \ldots, m$. Entonces $(\alpha_1 - \beta_1)s_1 + \cdots + (\alpha_m - \beta_m)s_m = \overline{0}$ y por ser $\{s_1, \ldots, s_m\}$ linealmente independientes, debe ser $\alpha_i - \beta_i = 0$ para toda $i = 1, \ldots, m$,es decir $\alpha_i = \beta_i$ para toda $i = 1, \ldots, m$. Por lo tanto la expresión de s como una combinación lineal de $\{s_1, \ldots, s_m\}$ es única.
$\Longleftarrow$) Supongamos que cada vector $s \in S$ se expresa de manera única como combinación lineal de $\{s_1, \ldots, s_m\}$. Esto significa que $\{s_1, \ldots, s_m\}$ genera a $\mathbb{R}^n$, así que sólo nos queda demostrar que son linealmente independientes, pero si $\alpha_1 s_1 + \cdot + \alpha_m s_m = \overline{0}$, ya que también $0s_1 + \cdots + 0s_m = \overline{0}$, por la unicidad $\alpha_1 = \cdots = \alpha_m = 0$. Luego $\{s_1, \ldots, s_m\}$ es una base de S. ∎

Ejemplo 14.2.32. Para cada $n \in \mathbb{N}$, $n \geq 1$, si

$$\overline{e}_1 = (1, 0, 0, \ldots, 0),\ \overline{e}_2 = (0, 1, 0, \ldots, 0), \ldots, \overline{e}_n = (0, 0, 0, \ldots, 1),$$

$\{\overline{e}_1, \ldots, \overline{e}_n\}$ es una base de $\mathbb{R}^n$ (véase los ejemplos 14.2.19 y 14.2.25) y se le conoce como la ***base canónica*** de $\mathbb{R}^n$.

Si observamos los ejemplos que hemos dado de conjuntos linealmente independientes en $\mathbb{R}^n$, en cada caso la cardinalidad de estos conjuntos está acotada precisamente por n, esto es el ejemplo 14.2.21 (b) $\{\overline{s}\}$ es linealmente independiente donde $n \geq 1$ y por lo tanto el subespacio $S =< \overline{s} >$ tiene como base a $\{\overline{s}\}$; en el ejemplo 14.2.23 $\{(1, 0, 0), (1, 1, 0), (1, 1, 1)\}$ es linealmente independiente en $\mathbb{R}^3$. Veremos enseguida que cualquier conjunto de vectores en $\mathbb{R}^n$ con más de n elementos es linealmente dependiente en $\mathbb{R}^n$.

Teorema 14.2.33. *Sean $\overline{s}_1, \ldots, \overline{s}_m \in \mathbb{R}^n$. Si $m > n$, entonces $\overline{s}_1, \ldots, \overline{s}_m$ son linealmente dependientes.*

Demostración. Para ver que $\overline{s}_1, \ldots, \overline{s}_m$ son linealmente dependientes debemos encontrar $x_1, \ldots, x_m \in \mathbb{R}$ no todos cero tales que $x_1\overline{s}_1 + \cdots + x_m\overline{s}_m = \overline{0}$.

Esta igualdad es equivalente al siguiente sistema de ecuaciones lineales

$$\left\{\begin{array}{ccccccc} s_{11}x_1 & + s_{12}x_2 & + & \cdots & + s_{1m}x_m & = & 0 \\ s_{21}x_1 & + s_{22}x_2 & + & \cdots & + s_{2m}x_m & = & 0 \\ \vdots & & \vdots & \vdots\vdots & \vdots & & \vdots \\ s_{n1}x_1 & + s_{n2}x_2 & + & \cdots & + s_{nm}x_m & = & 0 \end{array}\right.$$

donde $\overline{s}_i = (s_{1i}, s_{2i}, \ldots, s_{ni})$ para $i = 1, \ldots, m$, así que bastará demostrar que este sistema de ecuaciones lineales tiene una solución no trivial. Pero esto es inmediato del teorema 14.1.17 puesto que por hipótesis el número n de ecuaciones es menor que el número de indeterminadas que es m. ∎

Corolario 14.2.34. *Si $\overline{s}_1, \ldots, \overline{s}_m \in \mathbb{R}^n$ son linealmente independientes, entonces $m \leq n$.*

Con la ayuda de este último teorema demostraremos que cada subespacio de $\mathbb{R}^n$ tiene una base, por lo que a los elementos de un subespacio los podremos describir a través de de ella, esto es, si $\overline{s}_1, \ldots, \overline{s}_m$ es una base del subespacio S de $\mathbb{R}^n$, entonces cada elemento de S se expresará de manera única (ver el teorema 14.2.31) como $\alpha_1\overline{s}_1 + \cdots + \alpha_m\overline{s}_m$ donde $\alpha_1, \ldots, \alpha_m \in \mathbb{R}$.

Lema 14.2.35. *Sea S un subespacio de $\mathbb{R}^n$ y $\overline{s}_1, \ldots, \overline{s}_k$ vectores linealmente independientes de S. Si $\overline{s} \in S$ es tal que $\overline{s} \notin \langle \overline{s}_1, \ldots, \overline{s}_k \rangle$, entonces $\overline{s}_1, \ldots, \overline{s}_k, \overline{s}$ son linealmente independientes*

Demostración. Supongamos que $\alpha_1\overline{s}_1 + \cdots + \alpha_k\overline{s}_k + \alpha\overline{s} = \overline{0}$. Mostraremos que la única posibilidad para que esto se dé es que $\alpha_1 = \cdots = \alpha_k = \alpha = 0$.
Si fuera $\alpha \neq 0$, entonces $\overline{s} = \frac{\alpha_1}{\alpha}\overline{s}_1 + \cdots + \frac{\alpha_k}{\alpha}\overline{s}_k$ y por lo tanto $\overline{s} \in \langle \overline{s}_1, \ldots, \overline{s}_k \rangle$ que contradice la hipótesis. Luego debe ser $\alpha = 0$ y entonces

$$\alpha_1\overline{s}_1 + \cdots + \alpha_k\overline{s}_k = \overline{0}.$$

Pero por ser $\overline{s}_1, \ldots, \overline{s}_k$ linealmente independientes concluimos que

$$\alpha_1 = \cdots = \alpha_k = 0 = \alpha.$$ ∎

Estamos ahora en condiciones de demostrar que cada subespacio de $\mathbb{R}^n$ tiene una base.

Proposición 14.2.36. *Cada subconjunto linealmente independiente de un subespacio S de R^n se puede extender a una base de S.*

Demostración. Sea $\{\overline{s}_1, \ldots, \overline{s}_k\}$ un subconjunto linealmente independiente de un subespacio $S \subseteq \mathbb{R}^n$. Si $\overline{s}_1, \ldots, \overline{s}_k$ generan a S, este conjunto será una base. Si $\langle \overline{s}_1, \ldots, \overline{s}_k \rangle \subsetneq S$, sea $\overline{s}_{k+1} \in S - \langle \overline{s}_1, \ldots, \overline{s}_k \rangle$. Luego por el lema 14.2.35 $\{\overline{s}_1, \ldots, \overline{s}_k, \overline{s}_{k+1}\}$ es linealmente independiente. Si este conjunto genera a S éste será una base de S, si no es así, tomamos $\overline{s}_{k+2} \in S - \langle \overline{s}_1, \ldots, \overline{s}_k, \overline{s}_{k+1} \rangle$ para obtener $\{\overline{s}_1, \ldots, \overline{s}_k, \overline{s}_{k+1}, \overline{s}_{k+2}\}$ linealmente independiente. Continuando con este proceso, debido a que no puede haber más de n elementos linealmente independientes (corolario 14.2.34), para alguna $t \geq 0$, se tendrá

$$\{\overline{s}_1, \ldots, \overline{s}_k, \overline{s}_{k+1}, \ldots, \overline{s}_{k+t}\}$$

linealmente independiente y $\langle \overline{s}_1, \ldots, \overline{s}_k, \overline{s}_{k+1}, \ldots, \overline{s}_{k+t} \rangle = S$ y por lo tanto será una base de S. ∎

Teorema 14.2.37. *Sea S un subespacio de $\mathbb{R}^n$. Entonces S tiene una base.*

Demostración. Si $S = \left\{\overline{0}\right\}$ ya hemos dicho que $\varnothing$ es una base, así que podemos suponer $S \neq \{0\}$.
Sea $\overline{s}_1 \in S$, $\overline{s}_1 \neq \overline{0}$. Entonces $\{\overline{s}_1\}$ es linealmente independiente y por la proposición 14.2.36, $\{\overline{s}_1\}$ se puede extender a una base de S. ∎

El siguiente resultado nos permitirá demostrar que cualesquiera dos bases en un subespacio tienen el mismo número de elementos.

Teorema 14.2.38. *Si $\overline{s}_1, \ldots, \overline{s}_m$ generan un subespacio S de $\mathbb{R}^n$, entonces más de m elementos en S son linealmente dependientes.*

Demostración. Basta considerar $m + 1$ elementos de S ya que la proposición 14.2.26 cualquier conjunto finito que contiene a un conjunto linealmente dependiente también lo es.
Haremos la demostración por inducción sobre m.

$1°/$ Supongamos que $S = \langle \overline{s} \rangle$ y sean $\overline{t}_1, \overline{t}_2 \in S$. Si al menos uno de los vectores es $\overline{0}$, sabemos por el ejemplo 14.2.21 (a) que son linealmente dependientes, así que podemos suponer que $\overline{t}_1 \neq \overline{0}$ y $\overline{t}_2 \neq \overline{0}$ en cuyo caso $\overline{t}_1 = \alpha_1 \overline{s}$ y $\overline{t}_2 = \alpha_2 \overline{s}$ donde $\alpha_1, \alpha_2 \in \mathbb{R} - \{0\}$. Entonces $\alpha_2 \overline{t}_1 - \alpha_1 \overline{t}_2 = \alpha_2 \alpha_1 \overline{s} - \alpha_1 \alpha_2 \overline{s} = \overline{0}$ con $\alpha_1 \neq 0$ y $\alpha_2 \neq 0$ y por lo tanto $\overline{t}_1$ y $\overline{t}_2$ son linealmente dependientes.
$2°/$ Supongamos cierto el resultado para $m-1 > 0$ y consideremos $S = \langle \overline{s}_1, \ldots, \overline{s}_m \rangle$ y $\overline{t}_1, \ldots, \overline{t}_{m+1} \in S$. Entonces

$$\begin{array}{rcccccc} \overline{t}_1 & = & a_{11}\overline{s}_1 & + & \cdots & + & a_{1m}\overline{s}_m \\ \vdots & & \vdots & & \vdots\vdots\vdots & & \vdots \\ \overline{t}_{m+1} & = & a_{(m+1)1}\overline{s}_1 & + & \cdots & + & a_{(m+1)m}\overline{s}_m \end{array}$$

Si $a_{im} = 0$ para toda $i = 1, \ldots, m+1$ se tendrá entonces que

$$\overline{t}_1, \ldots, \overline{t}_{m+1} \in \langle \overline{s}_1, \ldots, \overline{s}_{m-1} \rangle,$$

lo cual, por hipótesis de inducción, implica que $\overline{t}_1, \ldots, \overline{t}_{m+1}$ son linealmente dependientes. Ahora si algún $a_{im} \neq 0$, podemos suponer, sin pérdida de generalidad, que $a = a_{(m+1)m} \neq 0$.

Para cada $i = 1, \ldots, m$ sea $a_i = \frac{a_{im}}{a}$ y $\overline{t}_i{}' = \overline{t}_i - a_i\overline{t}_{m+1}$

$$\begin{aligned} \overline{t}_i{}' &= \overline{t}_i - a_i\overline{t}_{m+1} \\ &= a_{i1}\overline{s}_1 + \cdots + a_{i(m-1)}\overline{s}_{m-1} + a_{im}\overline{s}_m - a_i[a_{(m+1)1}\overline{s}_1 + \cdots + a_{(m+1)(m-1)}\overline{s}_{m-1} + a_{(m+1)m}\overline{s}_m] \\ &= (a_{i1} - a_i a_{(m+1)1})\overline{s}_1 + \cdots + (a_{i(m-1)} - a_i a_{(m+1)(m-1)})\overline{s}_{m-1} + \underbrace{(a_{im} - a_{im})}_{0}\overline{s}_m) \end{aligned}$$

Entonces $\overline{t}_1{}', \ldots, \overline{t}_m{}' \in \langle \overline{s}_1, \ldots, \overline{s}_{m-1} \rangle$. Luego por hipótesis de inducción, $\overline{t}_1{}', \ldots, \overline{t}_m{}'$ son linealmente dependientes y por lo tanto existen $\alpha_1, \ldots, \alpha_m \in \mathbb{R}$ no todos cero tales que $\alpha_1\overline{t}_1{}' + \cdots + \alpha_m\overline{t}_m{}' = \overline{0}$. De aquí obtenemos la combinación lineal igual a cero que buscamos ya que

$$\begin{aligned} \alpha_1\overline{t}_1 + \cdots + \alpha_m\overline{t}_m - (\alpha_1 a_1 + \cdots + \alpha_m a_m)\overline{t}_{m+1} &= \left(\overline{t}_1 - a_1\overline{t}_{m+1}\right) + \cdots + \alpha_m\left(\overline{t}_m - a_m\overline{t}_{m+1}\right) \\ &= \alpha_1\overline{t}_1{}' + \cdots + \alpha_m\overline{t}_m{}' \\ &= \overline{0} \end{aligned}$$

Esto significa que $\overline{t}_1, \ldots, \overline{t}_m, \overline{t}_{m+1}$ son linealmente dependientes. ■

Teorema 14.2.39. *Si $\overline{s}_1, \ldots, \overline{s}_m$ generan a un subespacio S de $\mathbb{R}^n$, entonces existe $\{\overline{s}_{i_1}, \ldots, \overline{s}_{i_k}\} \subseteq \{\overline{s}_1, \ldots, \overline{s}_m\}$ tal que $\{\overline{s}_{i_1}, \ldots, \overline{s}_{i_k}\}$ es una base de S.*

Demostración. Si $\{\overline{s}_1, \ldots, \overline{s}_m\}$ es linealmente independiente, entonces será base de S. En caso contrario, se tendrá una combinación lineal

$$\alpha_1\overline{s}_1 + \cdots + \alpha_m\overline{s}_m = \overline{0}$$

donde no todos los α_i's son cero. Podemos suponer que $\alpha_1 \neq 0$. Entonces $\overline{s}_1 = \frac{-\alpha_2}{\alpha_1}\overline{s}_2 + \cdots + \frac{-\alpha_m}{\alpha_1}\overline{s}_m$. Afirmamos que $\{\overline{s}_2, \ldots, \overline{s}_m\}$ genera a S. Sea $\overline{s} \in S$. Entonces por hipótesis, $\overline{s} = \beta_1\overline{s}_1 + \cdots + \beta_m\overline{s}_m$ y sustituyendo $\overline{s}_1$ obtenemos

$$\overline{s} = \beta_1\left(\frac{-\alpha_2}{\alpha_1}\overline{s}_2 + \cdots + \frac{-\alpha_m}{\alpha_1}\overline{s}_m\right) + \beta_2\overline{s}_2 + \cdots + \beta_m\overline{s}_m = \left(\frac{-\beta_1\alpha_2}{\alpha_1} + \beta_2\right)\overline{s}_2 + \cdots + \left(\frac{-\beta_1\alpha_m}{\alpha_1} + \beta_m\right)\overline{s}_m.$$

Si $\{\overline{s}_2, \ldots, \overline{s}_m\}$ es linealmente independiente, entonces será base de S, si no lo es repetimos el proceso y extraemos de este conjunto alguno que sea combinación

lineal de los restantes y el conjunto resultante seguirá generando a S. Finalmente continuando de la misma manera, llegaremos a una base $\{\overline{s}_{i_1}, \ldots, \overline{s}_{i_k}\}$ de S. ■

Teorema 14.2.40. *Cualesquiera dos bases de un subespacio S de $\mathbb{R}^n$ tienen el mismo número de elementos.*

Demostración. Sean $\{\overline{s}_1, \ldots, \overline{s}_m\}$ y $\{\overline{t}_1, \ldots, \overline{t}_k\}$ bases de S y supongamos que $m \leq k$. Veremos que la posibilidad $m < k$ no se puede dar.
Si $m < k$, como $\overline{s}_1, \ldots, \overline{s}_m$ generan a S por ser base y $\overline{t}_1, \ldots, \overline{t}_k \in S$, entonces por el teorema 14.2.40, $\overline{t}_1, \ldots, \overline{t}_k$ son linealmente dependientes, lo que no puede ser puesto que $\overline{t}_1, \ldots, \overline{t}_k$ son linealmente independientes por ser elementos de una base. Por lo tanto debe ser $m = k$. ■

Basándonos en este último teorema cada subespacio de $\mathbb{R}^n$ determina un único número natural entre 1 y n que es el número de elementos que tiene cualquier base. Daremos un nombre especial a este número.

Definición 14.2.41. *Sea S un subespacio de $\mathbb{R}^n$. Al número de elementos que tiene cualquier base de S se la llama la* **dimensión** *de S sobre $\mathbb{R}$.*

Notación 14.2.42. *A la dimensión de un subespacio S de $\mathbb{R}^n$ la denotamos por* $\mathbf{dim}_{\mathbb{R}}\, \boldsymbol{S}$.

Ejemplo 14.2.43.

(a) Como hemos convenido que $\varnothing$ es una base para $\left\{\overline{0}\right\}$, entonces $\dim_{\mathbb{R}} \left\{\overline{0}\right\} = 0$.
(b) $\dim_{\mathbb{R}} \mathbb{R}^n = n$. Esto es porque $\{(1, 0, \ldots, 0), (0, 1, \ldots, 0), \ldots, (0, 0, \ldots, 1)\}$ es un base de $\mathbb{R}^n$ (véase el ejemplo 14.2.32).
(c) Sea $S = \{(\alpha, \alpha, \beta, \beta) \mid \alpha, \beta \in \mathbb{R}\} \subseteq \mathbb{R}^4$. S es un subespacio de $\mathbb{R}^4$ (véase el ejercicio 14.2.4 (vi)) y $\{(1, 1, 0, 0), (0, 0, 1, 1)\}$ es una base para S:
(i) Sea $\overline{s} \in S$. Entonces $\overline{s} = (\alpha, \alpha, \beta, \beta) = \alpha(1, 1, 0, 0) + \beta(0, 0, 1, 1)$. Luego $S = \langle (1, 1, 0, 0), (0, 0, 1, 1) \rangle$.
(ii) $(1, 1, 0, 0)$ y $(0, 0, 1, 1)$ son linealmente independientes ya que si $\alpha(1, 1, 0, 0) + \beta(0, 0, 1, 1) = (0, 0, 0, 0)$, entonces $(\alpha, \alpha, \beta, \beta) = (0, 0, 0, 0)$ y por lo tanto $\alpha = \beta = 0$.
Luego $\dim_{\mathbb{R}} S = 2$.

Teorema 14.2.44. *Si S es un subespacio vectorial de $\mathbb{R}^n$, entonces* $\dim_{\mathbb{R}} S \leq n$ *y si* $\dim_{\mathbb{R}} S = n$, *entonces* $S = \mathbb{R}^n$.

Demostración. Si $\{\overline{s}_1, \ldots, \overline{s}_m\}$ es una base de S, entonces es un conjunto linealmente independiente en $\mathbb{R}^n$. Entonces por el corolario 142.28, debe ser $m \leq n$. Ahora supongamos que $m = n$. Si fuera $S \subsetneq \mathbb{R}^n$, existiría $\overline{s} \in \mathbb{R}^n$ tal que $\overline{s} \notin S$ y por lo tanto por el lema 14.2.35, sería $\{\overline{s}_1, \ldots, \overline{s}_m, \overline{s}\}$ linealmente independiente, lo que contradice el teorema 14.2.33. Luego $S = \mathbb{R}^n$. ∎

§ 14.3. Retorno a sistemas de ecuaciones lineales

Consideramos el sistema homogéneo de ecuaciones lineales

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = 0 \\ a_{21}x_1 + \cdots + a_{2n}x_n = 0 \\ \vdots \quad \vdots\vdots\vdots \quad \vdots \quad \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = 0 \end{cases}$$

En la sección 14.2 demostramos que el conjunto S de soluciones de este sistema es un subespacio de $\mathbb{R}^n$ y por lo tanto tiene una base, lo que significa que a S lo podemos describir a través de ella, es decir, si $\overline{s}_1, \ldots, \overline{s}_k$ es una base de S, entonces

$$S = \{\alpha_1\overline{s}_1 + \cdots + \alpha_k\overline{s}_k \mid \alpha_i \in \mathbb{R}, \text{ para } i = 1, \ldots, k\}.$$

Veamos algunos ejemplos para ilustrar esta situación.
Encontremos una base para el subespacio S de soluciones de los siguientes

Ejemplo 14.3.1.

$$\begin{cases} 2x_1 - 4x_2 + 3x_3 - 2x_4 + x_5 = 0 \\ x_1 - x_2 - x_3 + x_4 - 3x_5 = 0 \\ x_2 + 2x_3 - x_4 + x_5 = 0 \\ 3x_1 - x_2 + x_3 - 2x_4 - x_5 = 0 \end{cases}$$

Trabajamos con la matriz de coeficientes

$$\begin{pmatrix} 2 & -4 & 3 & -2 & 1 \\ 1 & -1 & -1 & 1 & -3 \\ 0 & 1 & 2 & -1 & 1 \\ 3 & -1 & 1 & -2 & -1 \end{pmatrix} \xrightarrow[R_1 \longleftrightarrow R_2]{} \begin{pmatrix} 1 & -1 & -1 & 1 & -3 \\ 2 & -4 & 3 & -2 & 1 \\ 0 & 1 & 2 & -1 & 1 \\ 3 & -1 & 1 & -2 & -1 \end{pmatrix} \xrightarrow[R_4-3R_1]{R_2-2R_1}$$

$$\begin{pmatrix} 1 & -1 & -1 & 1 & -3 \\ 0 & -2 & 5 & -4 & 7 \\ 0 & 1 & 2 & -1 & 1 \\ 0 & 2 & 4 & -5 & 8 \end{pmatrix} \xrightarrow[R_2 \longleftrightarrow R_3]{} \begin{pmatrix} 1 & -1 & -1 & 1 & -3 \\ 0 & 1 & 2 & -1 & 1 \\ 0 & -2 & 5 & -4 & 7 \\ 0 & 2 & 4 & -5 & 8 \end{pmatrix} \xrightarrow[R_3+2R_2]{R_1+R_2} \xrightarrow[R_4-2R_2]{}$$

$$\begin{pmatrix} 1 & 0 & 1 & 0 & -2 \\ 0 & 1 & 2 & -1 & 1 \\ 0 & 0 & 9 & -6 & 9 \\ 0 & 0 & 0 & -3 & 6 \end{pmatrix} \overset{\frac{1}{9}R_3}{\underset{-\frac{1}{3}R_4}{\sim}} \begin{pmatrix} 1 & 0 & 1 & 0 & -2 \\ 0 & 1 & 2 & -1 & 1 \\ 0 & 0 & 1 & -\frac{2}{3} & 1 \\ 0 & 0 & 0 & 1 & -2 \end{pmatrix} \overset{R_1-R_3}{\underset{R_2-2R_3}{\sim}}$$

$$\begin{pmatrix} 1 & 0 & 0 & \frac{2}{3} & -3 \\ 0 & 1 & 0 & \frac{1}{3} & -1 \\ 0 & 0 & 1 & -\frac{2}{3} & 1 \\ 0 & 0 & 0 & 1 & -2 \end{pmatrix} \overset{R_1-\frac{2}{3}R_4}{\underset{R_3+\frac{2}{3}R_4}{\underset{R_2-\frac{1}{3}R_4}{\sim}}} \begin{pmatrix} 1 & 0 & 0 & 0 & -\frac{5}{3} \\ 0 & 1 & 0 & 0 & -\frac{1}{3} \\ 0 & 0 & 1 & 0 & -\frac{1}{3} \\ 0 & 0 & 0 & 1 & -2 \end{pmatrix}$$

El sistema de ecuaciones lineales al que corresponde la última matriz es

$$\begin{cases} x_1 & & & & & - & \frac{5}{3}x_5 = 0 \\ & x_2 & & & & - & \frac{1}{3}x_5 = 0 \\ & & x_3 & & & - & \frac{1}{3}x_5 = 0 \\ & & & x_4 & & - & 2x_5 = 0 \end{cases}$$

Por cada valor que demos a x_5 obtenemos una solución del sistema de ecuaciones.
Para $x_5 = 1$, debe ser $x_1 = \frac{5}{3}, x_2 = \frac{1}{3}, x_3 = \frac{1}{3}$ y $x_4 = 2$.
Afirmamos que $\left(\frac{5}{3}, \frac{1}{3}, \frac{1}{3}, 2, 1\right)$ es una base del subespacio S de soluciones.

1°/ Evidentemente $\left(\frac{5}{3}, \frac{1}{3}, \frac{1}{3}, 2, 1\right)$ es linealmente independiente.
2°/ Sea $(a_1, a_2, a_3, a_4, a_5)$ una solución del sistema. Entonces

$$a_1 = \tfrac{5}{3}a_5, a_2 = \tfrac{1}{3}a_5, a_3 = \tfrac{1}{3}a_5, a_4 = 2a_5.$$

Luego $(a_1, a_2, a_3, a_4, a_5) = \left(\frac{5}{3}a_5, \frac{1}{3}a_5, \frac{1}{3}a_5, 2a_5, a_5\right) = a_5\left(\frac{5}{3}, \frac{1}{3}, \frac{1}{3}, 2, 1\right)$ y por lo tanto $\left(\frac{5}{3}, \frac{1}{3}, \frac{1}{3}, 2, 1\right)$ genera a S.

Entonces $S = \{\alpha\left(\frac{5}{3}, \frac{1}{3}, \frac{1}{3}, 2, 1\right) \mid \alpha \in \mathbb{R}\}$ y $\dim_{\mathbb{R}} S = 1$.

Ejemplo 14.3.2.

$$\begin{cases} x_1 + 2x_2 - 3x_3 + x_4 - x_5 = 0 \\ -2x_1 - 4x_2 + x_3 - x_4 + 2x_5 = 0 \\ 3x_1 + 6x_2 + 2x_3 + 3x_4 + x_5 = 0 \end{cases}$$

$$\begin{pmatrix} 1 & 2 & -3 & 1 & -1 \\ -2 & -4 & 1 & -1 & 2 \\ 3 & 6 & 2 & 3 & 1 \end{pmatrix} \overset{\substack{R_2+2R_1 \\ R_3-3R_1}}{\sim} \begin{pmatrix} 1 & 2 & -3 & 1 & -1 \\ 0 & 0 & -5 & 1 & 0 \\ 0 & 0 & 11 & 0 & 4 \end{pmatrix} \overset{-\frac{1}{5}R_2}{\sim}$$

$$\begin{pmatrix} 1 & 2 & -3 & 1 & -1 \\ 0 & 0 & 1 & -\frac{1}{5} & 0 \\ 0 & 0 & 11 & 0 & 4 \end{pmatrix} \overset{\substack{R_1+3R_2 \\ R_3-11R_2}}{\sim} \begin{pmatrix} 1 & 2 & 0 & \frac{2}{5} & -1 \\ 0 & 0 & 1 & -\frac{1}{5} & 0 \\ 0 & 0 & 0 & \frac{11}{5} & 4 \end{pmatrix} \overset{\frac{5}{11}R_3}{\sim}$$

$$\begin{pmatrix} 1 & 2 & 0 & \frac{2}{5} & -1 \\ 0 & 0 & 1 & -\frac{1}{5} & 0 \\ 0 & 0 & 0 & 1 & \frac{20}{11} \end{pmatrix} \overset{\substack{R_1-\frac{2}{5}R_3 \\ R_2+\frac{1}{5}R_3}}{\sim} \begin{pmatrix} 1 & 2 & 0 & 0 & -\frac{19}{11} \\ 0 & 0 & 1 & 0 & \frac{4}{11} \\ 0 & 0 & 0 & 1 & \frac{20}{11} \end{pmatrix}$$

El sistema de ecuaciones lineales es entonces

$$\begin{cases} x_1 + 2x_2 - \frac{19}{11}x_5 = 0 \\ x_3 + \frac{4}{11}x_5 = 0 \\ x_4 + \frac{20}{11}x_5 = 0 \end{cases}$$

Por cada valor que le demos a x_2 y x_5 obtenemos automáticamente los valores de x_1, x_3 y x_4, a saber $x_1 = \frac{19}{11}x_5 - 2x_2$, $x_3 = -\frac{4}{11}x_5$ y $x_4 = -\frac{20}{11}x_5$.
Consideremos las siguientes dos parejas de valores de x_2 y x_5: $x_2 = 1$, $x_5 = 0$ y $x_2 = 0$, $x_5 = 1$. Entonces para la primera pareja obtenemos $x_1 = -2$, $x_3 = 0$ y $x_4 = 0$ y para la segunda $x_1 = \frac{19}{11}$, $x_3 = -\frac{4}{11}$ y $x_4 = -\frac{20}{11}$. Esto es, $(-2, 1, 0, 0, 0)$ y $\left(\frac{19}{11}, 0, -\frac{4}{11}, -\frac{20}{11}, 1\right)$ son soluciones del sistema. Mostraremos que forman una base para S.

1°/ Son linealmente independientes:
$\alpha(-2, 1, 0, 0, 0) + \beta\left(\frac{19}{11}, 0, -\frac{4}{11}, -\frac{20}{11}, 1\right) = (0, 0, 0, 0)$ implica que

$$\begin{aligned} -2\alpha + \tfrac{19}{11}\beta &= 0 \\ \alpha + 0\beta &= 0 \\ 0\alpha - \tfrac{4}{11}\beta &= 0 \\ 0\alpha - \tfrac{20}{11}\beta &= 0 \\ 0\alpha + \beta &= 0 \end{aligned}$$

Donde de la segunda igualdad se tiene que $\alpha = 0$ y de la última $\beta = 0$.

2°/ $(-2, 1, 0, 0, 0)$ y $\left(\frac{19}{11}, 0, -\frac{4}{11}, -\frac{20}{11}, 1\right)$ generan a S:
Sea $\overline{s} = (a_1, a_2, a_3, a_4, a_5) \in S$. Entonces
$a_1 = \frac{19}{11}a_5 - 2a_2$, $a_3 = -\frac{4}{11}a_5$ y $a_4 = -\frac{20}{11}a_5$ por lo que

$\overline{s} = \left(\frac{19}{11}a_5 - 2a_2, a_2, -\frac{4}{11}a_5, -\frac{20}{11}a_5, a_5\right)$.
Encontremos α y β en $\mathbb{R}$ tales que

$$\left(\frac{19}{11}a_5 - 2a_2, a_2, -\frac{4}{11}a_5, -\frac{20}{11}a_5, a_5\right) = \alpha(-2,1,0,0,0) + \beta\left(\frac{19}{11}, 0, -\frac{4}{11}, -\frac{20}{11}, 1\right).$$

Esto da lugar a

$$\begin{array}{rcrcl} -2\alpha & + & \frac{19}{11}\beta & = & 0 \\ \alpha & + & 0\beta & = & a_2 \\ 0\alpha & - & \frac{4}{11}\beta & = & -\frac{4}{11}a_5 \\ 0\alpha & - & \frac{20}{11}\beta & = & -\frac{20}{11}a_5 \\ 0\alpha & + & \beta & = & a_5 \end{array}$$

y de estas llegamos a que $\alpha = a_2$ y $\beta = a_5$ satisfacen cada una de las igualdades. Entonces

$$\left(\frac{19}{11}a_5 - 2a_2, a_2, -\frac{4}{11}a_5, -\frac{20}{11}a_5, a_5\right) = a_2(-2,1,0,0) + a_5\left(\frac{19}{11}, 0, -\frac{4}{11}, -\frac{20}{11}, 1\right).$$

En este caso $\dim_{\mathbb{R}} S = 2$.

Ejemplo 14.3.3.

$$\begin{cases} 2x_1 + 3x_2 - 4x_3 + x_4 = 0 \\ x_1 - x_2 + 3x_3 - x_4 = 0 \\ x_1 + x_3 + 2x_4 = 0 \\ x_2 + x_3 + x_4 = 0 \\ x_1 - 2x_2 - 2x_3 + 3x_4 = 0 \\ x_1 - 3x_2 + 5x_3 - 4x_4 = 0 \end{cases}$$

$$\begin{pmatrix} 2 & 3 & -4 & 1 \\ 1 & -1 & 3 & -1 \\ 1 & 0 & 1 & 2 \\ 0 & 1 & 1 & 1 \\ 1 & -2 & -2 & 3 \\ 1 & -3 & 5 & -4 \end{pmatrix} \xrightarrow{R_1 \longleftrightarrow R_3} \begin{pmatrix} 1 & 0 & 1 & 2 \\ 1 & -1 & 3 & -1 \\ 2 & 3 & -4 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & -2 & -2 & 3 \\ 1 & -3 & 5 & -4 \end{pmatrix} \xrightarrow[R_3-2R_1]{R_2-R_1} \begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & -1 & 2 & -3 \\ 0 & 3 & -6 & -3 \\ 0 & 1 & 1 & 1 \\ 0 & -2 & -3 & 1 \\ 0 & -3 & 4 & -6 \end{pmatrix} \xrightarrow{(-1)R_2}$$

$$\begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & -2 & 3 \\ 0 & 3 & -6 & -3 \\ 0 & 1 & 1 & 1 \\ 0 & -2 & -3 & 1 \\ 0 & -3 & 4 & -6 \end{pmatrix} \xrightarrow[R_4-R_2]{R_3-3R_2} \begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & -2 & 3 \\ 0 & 0 & 0 & -12 \\ 0 & 0 & 3 & -2 \\ 0 & 0 & -7 & 7 \\ 0 & 0 & -2 & 3 \end{pmatrix} \xrightarrow{R_3 \longleftrightarrow R_6} \begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & -2 & 3 \\ 0 & 0 & -2 & 3 \\ 0 & 0 & 3 & -2 \\ 0 & 0 & -7 & 7 \\ 0 & 0 & 0 & -12 \end{pmatrix} \xrightarrow{\left(-\frac{1}{2}\right)R_3}$$

$$\begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & -2 & 3 \\ 0 & 0 & 1 & -\frac{3}{2} \\ 0 & 0 & 3 & -2 \\ 0 & 0 & -7 & 7 \\ 0 & 0 & 0 & -12 \end{pmatrix} \overset{\substack{R_1-R_3 \\ R_2+2R_3 \\ R_4-3R_3 \\ R_5+7R_3}}{\sim} \begin{pmatrix} 1 & 0 & 0 & \frac{7}{2} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -\frac{3}{2} \\ 0 & 0 & 0 & \frac{5}{2} \\ 0 & 0 & 0 & -\frac{7}{2} \\ 0 & 0 & 0 & -12 \end{pmatrix} \overset{(\frac{2}{5})R_4}{\sim} \begin{pmatrix} 1 & 0 & 0 & \frac{7}{2} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -\frac{3}{2} \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -\frac{7}{2} \\ 0 & 0 & 0 & -12 \end{pmatrix} \overset{\substack{R_1-\frac{7}{2}R_4 \\ R_3+\frac{3}{2}R_4 \\ R_5+\frac{7}{2}R_4 \\ R_6+12R_4}}{\sim}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

El sistema de ecuaciones es entonces

$$\begin{cases} x_1 = 0 \\ x_2 = 0 \\ x_3 = 0 \\ x_4 = 0 \end{cases}$$

Donde la única solución es la trivial, es decir, $S = \{(0,0,0,0,0)\}$ y $\dim_{\mathbb{R}} S = 0$.

Ejemplo 14.3.4.

$$\begin{cases} x_1 + 2x_2 - 3x_3 = 0 \\ 2x_1 - x_2 + x_3 = 0 \\ 3x_1 + x_2 - 2x_3 = 0 \\ -6x_1 + 3x_2 - 3x_3 = 0 \end{cases}$$

$$\begin{pmatrix} 1 & 2 & -3 \\ 2 & -1 & 1 \\ 3 & 1 & -2 \\ -6 & 3 & -3 \end{pmatrix} \overset{\substack{R_2-2R_1 \\ R_3-3R_1 \\ R_4+6R_1}}{\sim} \begin{pmatrix} 1 & 2 & -3 \\ 0 & -5 & 7 \\ 0 & -5 & 7 \\ 0 & 15 & -21 \end{pmatrix} \overset{\substack{R_3-R_2 \\ R_4+3R_2}}{\sim} \begin{pmatrix} 1 & 2 & -3 \\ 0 & -5 & 7 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \overset{-\frac{1}{5}R_2}{\sim} \begin{pmatrix} 1 & 2 & -3 \\ 0 & 1 & -\frac{7}{5} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\overset{R_1-2R_2}{\sim} \begin{pmatrix} 1 & 0 & -\frac{1}{5} \\ 0 & 1 & -\frac{7}{5} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

El sistema de ecuaciones es

$$\begin{cases} x_1 - \frac{1}{5}x_3 = 0 \\ x_2 - \frac{7}{5}x_3 = 0 \end{cases}$$

Para $x_3 = 1$, $\left(\frac{1}{5}, \frac{7}{5}, 1\right)$ es una solución del sistema que además es base de S.

1°/ Es claro que es linealmente independiente.

$2°/$ Si $(a_1, a_2, a_3) \in S$, entonces $a_1 = \frac{1}{5}a_3$ y $a_2 = \frac{7}{5}a_3$ y por lo tanto

$$(a_1, a_2, a_3) = a_3\left(\frac{1}{5}, \frac{7}{5}, 1\right)$$

así que $\left(\frac{1}{5}, \frac{7}{5}, 1\right)$ genera a S.

Luego $\dim_{\mathbb{R}} S = 1$.

Analizando estos cuatro ejemplos la parte que hay que destacar es que encontramos los elementos de una base para el subespacio S de soluciones de la siguiente manera: considerando la matriz escalonada reducida, si $x_{k_1}, \ldots, x_{k_j}$ son las indeterminadas (dependientes) correspondientes al primer elemento $\neq 0$ de cada renglón y $x_{\ell_1}, \ldots, x_{\ell_r}$ son las restantes, entonces para cada $i = 1, \ldots, r$ tomamos $x_{\ell_i} = 1$ y $x_{\ell_m} = 0$ para $m = 1, \ldots, r$ y $m \neq i$ con lo cual quedan determinados los valores de $x_{k_1}, \ldots, x_{k_j}$ y así tendremos r soluciones que forman una base de S. Además este número de soluciones es precisamente $n - j$ donde n es el número de indeterminadas y j el número de renglones distintos de cero de la matriz. Siguiendo esta idea tenemos

Teorema 14.3.5. *Sea*

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = 0 \\ a_{21}x_1 + \cdots + a_{2n}x_n = 0 \\ \vdots \quad \vdots\vdots\vdots \quad \vdots \quad \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = 0 \end{cases}$$

un sistema homogéneo de m ecuaciones lineales en n indeterminadas y sean A la matriz asociada a este sistema, B una matriz escalonada reducida equivalente a A y S el subespacio de soluciones. Entonces $\dim_{\mathbb{R}} S = n - j$ *donde j es el número de renglones distintos de cero de B.*

Demostración. Como en la demostración del teorema 14.1.17, consideramos el siguiente sistema que tiene a B como matriz de coeficientes

$$\begin{cases} x_{k_1} + \sum_{i=1}^{t} b_{1\ell_i}x_{\ell_i} = 0 \\ \vdots \qquad \vdots \qquad \vdots \\ x_{k_j} + \sum_{i=1}^{t} b_{j\ell_i}x_{\ell_i} = 0 \end{cases}$$

donde $t + j = n$ y $x_{k_1}, \ldots, x_{k_j}, x_{\ell_1}, \ldots, x_{\ell_t}$ son las indeterminadas $x_1, \ldots, x_n$ no necesariamente en ese orden. Recordamos que dando valores a $x_{\ell_1}, \ldots, x_{\ell_t}$ quedan determinadas automáticamente los valores de $x_{k_1}, \ldots, x_{k_j}$ y con esto obtenemos una solución del sistema. Definimos, para cada $r = 1, \ldots, t$, $\overline{s}_r = (\alpha_{r1}, \ldots, \alpha_{rn})$ donde

$$\alpha_{ri} = \begin{cases} 1 \text{ si } i = \ell_r \\ 0 \text{ si } i \neq \ell_r \text{ e } i \in \{\ell_1, \ldots \ell_t\} \\ -b_{u\ell_r} \text{ si } i = k_u,\ u = 1, \ldots, j \end{cases}$$

Entonces para $r = 1, \ldots, t$, $\overline{s}_r$ es solución del sistema ya que para toda $q = 1, \ldots, j$

$$\alpha_{rk_q} + \sum_{i=1}^{t} b_{q\ell_i}\alpha_{r\ell_i} = -b_{q\ell_r} + b_{q\ell_r} = 0$$

Afirmamos que $\{\overline{s}_1, \ldots, \overline{s}_t\}$ es una base de S.

1°/ $\overline{s}_1, \ldots, \overline{s}_t$ son linealmente independientes.
Sea $\beta_1\overline{s}_1 + \cdots + \beta_t\overline{s}_t = \overline{0}$. Para $r = 1, \ldots, t$ la coordenada ℓ_r de esta combinación lineal es $\beta_1 \cdot 0 + \cdots + \beta_r \cdot 1 + \cdots + \beta_t \cdot 0 = 0$ por lo que $\beta_1 = \beta_2 = \cdots = \beta_t = 0$.

2°/ $\overline{s}_1, \ldots, \overline{s}_t$ generan a S.
Sea $\overline{s} = (\gamma_1, \ldots, \gamma_n) \in S$. Entonces

$$\gamma_{k_1} + \sum_{h=1}^{t} b_{1\ell_h}\gamma_{\ell_h} = 0; \ldots; \ \gamma_{k_j} + \sum_{h=1}^{t} b_{j\ell_h}\gamma_{\ell_h} = 0$$

Esto es, $\gamma_{k_u} = -\sum_{h=1}^{t} b_{u\ell_h}\gamma_{\ell_h}$ para $u = 1, \ldots, j$.
Afirmamos que $\overline{s} = \gamma_{\ell_1}\overline{s}_1 + \cdots + \gamma_{\ell_j}\overline{s}_j$ y para ver esto sólo debemos verificar que las correspondientes coordenadas de ambos vectores de la igualdad son las mismas.
Recordamos que para cada $i = 1, \ldots, t$, la coordenada ℓ_i de $\overline{s}_r$ es 0 si $i \neq r$ y 1 si $i = r$ y para cada $u = 1, \ldots, j$ la coordenada k_u de $\overline{s}_r$ es $-b_{u\ell_r}$. Luego

	$\overline{s}$	$\gamma_{\ell_1}\overline{s}_1 + \cdots + \gamma_{\ell_j}\overline{s}_j$
coordenada ℓ_i	γ_{ℓ_i}	γ_{ℓ_i}
coordenada k_u	γ_{k_u}	$\gamma_{\ell_1}(-b_{u\ell_1})+\gamma_{\ell_2}(-b_{u\ell_2})+\cdots+\gamma_{\ell_t}(-b_{u\ell_t})=-\sum_{h=1}^{t} b_{u\ell_h}\gamma_{\ell_h}=\gamma_{k_u}$

donde $i = 1, \ldots, t$ y $u = 1, \ldots, j$

Con esto concluimos que $\dim_{\mathbb{R}} S = n - j$. ■

Ejemplo 14.3.6.

$$\begin{cases} 2x_1 - 3x_2 - 7x_3 + 5x_4 + 2x_5 = 0 \\ x_1 - 2x_2 - 4x_3 + 3x_4 + x_5 = 0 \\ 2x_1 - 4x_3 + 2x_4 + 2x_5 = 0 \\ x_1 - 5x_2 - 7x_3 + 6x_4 + x_5 = 0 \end{cases}$$

Encontraremos una base para el subespacio S de soluciones de este sistema homogéneo de ecuaciones.

$$\begin{pmatrix} 2 & -3 & -7 & 5 & 2 \\ 1 & -2 & -4 & 3 & 1 \\ 2 & 0 & -4 & 2 & 2 \\ 1 & -5 & -7 & 6 & 1 \end{pmatrix} \xrightarrow[R_1 \longleftrightarrow R_2]{} \begin{pmatrix} 1 & -2 & -4 & 3 & 1 \\ 2 & -3 & -7 & 5 & 2 \\ 2 & 0 & -4 & 2 & 2 \\ 1 & -5 & -7 & 6 & 1 \end{pmatrix} \xrightarrow[\substack{R_3-2R_1 \\ R_4-R_1}]{R_2-2R_1} \begin{pmatrix} 1 & -2 & -4 & 3 & 1 \\ 0 & 1 & 1 & -1 & 0 \\ 0 & 4 & 4 & -4 & 0 \\ 0 & -3 & -3 & 3 & 0 \end{pmatrix} \xrightarrow[\substack{R_3-4R_2 \\ R_4+3R_2}]{R_1+2R_2}$$

$$\begin{pmatrix} 1 & 0 & -2 & 1 & 1 \\ 0 & 1 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Entonces el sistema de ecuaciones equivalente al inicial es

$$\begin{cases} x_1 - 2x_3 + x_4 + x_5 = 0 \\ x_2 + x_3 - x_4 = 0 \end{cases}$$

Las variables independientes serán x_3, x_4, x_5 y para las variables dependientes se tiene que $x_1 = 2x_3 - x_4 - x_5$; $x_2 = -x_3 + x_4$.
Dando los siguientes valores a x_3, x_4 y x_5 obtenemos una base para S:
$x_3 = 1, x_4 = 0, x_5 = 0$; $x_3 = 0, x_4 = 1, x_5 = 0$; $x_3 = 0, x_4 = 0, x_5 = 1$.
Luego $\overline{s}_1 = (2, -1, 1, 0, 0), \overline{s}_2 = (-1, 1, 0, 1, 0)$ y $\overline{s}_3 = (-1, 0, 0, 0, 1)$ conforman dicha base, por lo que

$$S = \{\alpha\overline{s}_1 + \beta\overline{s}_2 + \gamma\overline{s}_3 \mid \alpha, \beta, \gamma \in \mathbb{R}\} = \{(2\alpha - \beta - \gamma, -\alpha + \beta, \alpha, \beta, \gamma) \mid \alpha, \beta, \gamma \in \mathbb{R}\}.$$

Pasamos ahora al caso general de un sistema no-homogéneo de ecuaciones lineales. En el caso en que el sistema tiene solución, en la sección 14.1 exhibimos una manera de encontrar al menos una lo que veremos es que con eso basta ya que las restantes las obtenemos con esta solución encontrada y el conjunto de soluciones de un sistema homogéneo asociado cuya definición damos a continuación.

Definición 14.3.7. *Dado el sistema no-homogéneo de ecuaciones lineales*

$$\left\{\begin{array}{rcccl} a_{11}x_1 + & \cdots & + a_{1n}x_n & = & b_1 \\ a_{21}x_1 + & \cdots & + a_{2n}x_n & = & b_2 \\ \vdots & \vdots\vdots\vdots & \vdots & & \vdots \\ a_{m1}x_1 + & \cdots & + a_{mn}x_n & = & b_m \end{array}\right.$$

su sistema homogéneo asociado es el siguiente

$$\left\{\begin{array}{rcccl} a_{11}x_1 + & \cdots & + a_{1n}x_n & = & 0 \\ a_{21}x_1 + & \cdots & + a_{2n}x_n & = & 0 \\ \vdots & \vdots\vdots\vdots & \vdots & & \vdots \\ a_{m1}x_1 + & \cdots & + a_{mn}x_n & = & 0 \end{array}\right.$$

Teorema 14.3.8. *Supongamos que el sistema no-homogéneo de ecuaciones lineales*

$$\left\{\begin{array}{rcccl} a_{11}x_1 + & \cdots & + a_{1n}x_n & = & b_1 \\ a_{21}x_1 + & \cdots & + a_{2n}x_n & = & b_2 \\ \vdots & \vdots\vdots\vdots & \vdots & & \vdots \\ a_{m1}x_1 + & \cdots & + a_{mn}x_n & = & b_m \end{array}\right.$$

tiene al menos una solución. Sean S' el conjunto de todas las soluciones, $\overline{s}_0$ una solución particular (cualquiera) y S el conjunto de soluciones del sistema homogéneo asociado. Entonces

$$S' = \overline{s}_0 + S = \{\overline{s}_0 + \overline{s} \mid \overline{s} \in S\}.$$

Demostración. Sea $\overline{s}_0 = (\alpha_1, \ldots, \alpha_n)$. Entonces $a_{i1}\alpha_1 + \cdots + a_{in}\alpha_n = b_i$ para toda $i = 1, \ldots, m$.

$1^\circ/$ $\overline{s}_0 + S \subseteq S'$

Sea $\overline{s}_1 \in \overline{s}_0 + S$, esto es, $\overline{s}_1 = \overline{s}_0 + \overline{s}$, donde $\overline{s} = (\beta_1, \ldots, \beta_n) \in S$, esto es

$$a_{i1}\beta_1 + \cdots + a_{in}\beta_n = 0$$

para toda $i = 1, \ldots, m$. $\overline{s}_1 = (\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n)$ es solución del sistema no-homogéneo;

$$a_{i1}(\alpha_1 + \beta_1) + \cdots + a_{in}(\alpha_n + \beta_n) = (a_{i1}\alpha_1 + \cdots + a_{in}\alpha_n) + (a_{i1}\beta_1 + \cdots + a_{in}\beta_n) = b_i + 0 = b_i$$

para toda $i = 1, \ldots, m$, y por lo tanto $\overline{s}_1 \in S'$.

$2°/$ $S' \subseteq \overline{s}_0 + S$
Sea $\overline{s}\,' = (\gamma_1, \ldots, \gamma_n) \in S'$. Entonces $a_{i1}\gamma_1 + \cdots + a_{in}\gamma_n = b_i$ para toda $i = 1, \ldots, m$. Luego $\overline{s} = \overline{s}\,' - \overline{s}_0 = (\alpha_1 - \gamma_1, \ldots, \alpha_n - \gamma_n) \in S$ puesto que para toda $i = 1, \ldots, m$ se tiene que

$$a_{i1}(\alpha_1 - \gamma_1) + \cdots + a_{in}(\alpha_n - \gamma_n) = (a_{i1}\alpha_1 + \cdots + a_{in}\alpha_n) - (a_{i1}\gamma_1 + \cdots + a_{in}\gamma_n) = b_i - b_i = 0.$$

Por lo tanto $\overline{s}\,' = \overline{s}_0 + \overline{s} \in \overline{s}_0 + S$. ∎

Este último teorema dice entonces que podemos describir <u>todas</u> las soluciones de un sistema no homogéneo de ecuaciones lineales mediante un número finito de soluciones: Si $\overline{s}_0$ es una solución particular del sistema no-homogéneo y $\overline{s}_1, \ldots, \overline{s}_t$ es una base del espacio de soluciones de su sistema homogéneo asociado, entonces

$$S' = \{\overline{s}_0 + \alpha_1\overline{s}_1 + \cdots + \alpha_t\overline{s}_t \mid \alpha_i \in \mathbb{R} \text{ para } i = 1, \ldots, t\}.$$

Ejemplo 14.3.9. Consideremos el siguiente sistema no-homogéneo de ecuaciones lineales

$$\begin{cases} 2x_1 - 3x_2 - 7x_3 + 5x_4 + 2x_5 = 0 \\ x_1 - 2x_2 - 4x_3 + 3x_4 + x_5 = 1 \\ 2x_1 - 4x_3 + 2x_4 + 2x_5 = -6 \\ x_1 - 5x_2 - 7x_3 + 6x_4 + x_5 = -2 \end{cases}$$

y encontremos todas sus soluciones (si existen). La matriz aumentada y la matriz de coeficientes son respectivamente

$$\begin{pmatrix} 2 & -3 & -7 & 5 & 2 & 0 \\ 1 & -2 & -4 & 3 & 1 & 1 \\ 2 & 0 & -4 & 2 & 2 & -6 \\ 1 & -5 & -7 & 6 & 1 & -2 \end{pmatrix}, \quad \begin{pmatrix} 2 & -3 & -7 & 5 & 2 \\ 1 & -2 & -4 & 3 & 1 \\ 2 & 0 & -4 & 2 & 2 \\ 1 & -5 & -7 & 6 & 1 \end{pmatrix}$$

Observamos que el sistema homogéneo asociado es el mismo que el del ejemplo 14.3.6, así que realizando las mismas operaciones elementales sobre renglones en la matriz aumentada, la matriz escalonada reducida equivalente a ésta será

$$\begin{pmatrix} 1 & 0 & -2 & 1 & 1 & -3 \\ 0 & 1 & 1 & -1 & 0 & -2 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

El sistema de ecuaciones lineales equivalente al inicial es entonces

$$\begin{cases} x_1 - 2x_3 + x_4 + x_5 = -3 \\ x_2 + x_3 - x_4 = -2 \end{cases}$$

Nota 14.3.10. Aquí hemos omitido las ecuaciones correspondientes al tercer y cuarto renglón de la matriz ya que como hemos comentado resulta irrelevante ya que sin importar los valores que tomen $x_1, \ldots, x_5$, siempre se tendrá $0 \cdot x_1 + 0 \cdot x_2 + 0 \cdot x_3 + 0 \cdot x_4 + 0 \cdot x_5 = 0$.

Considerando $x_3 = x_4 = x_5 = 0$, obtenemos $x_1 = -3$ y $x_2 = -2$, por lo que $(-3, -2, 0, 0, 0)$ es una solución particular del sistema y por lo tanto el conjunto S de todas las soluciones de éste está dado por

$$S = \{(-3, -2, 0, 0, 0) + \alpha\overline{s}_1 + \beta\overline{s}_2 + \gamma\overline{s}_3 \mid \alpha, \beta, \gamma \in \mathbb{R}\} =$$

$$\{(-3 + 2\alpha - \beta - \gamma, -2 - \alpha + \beta, \alpha, \beta, \gamma) \mid \alpha, \beta, \gamma \in \mathbb{R}\}$$

Véase el ejemplo 14.3.6.

§ § Ejercicios sección 14.1.

14.1.1. Demuestre que la relación dada en la definición 14.1.10 (pág. 487), es de equivalencia.

14.1.2. En cada uno de los siguientes casos encuentre una matriz escalonada reducida equivalente a la matriz dada.

$$(a)\begin{pmatrix} -1 & 0 & 0 & 1 \\ 2 & 2 & -1 & -1 \\ -2 & 2 & -1 & 3 \\ 1 & -2 & 0 & -1 \\ 2 & 3 & 1 & 0 \end{pmatrix} \qquad (b)\begin{pmatrix} 1 & -2 & 1 & 2 & 1 \\ 1 & 1 & -1 & 1 & 2 \\ 1 & 7 & -5 & -1 & 3 \end{pmatrix}$$

$$(c)\begin{pmatrix} 7 & 2 & -1 & -1 & 3 \\ 2 & -1 & 1 & 0 & 0 \\ -1 & 3 & 0 & -1 & 1 \\ 2 & 2 & 3 & 3 & 4 \end{pmatrix}$$

14.1.3. Suponga que las matrices dadas en el ejercicio 1.2 son las matrices asociadas de un sistema de ecuaciones lineales. En cada caso dé el sistema de ecuaciones y el correspondiente a la matriz asociada reducida que se encontró. Diga cuál de ellas tiene solución y para estas encuentre todas las soluciones.

14.1.4. Demuestre que el siguiente sistema de ecuaciones tiene una única solución y diga cuál es esta solución

$$\begin{cases} & 3x_2 & & - & 4x_4 = -1 \\ x_1 + & x_2 - & x_3 & & = 1 \\ 4x_1 + & 3x_2 & & - & x_4 = 6 \\ x_1 - & x_2 + & x_3 - & & x_4 = 0 \end{cases}$$

14.1.5. Describa cómo son todas las matrices escalonadas reducidas de orden 3×3.

14.1.6. Considere el sistema de 3 ecuaciones lineales con dos 2 incógnitas

$$(A) \begin{cases} 5x - 2y = 1 \\ -x + 2y = 2 \\ 4x + 2y = 9 \end{cases}$$

Al sustituir la segunda y tercera ecuación por la suma de ellas se obtiene el sistema

$$(B) \begin{cases} 5x - 2y = 1 \\ 3x + 4y = 11 \end{cases}$$

Demuestre que toda solución del sistema (A) es también solución del sistema (B). Es decir, compruebe que el conjunto solución del sistema (A) es un subconjunto del conjunto solución del sistema (B). ¿Es válida también la otra contención? ¿Son (A) y (B) sistemas equivalentes? Explique.

14.1.7. Determine en cada caso si los elementos del conjunto S dado son soluciones del sistema correspondiente.

1) $\begin{cases} 2x_1 - x_2 = 3 \\ x_1 + 3x_2 = 5 \end{cases}$, $S = \{(1,-1),(2,1)\}$.

2) $\begin{cases} x_1 - 2x_2 + x_3 - 3x_4 = -2 \\ 2x_1 + x_2 - x_3 + 2x_4 = -1 \\ x_1 + 3x_2 - 2x_3 + 5x_4 = 1 \end{cases}$, $S = \{(1,7,8,-1),(3,3,1,0),(2,9,14,0)\}$.

3) $\begin{cases} x_1 + 2x_2 - x_3 = 2 \\ 2x_1 + 3x_2 + 5x_3 = 5 \\ -x_1 - 3x_2 + 8x_3 = -1 \end{cases}$, $S = \{(4-13t,-2+7t,t) \mid t \in \mathbb{R}\}$.

14.1.8. Prueba que $(1,2,\ldots,n)$ es solución de

$$\begin{cases} 2x_1 + 2x_2 + \ldots + 2x_n = n^2 + n \\ -2x_1 + 2x_2 - \ldots + 2x_n = n \end{cases} \quad (n \text{ par})$$

14.1.9. Diga si los siguientes sistemas de ecuaciones lineales definidos sobre el campo $\mathbb{R}$ son equivalentes, justificando su respuesta.

(*i*) $\begin{cases} x_1 - x_2 = 0 \\ 2x_1 + x_2 = 0 \end{cases}$ y $\begin{cases} 3x_1 + x_2 = 0 \\ x_1 + x_2 = 0 \end{cases}$.

(*ii*) $\begin{cases} x_1 + - x_3 = 0 \\ x_2 + 3x_3 = 0 \end{cases}$ y $\begin{cases} -x_1 + x_2 + 4x_3 = 0 \\ x_1 + 3x_2 + 8x_3 = 0 \\ \frac{1}{2}x_1 + x_2 + \frac{5}{2}x_3 = 0 \end{cases}$.

(*iii*) $\begin{cases} 2x_1 - x_2 + x_3 = 2 \\ x_1 + 3x_2 + 4x_3 = 0 \end{cases}$ y $\begin{cases} -7x_1 + - 7x_3 = -6 \\ x_1 + \frac{13}{2}x_2 + \frac{15}{2}x_3 = -1 \end{cases}$.

14.1.10. Sea

$$A = \begin{pmatrix} 1 & 2 & -4 & -4 & 5 \\ 2 & 4 & 0 & 0 & 2 \\ 2 & 3 & 2 & 1 & 5 \\ -1 & 1 & 3 & 6 & 5 \end{pmatrix}.$$

Realice la siguiente secuencia de operaciones elementales con renglones sobre la matriz A.

$$R_2 - 2R_1, R_3 - 2R_1, R_4 + R_1, R_2 \longleftrightarrow R_3, R_4 + 3R_2, \left(\tfrac{1}{8}\right) R_2, R_4 - 29R_3.$$

14.1.11. ¿Cuál es la operación elemental con renglones que "deshace" cada una de las tres operaciones elementales con renglones $R_i \longleftrightarrow R_j$, αR_i, $R_i + \alpha R_j$?

14.1.12. Considere las matrices

$$A = \begin{pmatrix} 2 & 0 & -1 \\ 1 & 1 & 0 \\ -1 & 1 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 3 & 1 & -1 \\ 3 & 5 & 1 \\ 2 & 2 & 0 \end{pmatrix}.$$

Demuestre que B se obtiene de A mediante un número finito de operaciones elementales sobre los renglones, es decir, A y B son matrices equivalentes.

14.1.13. ¿Qué está mal con la siguiente "demostración" de que toda matriz con al menos dos renglones es equivalente por renglones a una matriz con un renglón de ceros?

> **Demostración**. Realice $R_2 + R_1$ y $R_1 + R_2$. Ahora los renglones 1 y 2 son idénticos. Ahora realice $R_2 - R_1$ para obtener un renglón de de ceros en el segundo renglón?

14.1.14. Considere la matriz $A = \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix}$. Muestre que cualquiera de los tres tipos de operaciones elementales con renglones puede usarse para crear un 1 en la parte superior de la primera columna. ¿Cuál prefiere y por qué?

14.1.15. Considere la matriz $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ con coeficientes reales. Supóngase que A es una matriz escalonada reducida por renglones y que $a + b + c + d = 0$. Demuestre que existen exactamente dos de estas matrices.

14.1.16. Los estudiantes frecuentemente realizan el siguiente tipo de cálculo para introducir un cero en una matriz:

$$\begin{pmatrix} 3 & 1 \\ 2 & 4 \end{pmatrix} \underset{3R_2-2R_1}{\sim} \begin{pmatrix} 3 & 1 \\ 0 & 10 \end{pmatrix}$$

Sin embargo, $3R_2-2R_1$ no es una operación elemental con renglones. ¿Por qué no? demuestre cómo lograr el mismo resultado usando operaciones elementales con renglones.

14.1.17. Cada una de las siguientes matrices es la matriz aumentada de un sistema de ecuaciones lineales.

$$(a)\begin{pmatrix} 3 & -2 & 0 & 1 & 0 \\ 1 & 2 & -3 & 8 & 1 \\ 0 & 0 & 0 & 0 & 5 \end{pmatrix} (b)\begin{pmatrix} 1 & 2 & 3 & 4 & 0 \\ 5 & 6 & 7 & 8 & 0 \\ 9 & 10 & 11 & 12 & 0 \end{pmatrix} (c)\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 3 & 1 \\ 0 & 0 & 1 & 2 \end{pmatrix}$$

$$(d)\begin{pmatrix} 5 & 7 & 0 & 1 \\ 0 & 2 & -3 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

(1) Escriba el sistema correspondientes a cada matriz.
(2) Determine por inspección (esto es; sin realizar cálculo alguno) si el sistema lineal asociado a la matriz aumentada dada tiene
   (*i*) una solución única,
   (*ii*) un número infinito de soluciones o
   (*iii*) ninguna solución. Justifique sus respuestas.

14.1.18. Considere el siguiente sistema de ecuaciones lineales

$$(*)\quad \begin{cases} x_1 + x_2 - x_4 = 0 \\ x_1 + x_3 - x_4 = k \\ -x_1 + x_2 - 2x_3 + x_4 = -4 \end{cases}$$

(*a*) Para qué valor(es) de k el sistema $(*)$ tiene solución.
(*b*) Encuentre el conjunto solución del sistema $(*)$ para los valores determinados en el inciso (*a*).

14.1.19. Utilice la técnica de obtener una matriz escalonada reducida por renglones para decir si los siguientes sistemas de ecuaciones lineales tienen solución y, si sí, dé las soluciones.

1) $\begin{cases} x_1 - x_2 - x_3 + 2x_4 = 1 \\ 2x_1 - 2x_2 - x_3 + 3x_4 = 3 \\ -x_1 + x_2 - x_3 = -3 \end{cases}$ 2) $\begin{cases} x + 2y = -1 \\ x + y + z = 1 \\ -x + y - z = -1 \end{cases}$

3) $\begin{cases} x + 2y - 3z = 9 \\ 2x - y - z = 0 \\ 4x - y - z = 4 \end{cases}$ 4) $\begin{cases} \frac{1}{2}x + y - z - 6u = 0 \\ \frac{1}{6}x + \frac{1}{2}y - 3u + w = 0 \\ \frac{1}{3}x - 2z - 4w = 0 \end{cases}$

5) $\begin{cases} -x + z = -2 \\ 2x - y + z = 1 \\ -3x + 2y - 2z = -1 \\ x - 2y + 3z = -2 \\ 5x + 2y + 6z = -1 \end{cases}$ 6) $\begin{cases} x_1 + 2x_3 - 2x_4 = 1 \\ -x_1 + x_2 + x_4 = -2 \\ x_2 + 2x_3 - x_4 = 1 \end{cases}$

7) $\begin{cases} x - 2y + z + w = 0 \\ 3x + 2z - 2w = 0 \\ 4y - z - w = 0 \\ 5x + 3z - w = 0 \end{cases}$ 8) $\begin{cases} x - 2y + z + 4w = -1 \\ 2x + y - z - 5w = -6 \\ x - y + z + 2w = 0 \\ x + y + 2z - w = 5 \end{cases}$

9) $\begin{cases} x + y + 3z - 2u - w = 1 \\ 5x - 2y + 3z + 7u + 8w = 3 \\ -3x - y + 2z + 7u + 5w = 2 \\ 5x + 3y + z - 2u - 7w = 3 \end{cases}$

14.1.20. Considere los siguientes sistemas de ecuaciones lineales.

1) $\begin{cases} kx_1 + x_2 = -2 \\ 2x_1 - 2x_2 = 4 \end{cases}$ 2) $\begin{cases} x_1 + kx_2 = 1 \\ kx_1 + x_2 = 1 \end{cases}$

3) $\begin{cases} x_1 + x_2 + kx_3 = 1 \\ x_1 + kx_2 + x_3 = 1 \\ kx_1 + x_2 + x_3 = -2 \end{cases}$ 4) $\begin{cases} x_1 + x_2 + x_3 = 2 \\ x_1 + 4x_2 - x_3 = k \\ 2x_1 - x_2 + 4x_3 = k^2 \end{cases}$

¿Para qué valor(es) de k, si hay alguno, los sistemas tendrán
(a) ninguna solución, (b) una solución única,
(c) un número infinito de soluciones?

14.1.21. Resuelva los siguientes sistemas de ecuaciones lineales con las matrices aumentadas dadas.

$a)$ $\begin{pmatrix} 1 & -1 & -2 & 2 & -7 \\ -2 & 2 & 0 & 2 & -2 \\ -1 & 1 & 1 & -2 & 6 \\ -2 & 2 & -1 & 2 & -3 \end{pmatrix}$ $b)$ $\begin{pmatrix} 0 & 2 & -2 & -2 & 10 \\ -2 & -2 & 2 & 2 & -2 \\ -1 & -1 & 0 & 0 & 3 \\ -1 & -1 & 1 & -2 & -1 \end{pmatrix}$

$c)$ $\begin{pmatrix} -1 & 0 & 1 & 1 & -1 & -1 \\ 0 & 1 & 0 & -1 & -1 & 0 \\ 0 & 1 & -1 & -1 & 1 & -6 \\ 0 & 1 & 1 & -1 & 0 & 3 \\ 1 & -1 & -1 & 0 & 1 & 2 \end{pmatrix}$ $d)$ $\begin{pmatrix} 0 & -1 & -1 & -1 & -1 & 8 \\ 0 & 0 & -1 & -1 & 1 & 1 \\ -1 & 1 & -1 & 0 & -1 & -2 \\ 0 & 1 & 0 & 0 & 1 & -5 \\ -1 & 1 & -1 & 1 & 0 & -3 \end{pmatrix}$

14.1.22. En cada uno de los siguientes incisos, dé un ejemplo de un sistema de ecuaciones lineales en 3 indeterminadas que tenga la propiedad indicada o explique por qué tal sistema no puede existir.

(1) El sistema es homogéneo y el conjunto $\{(0, 0, 0)\}$ es su conjunto solución.
(2) El sistema es homogéneo y el conjunto $\{(1, 1, 3)\}$ es su conjunto solución.
(3) El conjunto $\{(1, 1, 3)\}$ es el conjunto solución del sistema.
(4) El sistema es homogéneo y el conjunto $\{(2t, t, -t) \mid t \in \mathbb{R}\}$ es su conjunto solución.
(5) El sistema es homogéneo y el conjunto $\{(1 + 2t, 2 + t, 1 - t) \mid t \in \mathbb{R}\}$ es su conjunto solución.

14.1.23. Proporcione ejemplos de sistemas homogéneos de m ecuaciones lineales con n indeterminadas con $m = n$ y con $m > n$ que tengan

(a) un número infinito de soluciones y
(b) una solución única.

14.1.24. Construya un sistema de ecuaciones lineales no homogéneo que tenga la matriz de coeficientes

$$A = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 2 \\ 0 & 1 & -1 \end{pmatrix}$$

y la solución particular $(1, -1, 4)$.

14.1.25. Demuestre que toda matriz puede llevarse a una ÚNICA matriz escalonada reducida mediante un número finito de operaciones elementales sobre renglones.

§ § Ejercicios sección 14.2.

14.2.1. Demuestre el teorema 14.2.2.

14.2.2. Demuestre que

(1) $\overline{0} = (0, 0, \ldots, 0) \in \mathbb{R}^n$ es el único elemento en $\mathbb{R}^n$ con la propiedad $\overline{s} + \overline{0} = \overline{s}$ para todo $\overline{s} \in \mathbb{R}^n$.
(2) Dado $\overline{s} \in \mathbb{R}^n$, existe un único $\overline{s}' \in \mathbb{R}^n$ tal que $\overline{s} + \overline{s}' = \overline{0}$.

14.2.3. Sea V un conjunto y K un campo. Suponga que en V se tiene definida una operación binaria a la que llamaremos suma y $\varphi : K \times V \longrightarrow V$ una función donde $\varphi(\alpha, v)$ lo denotamos por $\alpha \cdot v$ y a la que llamaremos el producto por escalares (a los elementos de K les llamamos escalares). Se dice que V es un espacio vectorial sobre K si para cualesquiera $v, v', v'' \in V$ y $\alpha, \beta \in K$ se satisface

(1) $(v + v') + v'' = v + (v' + v'')$
(2) $v + v' = v' + v$
(3) Existe $v_0 \in V$ tal que $v + v_0 = v_0 + v = v$
(4) Existe $u \in V$ tal que $v + u = v_0$
(5) $(\alpha + \beta) \cdot v = \alpha \cdot v + \beta \cdot v$
(6) $\alpha \cdot (v + v') = \alpha \cdot v + \alpha \cdot v'$
(7) $(\alpha\beta) \cdot v = \alpha \cdot (\beta \cdot v)$
(8) $1 \cdot v = v$ donde 1 es el neutro multiplicativo de K.

Demuestre que las siguientes afirmaciones son válidas en un espacio vectorial V sobre un campo K

(*i*) El vector v_0 del inciso (3) es único.
(*ii*) El vector u del inciso (4) es único.
(*iii*) Sean $v, v'v, v'' \in V$ tal que $v + v' = v + v''$. Entonces $v' = v''$.
(*iv*) $0 \cdot v = v_0$ para toda $v \in V$.
(*v*) $\alpha \cdot v_0 = v_0$ para toda $\alpha \in K$.
(*vi*) $\alpha \cdot v = v_0$ si y sólo si $\alpha = 0$ o $v = v_0$.
(*vii*) Sean $v, u \in V$ tal que $v + u = v_0$. Entonces $u = (-1) \cdot v$
(*viii*) $\alpha \cdot (v - v') = \alpha \cdot v - \alpha \cdot v'$

En general al vector v_0 del inciso (3) de la definición de espacio vectorial se le denota por $\overline{0}$, que por (*i*) sabemos que es único, en el estudio de que $\overline{0}$ es el vector de V que satisface $v + \overline{0} = \overline{0} + v = v$ para toda $v \in V$ y la naturaleza de $\overline{0}$ dependerá únicamente de V y la propiedad que lo caracteriza. Análogamente a u del inciso (4), que por (*ii*) es único, se le denota por $-v$.

14.2.4. Sean $\overline{s}_1, \ldots, \overline{s}_m \in \mathbb{R}^n$ linealmente independientes. Demostrar que si $r_1\overline{s}_1 + \cdots + r_m\overline{s}_m = r'_1\overline{s}_1 + \cdots + r'_m\overline{s}_m$, donde $r_i, r'_i \in \mathbb{R}$, para $i = 1, \ldots, m$, entonces $r_i = r'_i$ para toda $i = 1, \ldots, m$.

14.2.5. En cada uno de los siguientes incisos diga si S es un subespacio de $\mathbb{R}^n$. En caso afirmativo demuéstrelo y si no es subespacio diga porqué.

(*i*) $S = \{(a, b, 0) \mid a, b \in \mathbb{R}\ texty\ a + b = 0\} \subseteq \mathbb{R}^3$.

(*ii*) $S = \{(x, y, z, w) \mid x, y, z, w \in \mathbb{R}\ texty\ 3x - 2y + 2z - w = 0\} \subseteq \mathbb{R}^4$.

(*iii*) Considere el sistema de ecuaciones lineales

$$\left\{\begin{array}{ccccc} a_{11}x_1 + & \cdots & + a_{1n}x_n & = & b_1 \\ a_{21}x_1 + & \cdots & + a_{2n}x_n & = & b_2 \\ \vdots & \vdots\vdots\vdots & \vdots & & \vdots \\ a_{m1}x_1 + & \cdots & + a_{mn}x_n & = & b_m \end{array}\right.$$

y sea $S \subseteq \mathbb{R}^n$ el conjunto de soluciones del sistema. Diga exactamente cuándo S es un subespacio de $\mathbb{R}^n$.

(*iv*) $S = S' + S'' \subseteq \mathbb{R}^n$, donde S' y S'' son subespacios de $\mathbb{R}^n$ y $S' + S'' = \{\overline{s}' + \overline{s}'' \mid \overline{s}' \in S \text{ y } \overline{s}'' \in S''\}$.

(*v*) $S = \{(a, b, c, 1) \mid a, b, c \in \mathbb{R}\} \subseteq \mathbb{R}^4$.

(*vi*) $S = \{(r, r, r', r') \mid r, r' \in \mathbb{R}\} \subseteq \mathbb{R}^4$.

14.2.6. Sea $S \neq \left\{\overline{0}\right\}$ un subespacio de $\mathbb{R}^n$. Para $r \in \mathbb{R}$ definimos

$$r \cdot S = \{r \cdot \overline{s} \mid \overline{s} \in S\}.$$

Demuestre que $S = r \cdot S$ si y sólo si $r \neq 0$.

14.2.7. Dé tres bases para $\mathbb{R}^3$.

14.2.8. Sea S un subespacio de $\mathbb{R}^n$ de dimensión $m \geq 1$ sobre $\mathbb{R}$. Demostrar que existe una sucesión de subespacios de $\mathbb{R}^n$ $S_0, S_1, \ldots, S_{m-1}$ tal que

$$S_0 = \left\{\overline{0}\right\} \subsetneq S_1 \subsetneq \cdots \subsetneq S_{m-1} \subsetneq S,$$

donde $\dim_{\mathbb{R}} S_i = i$ para $i = 0, \ldots, m - 1$.

El espacio vectorial $\mathbb{R}^n$

14.2.9. Sean $\overline{s}_1 = (1,-1,1)$, $\overline{s}_2 = (-1,4,2)$ y $\overline{s}_3 = (3,0,-2)$ vectores en $\mathbb{R}^3$. Calcule:

$(a)\ \overline{s}_1 + \overline{s}_2$ $(b)\ \overline{s}_2 - \overline{s}_3$ $(c)\ \frac{1}{2}\cdot\overline{s}_2$
$(d)\ \overline{s}_3 - 2\cdot\overline{s}_1$ $(e)\ 2\cdot\overline{s}_2 + 3\cdot\overline{s}_3$ $(f)\ \alpha\cdot\overline{s}_1 + \beta\cdot\overline{s}_2 + \gamma\cdot\overline{s}_3$, con $\alpha,\beta,\gamma\in\mathbb{R}$

14.2.10. Resuelva las ecuaciones (para x y y)

(a) $(3,1)+(x,y)=(2,3)$,
(b) $(a,b)+(x,y)=(c,d)$,
(c) $(a,1)+(x,y)=(-3,b)$,
(d) $(x,y)+(a,b)=(0,0)$,
(e) $(x-y,x+y)-\frac{1}{2}\cdot(y,x)=(0,1)$.

14.2.11. Si $v_1=(1,0,0,0)$, $v_2=(1,1,0,0)$, $v_3=(1,1,1,0)$ y $v_4=(1,1,1,1)$ son vectores en $\mathbb{R}^4$, determine el vector

$$v = a_1v_1 + a_2v_2 + a_3v_3 + a_4v_4.$$

Generalice este ejercicio a $\mathbb{R}^n$.

Independencia lineal, bases y dimensión

14.2.12. Sean $\overline{s}_1,\overline{s}_2\in\mathbb{R}^n$. Pruebe que el conjunto $\{\overline{s}_1,\overline{s}_2\}$ es linealmente dependiente si y sólo si $\overline{s}_1$ o $\overline{s}_2$ es múltiplo del otro.

14.2.13. Dé un ejemplo de tres vectores linealmente dependientes en $\mathbb{R}^2$ tales que ninguno de los otros tres es múltiplo de otro.

14.2.14. Sea $\{\overline{s}_1,\ldots,\overline{s}_m\}$ un conjunto de vectores en $\mathbb{R}^n$ que tiene la propiedad de que el conjunto $\{\overline{s}_i,\overline{s}_j\}$ es linealmente dependiente cuando $i\neq j$. Demuestre que cada vector del conjunto es un múltiplo de un solo vector de ese conjunto.

14.2.15. Sean

$$\begin{array}{rcl}
\overline{s}_1 & = & (s_{11}, s_{21}, \ldots, s_{n1}) \\
\overline{s}_2 & = & (s_{12}, s_{22}, \ldots, s_{n2}) \\
\vdots & & \vdots \quad \vdots \qquad \vdots \\
\overline{s}_m & = & (s_{1n}, s_{2n}, \ldots, s_{nm})
\end{array}$$

vectores en $\mathbb{R}^n$. Demuestre que el conjunto $\{\overline{s}_1, \ldots, \overline{s}_m\}$ es linealmente dependiente si y sólo si el sistema homogéneo de ecuaciones lineales

$$\begin{cases} s_{11}x_1 + s_{12}x_2 + \ldots + s_{1n}x_m = 0 \\ s_{21}x_1 + s_{22}x_2 + \ldots + s_{2n}x_m = 0 \\ \vdots \quad\quad \vdots \quad\quad \vdots \quad\quad \vdots \\ s_{n1}x_1 + s_{n2}x_2 + \ldots + s_{nm}x_m = 0 \end{cases}$$

tiene soluciones no triviales.

14.2.16. Determine si el conjunto de vectores dado es linealmente dependiente o independiente. Si el conjunto es linealmente dependiente encuentre una relación de dependencia.

(1) $\{(9,-8),(-11,-3)\} \subseteq \mathbb{R}^2$.
(2) $\{(-6,1),(-12,-2)\} \subseteq \mathbb{R}^2$.
(3) $\{(0,-2),(1,2),(2,1)\} \subseteq \mathbb{R}^2$.
(4) $\{(1,0,0),(0,1,1)\} \subseteq \mathbb{R}^3$.
(5) $\{(3,1,1),(-1,2,-3),(8,5,0)\} \subseteq \mathbb{R}^3$.
(6) $\{(2,-1,4),(-4,2,-8)\} \subseteq \mathbb{R}^3$.
(7) $\{(1,2,3),(-1,1,-1),(4,-1,1)\} \subseteq \mathbb{R}^3$.
(8) $\{(0,2,-1,1),(2,2,0,1),(-6,-16,5,-1)\} \subseteq \mathbb{R}^4$.
(9) $\{(1,-2,1,1),(3,0,2,-2),(0,4,-1,1),(5,0,3,-1)\} \subseteq \mathbb{R}^4$.
(10) $\{(1,0,0,0),(1,1,0,0),(1,1,1,0),(1,1,1,1)\} \subseteq \mathbb{R}^4$.

14.2.17. ¿Para qué valor(es) α serán linealmente dependientes los vectores

$$v_1 = (3,2,1),\ v_2 = (-2,-1,-1) \text{ y } v_3 = (\alpha,5,2)?$$

14. 2.18. Sean v_1, v_2, v_3 vectores en $\mathbb{R}^n$. Demuestre que si $\{v_1, v_2, v_3\}$ es linealmente independiente, entonces también lo es $\{v_1 - v_2, v_2 - v_3, v_3 + v_1\}$.

14. 2.19. Sean $\{\overline{s}_1, \ldots, \overline{s}_m\}$ un subconjunto linealmente independiente de $\mathbb{R}^n$ y $s \in \mathbb{R}^n$. Prueba que si el conjunto $\{\overline{s}_1 + \overline{s}, \overline{s}_2 + \overline{s}, \ldots, \overline{s}_m + \overline{s}\}$ es linealmente dependiente, entonces $s \in \langle \overline{s}_1, \overline{s}_2, \ldots, \overline{s}_m \rangle$.

14.2.20. Prueba que el conjunto de vectores diferentes de cero $\{v_1, \ldots, v_m\}$ en $\mathbb{R}^n$ es linealmente dependiente si y sólo si uno de ellos es combinación lineal de los vectores precedentes, es decir, existe un entero $t \leq m$ y escalares $\alpha_1, \alpha_2, \ldots, \alpha_{t-1}$ tales que $v_t = \alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_{t-1} v_{t-1}$.

14. 2.21. Para cada uno de los siguientes conjuntos de vectores en $\mathbb{R}^3$, existen razones "evidentes" por las cuales tal conjunto no puede constituir una base para $\mathbb{R}^3$. Diga cuales son estas razones.

(1) $\{(3,-8,1),(6,2,-5)\}$.
(2) $\{(1,1,1),(2,2,2),(3,3,3)\}$.
(3) $\{(1,1,0),(1,1,1),(0,0,1),(2,3,5)\}$.
(4) $\{(2,1,3),(0,0,0),(3,1,-1)\}$.

14.2.22. Demuestre que los siguientes conjuntos son bases para el correspondiente $\mathbb{R}^n$.

(1) $\{(1,-1),(1,1)\} \subseteq \mathbb{R}^2$.
(2) $\{(1,0,-1),(1,0,1),(0,-1,0)\} \subseteq \mathbb{R}^3$.
(3) $\{(1,0,0,0),(1,1,0,0),(1,1,1,0),(1,1,1,1)\} \subseteq \mathbb{R}^4$.
(4) $\{(1,0,-1,0,0),(1,0,1,0,0),(0,1,0,-1,0),(0,1,0,1,0),(0,0,0,0,1)\} \subseteq \mathbb{R}^5$.

14. 2.23. En cada uno de los siguientes incisos encuentre una base para $\mathbb{R}^3$ que contenga al (a los) vector(es) indicado(s).

(1) $v_1 = (1,1,1)$.
(2) $v_1 = (0,1,0)$, $v_2 = (1,0,1)$.
(3) $v_1 = (2,3,1)$, $v_2 = (3,1,2)$.

14. 2.24. Encuentre dos bases para $\mathbb{R}^4$ que contengan a $(1,0,1,0)$ y $(0,1,0,1)$ y no tengan otros vectores en común.

14. 2.25. El conjunto de vectores $\{(-9,-7,8,-5,7),(9,4,1,6,7),(6,7,-8,5,-7)\}$ en $\mathbb{R}^5$ es linealmente independiente. Extienda este conjunto a una base para $\mathbb{R}^5$.

14. 2.26. Los vectores $\overline{s}_1 = (2,-3,1)$, $\overline{s}_2 = (1,4,-2)$, $\overline{s}_3 = (-8,12,-4)$, $\overline{s}_4 = (1,37,-4)$ y $\overline{s}_5 = (-3,-5,8)$ generan a $\mathbb{R}^3$. Encontrar un subconjunto de $\{\overline{s}_1, \overline{s}_2, \overline{s}_3, \overline{s}_4, \overline{s}_5\}$ que sea una base para $\mathbb{R}^3$.

14.2.27. Sea $S = \{(2a,-b,a+b) \in \mathbb{R}^3 \mid a,b \in \mathbb{R}\}$.

(1) Verifique que S es un subespacio de $\mathbb{R}^3$.
(2) Encuentre una base para S. Pruebe su respuesta.
(3) ¿Cuál es $\dim_{\mathbb{R}} S$?.

14.2.28. Encontrar bases para los siguientes subespacios de $\mathbb{R}^5$:

$$S = \left\{(a_1,a_2,a_3,a_4,a_5) \in \mathbb{R}^5 \mid a_1 - a_3 - a_4 = 0\right\}$$

y

$$S' = \left\{(a_1, a_2, a_3, a_4, a_5) \in \mathbb{R}^5 \mid a_2 = a_3 = a_4, a_1 + a_5 = 0\right\}.$$

¿Cuáles son las dimensiones de S y S'?

14. 2.29. Considere el subespacio S de $\mathbb{R}^4$ generado por los vectores $v_1 = (0, 1, -3, 2)$, $v_2 = (1, -1, 0, 1)$, $v_3 = (3, 0, 1, -1)$ y $v_4 = (4, 0, -2, 2)$. Obtenga una base para S formada por algunos de estos generadores. Extienda esta base a una base para $\mathbb{R}^4$.

14.2.30. Sean S y S' los subespacios de $\mathbb{R}^3$ dados por

$$S = \{(x, y, z) \mid x + y + z = 0\} \ y \ S' = \{(x, y, z) \mid x + y = 0\}.$$

Encuentre una base y la dimensión de S, S' y $S \cap S'$. Haga lo mismo para los subespacios de $\mathbb{R}^4$ dados por

$$S = \{(a, b, c, d) \mid b + c + d = 0\} \ y \ S' = \{(a, b, c, d) \mid a + b = 0, c = 2d\}.$$

14.2.31. Sea S el subespacio de $\mathbb{R}^4$ generado por los vectores

$$(1, 4, 3, 2), \ (2, 4, 6, 8) \ y \ (3, 6, 4, 2),$$

y sea S' el subespacio de $\mathbb{R}^4$ generado por los vectores

$$(2, 3, 1, 4), \ (1, 1, 2, 0) \ y \ (3, 1, 2, 4).$$

Encuentre una base y la dimensión de $S + S'$ y de $S \cap S'$. Haga lo mismo para los subespacios S y S' de $\mathbb{R}^5$ generados por los conjuntos de vectores

$$\{(1, 3, -2, 2, 3), (1, 4, -3, 4, 2), (2, 3, -1, -2, 9)\}$$

y

$$\{(1, 3, 0, 2, 1), (1, 5, -6, 6, 3), (2, 5, 3, 2, 1)\}.$$

14.2.32. Considere los siguientes subespacios de $\mathbb{R}^3$:

$$S = \left\{(x, y, z) \in \mathbb{R}^3 \mid x - 2y + z = 0\right\}$$

y

$$S' = \langle (3, -1, -1), (1, -1, 1), (1, 1, -3) \rangle .$$

(1) Encuentre una base para S y S'.
(2) Encuentre una base para $S \cap S'$ y $S + S'$.

14. 2.33. Sea S_1 y S_2 subespacios de $\mathbb{R}^n$ de dimensiones m_1 y m_2, respectivamente, donde $m_1 \geq m_2$. Demostrar que $\dim_{\mathbb{R}}(S \cap S') \leq m_2$ y $\dim_{\mathbb{R}}(S + S') \leq m_1 + m_2$. Dar ejemplos de subespacios de $\mathbb{R}^3$ donde cada desigualdad se convierta en igualdad.

14.2.34. Sea $\{v_1, v_2, \ldots, v_m\}$ es una base para $\mathbb{R}^n$ y sean $\alpha_1, \alpha_2, \ldots, \alpha_m$ elementos distintos de cero en $\mathbb{R}$. Pruebe que $\{\alpha_1 v_1, \alpha_2 v_2, \ldots, \alpha_m v_m\}$ es también una base para $\mathbb{R}^n$

14.2.35. Sea $\{v_1, v_2, \ldots, v_m\}$ es una base para $\mathbb{R}^n$. Pruebe que

$$\{v_1, v_1 + v_2, \ldots, v_1 + \ldots + v_m\}$$

es también una base para $\mathbb{R}^n$

14.2.36. Indique cuáles de las siguientes proposiciones son verdaderas. Justifique sus respuestas.

(1) Cualesquiera tres vectores en $\mathbb{R}^3$ forman una base para $\mathbb{R}^3$.
(2) Cualesquiera tres vectores linealmente independientes en $\mathbb{R}^3$ forman una base para $\mathbb{R}^3$.
(3) Una base en un subespacio de $\mathbb{R}^2$ es única.
(4) Si S es un subespacio de $\mathbb{R}^4$, entonces es posible encontrar cuatro vectores linealmente independientes en S.
(5) Si $S = \{(x, y, z) \in \mathbb{R}^3 \mid 2x + 11y - 17z = 0\}$, entonces $\dim_{\mathbb{R}} S = 2$.
(6) Existe una base de $\mathbb{R}^3$ que contiene a los vectores $\overline{s}_1 = (2, 1, 3)$ y $\overline{s}_2 = (4, 2, 6)$.
(7) Si $\{v_1, v_2, \ldots, v_m\}$ es una base para $\mathbb{R}^n$, entonces NO es posible encontrar un vector $v \in \mathbb{R}^n$ tal que $v \notin \langle v_1, v_2, \ldots, v_m \rangle$.

§§ Ejercicios sección 14.3.

14. 3.1. Encuentre una base y la dimensión del espacio solución del sistema homogéneo dado.

(1) 1)
$$\begin{cases} 2x + 3y - 4z = 0 \\ x - y + z = 0 \\ 2x + 8y - 10z = 0 \end{cases}$$

(2)
$$\begin{cases} y + 4z = 0 \\ x + 2y - z = 0 \\ 5x + 8y = 0 \end{cases}$$

$$(3)\ \begin{cases} 3x - y + 7z = 0 \\ 2x - y + 4z + \frac{1}{2}w = 0 \\ x - y + z + w = 0 \\ 6x - 4y + 10z + 3w = 0 \end{cases}$$

$$(4)\ \begin{cases} 2x_1 - x_2 + x_3 + x_4 = 0 \\ 3x_1 + 2x_2 - x_3 - x_4 = 0 \end{cases}$$

$$(5)\ \begin{cases} x + 2y - 3z + w = 0 \\ 2x + 2z - w = 0 \\ x - y + z - 2w = 0 \end{cases}$$

$$(6)\ \begin{cases} x_1 + 2x_2 + x_3 - x_4 - 2x_5 = 0 \\ 2x_1 + 3x_2 - x_3 - x_4 - x_5 = 0 \\ x_1 + x_2 - 2x_3 + x_5 = 0 \\ -3x_1 - 4x_2 + 3x_3 + x_4 = 0 \end{cases}$$

$$(7)\ \begin{cases} x_1 + 2x_2 + 3x_3 - 2x_4 + 4x_5 = 0 \\ 2x_3 + 3x_4 + x_5 = 0 \\ x_1 + 2x_2 - 10x_3 - 3x_4 + 11x_5 = 0 \\ -x_1 - 2x_2 + 4x_3 - 2x_4 + 6x_5 = 0 \end{cases}$$

14.3.2. Considere los siguientes sistemas ecuaciones lineales, los cuales son consistentes.

$$(1)\ \begin{cases} x_1 + x_2 - 5x_3 = -10 \\ x_1 + 2x_2 - 8x_3 = -17 \\ 4x_1 + 7x_2 - 29x_3 = -61 \end{cases}$$

$$(2)\ \begin{cases} x_1 + x_2 = 0 \\ 3x_1 + 3x_2 + x_3 = -1 \\ -2x_1 - 2x_2 + x_3 + x_4 = 0 \end{cases}$$

$$(3)\ \begin{cases} x_1 - 2x_2 + x_3 - 3x_4 = -2 \\ 2x_1 + x_2 - x_3 + 2x_4 = -1 \\ x_1 + 3x_2 - 2x_3 + 5x_4 = 1 \end{cases}$$

$$(4)\ \begin{cases} x_1 - x_2 - x_3 + 2x_4 = 4 \\ 2x_1 - x_2 + 3x_3 - x_4 = 2 \end{cases}$$

$$(5)\ \begin{cases} x_1 + 2x_2 - x_3 + x_4 + 2x_5 = 0 \\ x_2 + 2x_3 - 3x_4 - 3x_5 = 2 \\ x_3 + 5x_4 + 3x_5 = -3 \end{cases}$$

$$(6)\quad \begin{cases} 2x_1 + 2x_2 + 4x_3 = 10 \\ x_2 + 2x_3 + 2x_4 + 12x_5 = 0 \\ x_1 + x_2 + 2x_3 + 5x_4 + 30x_5 = 0 \\ x_1 + x_2 + 2x_3 + 2x_4 + 12x_5 = 3 \end{cases}$$

$$(7)\quad \begin{cases} x_1 + x_2 + 2x_3 + x_4 + 2x_5 - 2x_6 = 4 \\ 2x_1 + x_2 + x_3 + x_4 - x_6 = 0 \\ 3x_1 + 2x_2 + x_3 + 2x_4 - x_5 - x_6 = -2 \\ x_1 - x_2 - x_4 = 0 \end{cases}$$

(*a*) Escriba la solución de cada sistema como la suma de la solución general del sistema homogéneo asociado y una solución particular del sistema no homogéneo.

(*b*) Encuentre la dimensión y una base del conjunto de todas las soluciones del sistema homogéneo asociado a cada sistema.

14. 3.3. Encuentre un sistema homogéneo cuyo espacio solución está generado por el conjunto de vectores $\{(1,3,2),(4,5,8),(3,8,6)\}$ en $\mathbb{R}^3$. Haga los mismo para el conjunto $\{(1,-2,0,3),(1,-1,-1,4),(1,0,-2,5)\}$.

Las matemáticas no mienten, lo que hay son muchos matemáticos mentirosos.
Henry David Thoreau
1817 - 1862

***Capítulo* 15**

Matrices y determinantes

§ 15.1. Introducción a las matrices

En el capítulo 14 definimos una matriz de orden $m \times n$ con coeficientes en $\mathbb{R}$ como un arreglo de $m \cdot n$ números reales distribuidos en m renglones y n columnas donde la ubicación de cada elemento de la matriz está determinado por el renglón y la columna donde está colocado. Así pues, una matriz escrita formalmente como un objeto (conjunto) de la teoría de conjuntos no es otra cosa que la imagen de una función de $\{1, \ldots, m\} \times \{1, \ldots, n\}$ en $\mathbb{R}$. Al conjunto de matrices de $m \times n$ le daremos estructura de espacio vectorial, la que aprovecharemos para una posterior aplicación a sistemas de ecuaciones. Todas las matrices con las que trabajaremos aquí tendrán coeficientes reales, así que al referirnos a ellas omitiremos esto último de tal manera que cuando hablemos de una matriz entenderemos que sus coeficientes son números reales.

Notación 15.1*. A las matrices las denotaremos con letras mayúsculas:* $A, B, C, \ldots$ *o también* $\left(a_{ij}\right)_{m\times n}$ *donde m denota el número de renglones y n el número de columnas (o simplemente* (a_{ij}) *cuando no pueda haber confusión) y que en alguna ocasión resulta más cómodo e ilustrativo como se puede ver en la definición de suma y producto por escalares. Al conjunto de matrices de orden* $m \times n$ *lo denotaremos por* $M_{m\times n}(\mathbb{R})$*, es decir,*

$$M_{m\times n}(\mathbb{R}) = \left\{ \left(a_{ij}\right)_{m\times n} \mid a_{ij} \in \mathbb{R},\ i = 1, \ldots, m,\ j = 1, \ldots, n \right\}.$$

Al elemento a_{ij} colocado en el renglón i y columna j de una matriz A lo llamamos la **entrada ij** *de la matriz A.*

Introducimos la suma y producto por escalares en $M_{m\times n}(\mathbb{R})$.

Definición 15.1.2. *Dadas dos matrices $(a_{ij}), (b_{ij}) \in M_{m\times n}(R)$ y $\alpha \in \mathbb{R}$, la suma $(a_{ij}) + (b_{ij})$ y el producto $\alpha \cdot (a_{ij})$ son:*

$$(a_{ij}) + (b_{ij}) = (c_{ij}) \quad \alpha \cdot (a_{ij}) = (d_{ij}) \quad \text{donde } c_{ij} = a_{ij} + b_{ij} \text{ y } d_{ij} = \alpha a_{ij}$$

Entonces, la suma de (a_{ij}) y (b_{ij}) es la matriz que se obtiene de ellas el sumar las entradas correspondientes de cada matriz y el producto de α y (a_{ij}) es la matriz que resulta de multiplicar por α cada entrada de la matriz. Convenimos en escribir directamente $(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})$ y $\alpha \cdot (a_{ij}) = (\alpha a_{ij})$ donde $a_{ij} + b_{ij}$ y αa_{ij} son los elementos del renglón i, columna j de la suma y el producto por el escalar α, respectivamente.

Ejemplo 15.1.3. Sea $A = \begin{pmatrix} 1 & -1 \\ 0 & 3 \\ -1 & -2 \end{pmatrix}$, $B = \begin{pmatrix} 0 & -1 \\ 1 & 3 \\ 6 & 2 \end{pmatrix}$ y $\alpha = 5$. Entonces

$$A + B = \begin{pmatrix} 1+0 & -1-1 \\ 0+1 & 3+3 \\ -1+6 & -2+2 \end{pmatrix} = \begin{pmatrix} 1 & -2 \\ 1 & 6 \\ 5 & 0 \end{pmatrix} \quad \text{y}$$

$$5 \cdot A = \begin{pmatrix} 5\cdot 1 & 5\cdot(-1) \\ 5\cdot 0 & 5\cdot 3 \\ 5\cdot(-1) & 5\cdot(-2) \end{pmatrix} = \begin{pmatrix} 5 & -5 \\ 0 & 15 \\ -5 & -10 \end{pmatrix}$$

Como la suma de matrices y el producto por escalares se definió término a término es de esperar que hereden propiedades que tienen la suma y producto en $\mathbb{R}$; lo que convierte a $M_{m\times n}(\mathbb{R})$ en un espacio vectorial sobre $\mathbb{R}$ (véase el ejercicio 14.2.3 para la definición de espacio vectorial)

Teorema 15.1.4. *$M_{m\times n}(\mathbb{R})$ es un espacio vectorial sobre $\mathbb{R}$, es decir, para cualesquiera $(a_{ij}), (b_{ij}), (c_{ij}) \in M_{m\times n}(\mathbb{R})$ y cualesquiera $\alpha, \beta \in \mathbb{R}$*

(1) $\big[(a_{ij}) + (b_{ij})\big] + (c_{ij}) = (a_{ij}) + \big[(b_{ij}) + (c_{ij})\big]$
(2) $(a_{ij}) + (b_{ij}) = (b_{ij}) + (a_{ij})$
(3) *Existe* $(0_{ij}) \in M_{m\times n}(\mathbb{R})$ *tal que* $(a_{ij}) + (0_{ij}) = (0_{ij}) + (a_{ij}) = (a_{ij})$
(4) *Dado* $(a_{ij}) \in M_{m\times n}(\mathbb{R})$, *existe* (d_{ij}) *tal que* $(a_{ij}) + (d_{ij}) = (d_{ij}) + (a_{ij}) = (0_{ij})$
(5) $\alpha \cdot \big[(a_{ij}) + (b_{ij})\big] = \alpha \cdot (a_{ij}) + \alpha \cdot (b_{ij})$

(6) $(\alpha+\beta)\cdot(a_{ij}) = \alpha\cdot(a_{ij}) + \beta\cdot(a_{ij})$
(7) $(\alpha\beta)\cdot(a_{ij}) = \alpha\cdot\big[\beta\cdot(a_{ij})\big]$
(8) $1\cdot(a_{ij}) = (a_{ij})$

Demostración. Aplicando las propiedades de la suma y el producto en $\mathbb{R}$, tenemos que

(1)
$$\begin{aligned}\big[(a_{ij})+(b_{ij})\big]+(c_{ij}) &= (a_{ij}+b_{ij})+(c_{ij})\\ &= \big([a_{ij}+b_{ij}]+c_{ij}\big)\\ &= \big(a_{ij}+[b_{ij}+c_{ij}]\big)\\ &= (a_{ij})+\big(b_{ij}+c_{ij}\big)\\ &= (a_{ij})+\big[(b_{ij})+(c_{ij})\big].\end{aligned}$$

(2) $(a_{ij})+(b_{ij}) = (a_{ij}+b_{ij}) = (b_{ij}+a_{ij}) = (b_{ij})+(a_{ij})$.
(3) Si definimos (0_{ij}) tal que $0_{ij} = 0$ para toda $i = 1,\dots,m$ y $j = 1,\dots,n$, entonces $(a_{ij})+(0_{ij}) = (a_{ij}+0_{ij}) = (a_{ij}+0) = (a_{ij})$.
(4) Si definimos (d_{ij}) tal que $d_{ij} = -a_{ij}$ para toda $i = 1,\dots,m$ y $j = 1,\dots,n$, entonces $(a_{ij})+(d_{ij}) = (a_{ij}+d_{ij}) = (a_{ij}-[a_{ij}]) = (0_{ij})$.
(5) $\alpha\left[(a_{ij})+(b_j)\right] = \alpha(a_{ij}+b_{ij}) = (\alpha[a_{ij}+b_{ij}]) = (\alpha a_{ij}+\alpha b_{ij}) = (\alpha a_{ij})+(\alpha b_{ij})$.
(6) $(\alpha+\beta)\cdot(a_{ij}) = ([\alpha+\beta]a_{ij}) = (\alpha a_{ij}+\beta a_{ij}) = (\alpha a_{ij})+(\beta a_{ij}) = \alpha\cdot(a_{ij})+\beta\cdot(a_{ij})$.
(7) $(\alpha\beta)\cdot(a_{ij}) = ([\alpha\beta]a_{ij}) = (\alpha[\beta a_{ij}]) = \alpha\cdot(\beta a_{ij}) = \alpha\cdot[\beta\cdot(a_{ij})]$.
(8) $1\cdot(a_{ij}) = (1a_{ij}) = (a_{ij})$. ∎

A la matriz (0_{ij}) del inciso (3) la llamaremos la matriz cero de orden $m\times n$ y la denotamos por $\widetilde{0}_{m\times n}$ o simplemente $\widetilde{0}$ cuando no haya lugar a confusión. Entonces $A+\widetilde{0} = A$ para toda $A\in M_{m\times n}(\mathbb{R})$. Definimos ahora un producto para ciertas parejas de matrices el cual estará limitado a una condición sobre los órdenes de las matrices. Más concretamente, el producto $A\cdot B$ de las matrices A y B podrá realizarse solamente cuando el número de columnas de A coincida con el número de renglones de B. Aunque esta definición puede parecer extraña más adelante aparecerá de manera natural.

Definición 15.1.5. *Sean $A = (a_{ij})\in M_{m\times n}(\mathbb{R})$ y $B = (b_{ij})\in M_{n\times k}(\mathbb{R})$. El producto $A\cdot B$ de A y B es la matriz $(c_{ij})\in M_{m\times k}(\mathbb{R})$, donde para cada $i = 1,\dots,m$ y $j = 1,\dots,k$, $c_{ij} = \sum_{\ell=1}^{n} a_{i\ell}b_{\ell j} = a_{i1}b_{1j}+\cdots+a_{in}b_{nj}$.*

Observación 15.1.6. El coeficiente c_{ij} de la matriz producto que es precisamente el elemento ubicado en el renglón i y la columna j de la matriz producto $A \cdot B$ se obtiene de A y B a través del renglón i de A y la columna j de B.

Ejemplo 15.1.7. Sean

$$A = \begin{pmatrix} -1 & 1 \\ 0 & 2 \\ 3 & -2 \end{pmatrix} \in M_{3\times 2}(\mathbb{R}) \ y \ B = \begin{pmatrix} 0 & 1 & -1 & 2 \\ 5 & -7 & 1 & -1 \end{pmatrix} \in M_{2\times 4}(\mathbb{R}).$$

El número de columnas de A coincide con el número de renglones de B, así que podemos realizar el producto y el resultado deberá ser una matriz de orden 3×4.

$$\begin{aligned} A \cdot B &= \begin{pmatrix} (-1)\cdot 0+1\cdot 5 & (-1)\cdot 1+1\cdot(-7) & (-1)\cdot(-1)+1\cdot 1 & (-1)\cdot 2+1\cdot(-1) \\ 0\cdot 0+2\cdot 5 & 0\cdot 1+2\cdot(-7) & 0\cdot(-1)+2\cdot 1 & 0\cdot 2+2\cdot(-1) \\ 3\cdot 0+(-2)\cdot 5 & 3\cdot 1+(-2)\cdot(-7) & 3\cdot(-1)+(-2)\cdot 1 & 3\cdot 2+(-2)\cdot(-1) \end{pmatrix} \\ &= \begin{pmatrix} 5 & -8 & 2 & -3 \\ 10 & -14 & 2 & -2 \\ -10 & 17 & -5 & 8 \end{pmatrix} \in M_{3\times 4}(\mathbb{R}) \end{aligned}$$

Queda claro entonces de la definición que si $m \neq n$, en $M_{m\times n}(\mathbb{R})$ no está definido este producto para ningún par de matrices. Si $m = n$, en $M_{n\times n}(\mathbb{R})$ se tendrá definido el producto para cualesquiera dos matrices ahí. Este hecho le da una estructura más amplia a $M_{n\times n}(\mathbb{R})$ donde además la interacción del producto con la suma y producto por escalares se comportará de una manera bastante adecuada como veremos más adelante.

Teorema 15.1.8. *El producto de matrices es asociativo, esto es, si* $A = (a_{ij}) \in M_{m\times n}(\mathbb{R})$, $B = (b_{ij}) \in M_{n\times k}(\mathbb{R})$ *y* $C = (c_{ij}) \in M_{k\times p}$, *entonces* $(A\cdot B)\cdot C = A\cdot(B\cdot C)$.

Demostración. Primero observamos que tanto $(A \cdot B) \cdot C$ y $A \cdot (B \cdot C)$ son matrices que pertenecen a $M_{m\times p}(\mathbb{R})$, así que sólo nos falta verificar que tienen los mismos coeficientes. Veamos entonces que para cada $i = 1, \ldots, m$ y $j = 1, \ldots, p$ los coeficientes del renglón i y la columna j de ambas matrices son los mismos. Teniendo en cuenta que el coeficiente del renglón i y columna s de $A \cdot B$ es $\sum_{\ell=1}^{n} a_{i\ell} b_{\ell s}$ y el coeficiente del renglón ℓ y columna j de $B \cdot C$ es $\sum_{s=1}^{k} b_{\ell s} c_{sj}$ tenemos que si d_{ij} es el coeficiente del renglón i y la columna j de $(A \cdot B) \cdot C$ y d'_{ij} es el coeficiente del renglón i y la columna j de $A \cdot (B \cdot C)$ para $i = 1, \ldots, m$ y $j = 1, \ldots, p$, entonces

$$d_{ij} = \sum_{s=1}^{k} \left(\sum_{\ell=1}^{n} a_{i\ell} b_{\ell s} \right) c_{sj} = \sum_{s=1}^{k} \sum_{\ell=1}^{n} a_{i\ell} b_{\ell s} c_{sj} = \sum_{\ell=1}^{n} \sum_{s=1}^{k} a_{i\ell} b_{\ell s} c_{sj} = \sum_{\ell=1}^{n} a_{i\ell} \left(\sum_{s=1}^{k} b_{\ell s} c_{sj} \right) = d'_{ij}. \quad \blacksquare$$

En $M_{n\times n}(\mathbb{R})$ para cada $n = 1, 2, \ldots$ existe una matriz especial $I_{n\times n} = (e_{ij})$ definida por $e_{ij} = \begin{cases} 1 & \text{si } i = j; \\ 0 & \text{si } i \neq j. \end{cases}$ para $1 \leq i, j \leq n$ y a la cual llamaremos matriz identidad de orden $n \times n$ o simplemente de orden n. $I_{n\times n}$ tiene el siguiente aspecto

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots\vdots\vdots & \vdots & \vdots\vdots\vdots & \vdots \\ 0 & 0 & \cdots & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots\vdots\vdots & \vdots & \vdots\vdots\vdots & \vdots \\ 0 & 0 & \vdots\vdots\vdots & 0 & \vdots\vdots\vdots & 1 \end{pmatrix} \longleftarrow \text{renglón } j$$

$$\uparrow$$

columna j

Otras propiedades del producto, ahora con respecto a la suma y producto por escalares son:

Teorema 15.1.9. *Sean $A \in M_{m\times n}(\mathbb{R})$, $B, C \in M_{n\times k}(\mathbb{R})$ y $\alpha \in \mathbb{R}$. Entonces*

(1) $A \cdot (B + C) = A \cdot B + A \cdot C$.

(2) $\alpha \cdot (A \cdot B) = (\alpha \cdot A) \cdot B = A \cdot (\alpha \cdot B)$.

(3) $I_{m\times m} \cdot A = A = A \cdot I_{n\times n}$.

Demostración. Sean $A = (a_{ij}) \in M_{m\times n}(\mathbb{R})$, $B = (b_{ij}), C = (c_{ij}) \in M_{n\times k}(\mathbb{R})$.

(1) Es claro que $A\cdot(B+C)$ y $A\cdot B+A\cdot C$ pertenecen a $M_{m\times k}(\mathbb{R})$. Compararemos sus coeficientes. El coeficiente del renglón i y columna j de $A\cdot(B+C)$ es $\sum_{\ell=1}^{n} a_{i\ell}[b_{\ell j} + c_{\ell j}]$ y el respectivo de $A \cdot B + A \cdot C$ es $\sum_{\ell=1}^{n} a_{i\ell} b_{\ell j} + \sum_{\ell=1}^{n} a_{i\ell} c_{\ell j}$. Entonces

$$\sum_{\ell=1}^{n} a_{i\ell}[b_{\ell j} + c_{\ell j}] = \sum_{\ell=1}^{n} [a_{i\ell} b_{\ell j} + a_{i\ell} c_{\ell j}] = \sum_{\ell=1}^{n} a_{i\ell} b_{\ell j} + \sum_{\ell=1}^{n} a_{i\ell} c_{\ell j}.$$

Por lo tanto $A \cdot (B + C) = A \cdot B + A \cdot C$.

(2) El resultado se obtiene de la siguientes igualdades

$$\alpha \cdot \sum_{\ell=1}^{n} a_{i\ell} b_{\ell j} = \sum_{\ell=1}^{n} \alpha[a_{i\ell} b_{\ell j}] = \sum_{\ell=1}^{n} (\alpha a_{i\ell}) b_{\ell j} = \sum_{\ell=1}^{n} a_{i\ell} (\alpha b_{\ell j}).$$

(3) Para cada $i = 1, \ldots, m$ y $j = 1, \ldots, n$ la entrada ij de $I_{m\times m} \cdot A$ es $\sum_{\ell=1}^{n} e_{i\ell}a_{\ell j} = e_{ii}a_{ij} = a_{ij}$ y la entrada ij de la matriz $A \cdot I_{n\times n}$ es

$$\sum_{\ell=1}^{n} a_{i\ell}e_{\ell j} = a_{ij}e_{jj} = a_{ij}.$$

Por lo tanto $I_{m\times m} \cdot A = A$ y $A \cdot I_{n\times n} = A$. ∎

Trataremos ahora el caso $m = n$. Es claro, de la definición de producto, que para cualesquiera matrices A y B en $M_{n\times n}(\mathbb{R})$, $A \cdot B$ y $B \cdot A$ están definidas y pertenecen a $M_{n\times n}(\mathbb{R})$, así que tiene sentido es este caso preguntarse si $A \cdot B$ es igual a $B \cdot A$. La respuesta es no necesariamente, lo que puede verse en el ejemplo 15.1.10.
Teniendo en cuenta las propiedades de la suma de matrices (teorema 15.1.4 (1)-(4)) junto con este último teorema, podemos afirmar que

$$\underline{(M_{n\times n}(\mathbb{R}), +, \cdot) \text{ es un anillo}},$$

onde el neutro aditivo es la matriz cero de (de orden $n\times n$) y el neutro multiplicativo es la matriz identidad $I_{n\times n}$, el cual como veremos a continuación no es un anillo conmutativo así como tampoco es dominio entero para toda $n > 1$. El caso $n = 1$, es decir, las matrices de 1×1 podemos identificarlas con los números reales puesto que $(a) + (b) = (a + b)$ y $(a) \cdot (b) = (ab)$.

Ejemplo 15.1.10. Sean

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & -1 & 1 \\ 2 & 3 & -1 \end{pmatrix} \quad y \quad B = \begin{pmatrix} 2 & -1 & 0 \\ 3 & 1 & 1 \\ 0 & 2 & -1 \end{pmatrix}.$$

Entonces

$$A \cdot B = \begin{pmatrix} 2 & 1 & -1 \\ -3 & 1 & -2 \\ 13 & -1 & 4 \end{pmatrix} \text{ y } B \cdot A = \begin{pmatrix} 2 & 1 & 1 \\ 5 & 2 & 3 \\ -2 & -5 & 3 \end{pmatrix}$$

con lo cual $A \cdot B \neq B \cdot A$.

Ejemplo 15.1.11. Sean $A = \begin{pmatrix} 2 & 0 & 2 \\ 1 & 0 & 1 \\ 3 & 0 & 3 \end{pmatrix}$ y $B = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 3 \\ -1 & 0 & 0 \end{pmatrix}$. Entonces $A \cdot B = \widetilde{0}$.

Considerando que $M_{n\times n}(\mathbb{R})$ es un anillo, a las matrices que tengan inverso multiplicativo les daremos un nombre especial.

Definición 15.1.12. *Sea $A \in M_{n\times n}(\mathbb{R})$. A es* **invertible** *si A tiene inverso multiplicativo, es decir, existe $B \in M_{n\times n}(\mathbb{R})$ tal que $A \cdot B = B \cdot A = I_{n\times n}$ y en este caso llamamos a B la matriz inversa de A y la denotamos por $\mathbf{A^{-1}}$.*

Observación 15.1.13. La notación para la inversa A^{-1} de una matriz invertible no presenta ninguna confusión ya que ésta es única: Si $A \cdot B = B \cdot A = I_{n\times n}$ y $A \cdot C = I_{n\times n}$, entonces $C = I_{n\times n} \cdot C = (B \cdot A) \cdot C = B \cdot (A \cdot C) = B \cdot I_{n\times n} = B$.

Aun cuando es cierto para $m \neq n$, en $M_{m\times n}(\mathbb{R})$ no está definido el producto, puede suceder que para alguna matriz $A \in M_{m\times n}(\mathbb{R})$ exista una matriz $B \in M_{n\times m}(\mathbb{R})$ tal que $B \cdot A = I_{n\times n}$ o que $A \cdot B = I_{m\times m}$. En este sentido y abusando un poco del lenguaje es que definimos

Definición 15.1.14. *Sea $A \in M_{m\times n}(\mathbb{R})$. Una matriz $B \in M_{n\times m}(\mathbb{R})$ es un* **inverso izquierdo** *(***derecho***) de A si $B \cdot A = I_{n\times n}$ ($A \cdot B = I_{m\times m}$).*

Nota 15.1.15. En el caso en que $m = n$, es claro que si $A \in M_{n\times n}(\mathbb{R})$ es invertible, entonces A^{-1} es tanto inversa izquierda como derecha de A, así que uno podría preguntarse, si A tiene un inverso izquierdo B e inverso derecho C ¿qué relación puede haber entre B y C? Más adelante veremos que la respuesta es que debe ser $B = C$, razón por la cual A será invertible. No solamente esto, para ver que una matriz en $M_{n\times n}(\mathbb{R})$ es invertible bastará con mostrar que la matriz tiene un inverso izquierdo o un inverso derecho.

Nota 15.1.16. En el caso en que $m \neq n$, si $A \in M_{m\times n}(\mathbb{R})$ y tiene inverso izquierdo (derecho) éste no tiene porqué ser único (de hecho no lo es). Es más veremos que si A tiene un inverso izquierdo (derecho) automáticamente podemos afirmar que no tiene inverso derecho (izquierdo).

Teorema 15.1.17. *Si $A, B \in M_{n\times n}(\mathbb{R})$ son matrices invertibles, entonces A^{-1} y $A \cdot B$ son invertibles. Es más $\left(A^{-1}\right)^{-1} = A$ y $(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$.*

Demostración. A es la inversa de A^{-1} porque $A^{-1} \cdot A = A \cdot A^{-1} = I_{n\times n}$ con lo cual $\left(A^{-1}\right)^{-1} = A$.

$$\begin{aligned}(A \cdot B) \cdot \left(B^{-1} \cdot A^{-1}\right) &= A \cdot \left(B \cdot B^{-1}\right) \cdot A^{-1} \\ &= A \cdot I_{n\times n} \cdot A^{-1} \\ &= A \cdot A^{-1} \\ &= I_{n\times n}.\end{aligned}$$ ■

Corolario 15.1.18. *Si $A_1, \ldots, A_m \in M_{n\times n}(\mathbb{R})$, son matrices invertibles, entonces $B = A_1 \cdot \ldots \cdot A_m$ es una matriz invertible.*

Demostración. Como cada una de las matrices A_i es invertible, con inversa A_i^{-1}, podemos forma el producto $A_m^{-1} \cdots A_1^{-1}$. Que es la inversa buscada. ■

Corolario 15.1.19. *Sean $A, B, C \in M_{n\times n}(\mathbb{R})$ con $A = B \cdot C$ y C invertible. Entonces A es invertible si y sólo si B lo es.*

Demostración. Como C es invertible, también lo es C^{-1}, por el teorema 15.1.17. Ahora si B es invertible, por el mismo teorema 15.1.17, $B \cdot C = A$ es invertible. Si A es invertible, como $B = A \cdot C^{-1}$, entonces B lo es. ■

¿Como saber si una matriz es invertible o no? Con lo que tenemos hasta el momento no es fácil responder a esta pregunta.

Si un renglón, digamos el i, consta únicamente de ceros, es claro que la matriz no puede ser invertible ya que el multiplicar por la derecha por cualquier matriz, el renglón i del producto también constará de ceros por lo que nunca se obtendrá la matriz identidad; lo mismo sucede en el caso en que A tenga una columna de ceros, la j por ejemplo, pues al multiplicar por la izquierda por cualquier matriz la columna j del producto constará de ceros. Por supuesto estos son casos particulares.

En el afán de describir un mecanismo que nos permita no sólo saber si una matriz es invertible o no, sino además en caso de serlo obtener una matriz inversa, nos apoyaremos en las operaciones elementales no sólo únicamente sobre los renglones que ya hemos definido en el capítulo 14 sino que las introducimos también para columnas. Esto lo hacemos en general para cualquier matriz de $m \times n$ y posteriormente lo aplicaremos para nuestro objetivo que es el caso cuando $m = n$.

Operaciones elementales sobre renglones (columnas) de una matriz de orden $m \times n$.

(I) Intercambiar dos renglones (columnas).

(II) Multiplicar un renglón (columna) por un número real $\neq 0$.
(III) Sumar a un renglón (columna) un múltiplo real de otro renglón (columna).

Lo que veremos es que realizar una operación elemental sobre renglones (columnas) de una matriz A no es otra cosa que multiplicar la matriz A por la izquierda (derecha) por ciertas matrices muy especiales a las que llamaremos elementales cuya definición damos a continuación

Definición 15.1.20. *Una matriz $E \in M_{n\times n}(\mathbb{R})$ es elemental si resulta de la matriz identidad $I_{n\times n}$ al realizar una operación elemental sobre los renglones o sobre las columnas.*

En realidad las matrices elementales que se obtienen de la matriz identidad al realizar una operación elemental sobre renglones son las mismas que las matrices elementales que se obtienen de la matriz identidad mediante una operación elemental sobre las columnas.
Las matrices elementales tienen el siguiente aspecto

renglón i
renglón j

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix}$$

col. i col. j

matriz elemental que se obtiene de $I_{n\times n}$ al intercambiar el renglón i por el renglón j que es igual a la matriz elemental que se obtiene de $I_{n\times n}$ al intercambiar la columna i por la columna j.

renglón i

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \alpha & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \vdots & 0 & \vdots & 1 \end{pmatrix}$$

col. i

matriz elemental que se obtiene de $I_{n\times n}$ al multiplicar el renglón i por α ($\alpha \neq 0$) que es igual a la matriz elemental que se obtiene de $I_{n\times n}$ al multiplicar la columna i por α.

$$\begin{array}{c} \\ \text{renglón } i \\ \\ \text{renglón } j \\ \\ \\ \text{col. } i \quad \text{col. } j \end{array} \begin{pmatrix} 1 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & \cdots & \alpha & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix}$$

matriz elemental que se obtiene de $I_{n\times n}$ al sumar al renglón i α veces al renglón j que es igual a la matriz elemental que se obtiene de $I_{n\times n}$ al sumar a la columna j α veces la columna i.

Teorema 15.1.21. *Sea $A \in M_{m\times n}(\mathbb{R})$. Si B se obtiene de A al realizar una operación elemental sobre los renglones (columnas) y E es la matriz elemental que resulta de $I_{m\times m}$ ($I_{n\times n}$) al realizar la misma operación elemental que se hizo en A, entonces $E \cdot A = B$.*

Demostración. Sean

$$A = (a_{ij}), B = (b_{ij}) \in M_{m\times n}(\mathbb{R}) \quad y \quad E = (c_{kq}) \in M_{m\times m}(\mathbb{R}).$$

Considerando cada una de las operaciones elementales sobre los renglones

(I) Supongamos que B se obtiene de A al intercambiar el renglón i por el renglón j. Entonces $B = (b_{k\ell})$, donde $b_{k\ell} = a_{k\ell}$ si $k \neq i, j$; $b_{i\ell} = a_{j\ell}$ y $b_{j\ell} = a_{i\ell}$ para $\ell = 1, \ldots, n$ y $E = (c_{kq}) \in M_{m\times m}(\mathbb{R})$ donde

$$c_{kq} = \begin{cases} 1, & \text{si } k = q \text{ y } k \neq i, j \\ 1, & \text{si } (k = i \text{ y } q = j) \text{ o } (k = j \text{ y } q = i) \\ 0, & \text{en los demás casos} \end{cases}$$

Para verificar la igualdad $E \cdot A = B$ (ambas matrices del mismo orden) debemos ver que para toda $k = 1, \ldots, m$ y $\ell = 1, \ldots, n$ los elementos del renglón k y la columna ℓ de cada una de las matrices son iguales. Sea $E \cdot A = (d_{k\ell})$ ($k = 1, \ldots, m$ y $\ell = 1, \ldots, n$)

Si $k \neq i, j$,

$$d_{k\ell} = \sum_{s=1}^{m} c_{ks} a_{s\ell} = 0 \cdot a_{1\ell} + \cdots + 1 \cdot a_{k\ell} + \cdots + 0 \cdot a_{m\ell} = a_{k\ell}$$

Si $k = i$,

$$d_{i\ell} = \sum_{s=1}^{m} c_{is} a_{s\ell} = 0 \cdot a_{1\ell} + \cdots + 1 \cdot a_{j\ell} + \cdots + 0 \cdot a_{m\ell} = a_{j\ell}$$

Si $k = j$,

$$d_{i\ell} = \sum_{s=1}^{m} c_{js}a_{s\ell} = 0 \cdot a_{1\ell} + \cdots + 1 \cdot a_{i\ell} + \cdots + 0 \cdot a_{m\ell} = a_{i\ell}$$

Por lo tanto $E \cdot A = (d_{k\ell})(b_{k\ell}) = B$.

(II) Suponemos que B se obtiene de A al multiplicar el renglón i por $\alpha \neq 0$. Entonces para toda $k = 1, \ldots, m$ y $\ell = 1, \ldots, n$; $b_{k\ell} = a_{k\ell}$ si $k \neq i$ y $b_{i\ell} = \alpha \cdot a_{i\ell}$. En este caso $E = (c_{kq}) \in M_{m\times m}(\mathbb{R})$ es tal que para toda $k = 1, \ldots, m$ y $q = 1, \ldots, m$;

$$c_{kq} = \begin{cases} 1, & \text{si } k = q \neq i \\ \alpha, & \text{si } k = q = i \\ 0, & \text{si } k \neq q \end{cases}$$

Veamos entonces que $E \cdot A = (d_{k\ell}) = (b_{k\ell}) = B$.

Para $k \neq i$, se tiene que

$$d_{k\ell} = \sum_{s=1}^{m} c_{ks}a_{s\ell} = 0 \cdot a_{1\ell} + \cdots + 1 \cdot a_{k\ell} + \cdots + 0 \cdot a_{m\ell} = a_{k\ell}.$$

Para $k = i$,

$$d_{i\ell} = \sum_{s=1}^{m} c_{is}a_{s\ell} = 0 \cdot a_{1\ell} + \cdots + \alpha \cdot a_{i\ell} + \cdots + 0 \cdot a_{m\ell} = \alpha \cdot a_{i\ell} = b_{i\ell}.$$

Luego $E \cdot A = B$.

(III) Supongamos que B se obtiene de A al sumar al renglón i α veces el renglón j. Entonces para todo $k = 1, \ldots, m$ y $\ell = 1, \ldots, n$; $b_{k\ell} = a_{k\ell}$ si $k \neq i$ y $b_{i\ell} = a_{i\ell} + \alpha \cdot a_{j\ell}$ y $E = (c_{kq})$, donde para $k = 1, \ldots, m$ y $q = 1, \ldots, m$,

$$c_{kq} = \begin{cases} 1, & \text{si } k = q \\ \alpha, & \text{si } k = i, q = j \\ 0, & \text{en los demás casos} \end{cases}.$$

Debemos demostrar que $(d_{k\ell}) = (b_{k\ell})$.

Para $k \neq i$,

$$d_{k\ell} = \sum_{s=1}^{m} c_{ks}a_{s\ell} = 0 \cdot a_{1\ell} + \cdots + 1 \cdot a_{k\ell} + \cdots + 0 \cdot a_{m\ell} = a_{k\ell}.$$

Para $k = i$,

$$d_{k\ell} = \sum_{s=1}^{m} c_{is}a_{s\ell} = 0 \cdot a_{1\ell} + \cdots + 1 \cdot a_{i\ell} + \cdots + \alpha \cdot a_{j\ell} + \cdots + 0 \cdot a_{m\ell} = a_{i\ell} + \alpha \cdot a_{j\ell} = b_{i\ell}.$$

Entonces $E \cdot A = B$.

Por último, de manera similar se demuestra el resultado para operaciones elementales por columnas. ∎

Corolario 15.1.22. *Cada matriz elemental es invertible y su inversa es una matriz elemental.*

Demostración. Sea E una matriz elemental. Consideramos cada uno de los tres tipos de operación elemental.

(I) Supongamos que E se obtiene el intercambiar el renglón i por el renglón j. Si en E realizamos esta misma operación obtenemos la matriz identidad. Entonces por el teorema 15.1.21 $E \cdot E = I_{n\times n}$ y por lo tanto E es invertible donde $E^{-1} = E$.

(II) Supongamos que E se obtuvo de $I_{n\times n}$ al multiplicar el renglón i por $\alpha \neq 0$. Si E' es la matriz elemental que resulta de $I_{n\times n}$ al multiplicar el renglón i por α^{-1}. Entonces $E \cdot E' = E' \cdot E = I_{n\times n}$, luego E es invertible y $E' = E^{-1}$.

(III) Supongamos que E se obtiene de $I_{n\times n}$ al sumar al renglón i α veces el renglón j. Si E' es la matriz elemental que resulta de sumar al renglón i $(-\alpha)$ veces el renglón j, entonces $E' \cdot E = E \cdot E' = I_{n\times n}$, luego E es invertible y $E' = E^{-1}$. ∎

Veamos ahora cómo debe ser una matriz escalonada reducida $B \in M_{n\times n}(\mathbb{R})$ que es invertible. Como ya hemos visto (páginas 539-541), si B tiene un renglón que consta únicamente de ceros, entonces B no puede ser invertible, así que la primera conclusión que sacamos es que todos los renglones (y columnas) de B deben ser distintos de cero. Por ser escalonada reducida, B tiene el siguiente aspecto.

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1i} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2i} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots\vdots\vdots & \vdots & \vdots\vdots\vdots & \vdots \\ 0 & 0 & \cdots & a_{ii} & \cdots & a_{in} \\ \vdots & \vdots & \vdots\vdots\vdots & \vdots & \vdots\vdots\vdots & \vdots \\ 0 & 0 & \vdots\vdots\vdots & 0 & \vdots\vdots\vdots & a_{nn} \end{pmatrix}$$

donde, en principio, no necesariamente $a_{ii} \neq 0$. Veamos qué sucede si para alguna $i = 1, \ldots, n$ $a_{ii} = 0$. Es claro por la forma de B que si $a_{nn} = 0$, entonces todos los elementos del renglón n serán cero, que como ya hemos mencionado, esto no puede suceder. Así pues, supongamos que para alguna $i = 1, \ldots, n-1$, $a_{ii} = 0$. Afirmamos que $a_{jj} = 0$ para toda $j = 1, \ldots, n$ y para mostrar esto basta ver que $a_{(i+1)(i+1)} = 0$. Pero esto es inmediato porque el primer elemento distinto de cero, que es 1, aparece en el renglón i en al menos la columna $i + 1$, así que el primer elemento distinto de cero del renglón $i + 1$ debe aparecer más a la derecha de la columna $i+1$ y así se tiene que debe ser $a_{(i+1)(i+1)} = 0$. Sin embargo ya hemos visto por otra parte que debe ser $a_{nn} \neq 0$ lo cual es un absurdo. Concluimos entonces que $a_{ii} = 1$ para toda $i = 1, \ldots, n$ y por otro lado, dadas las características de B, los otros elementos de la columna i deben ser cero. Luego $B = I_{n\times n}$. Entonces tenemos

Lema 15.1.23. *Una matriz invertible $B \in M_{n\times n}(\mathbb{R})$ es escalonada reducida si y sólo si $B = I_{n\times n}$. Es decir, la única matriz escalonada reducida que es invertible es $I_{n\times n}$.*

Teorema 15.1.24. *Sea $A \in M_{n\times n}(\mathbb{R})$, $E_s \cdot \ldots \cdot E_1 \cdot A = B$, donde $E_1, \ldots, E_s$ son matrices elementales y B una matriz escalonada reducida. Si A es invertible, entonces*

$$A^{-1} = E_s \cdot \ldots \cdot E_1.$$

Demostración. Por el corolario 15.1.22, $E_1, \ldots, E_s$ son invertibles, luego por el corolario 15.1.18 $C = E_s \cdot \ldots \cdot E_1$ es invertible, y por la misma razón $C \cdot A = B$ es invertible ya que A lo es por hipótesis. Ahora, por el lema 15.1.23, debe ser $B = I_{n\times n}$ con lo cual tenemos que $C \cdot A = I_{n\times n}$. Por último, por la observación 15.1.13 se tiene que $A^{-1} = E_s \cdot \ldots \cdot E_1$. ∎

Corolario 15.1.25. *Una matriz $A \in M_{n\times n}(\mathbb{R})$ es invertible si y sólo si es producto de matrices elementales.*

Demostración. Si A es producto de matrices elementales, entonces A es invertible. Supongamos ahora que A es invertible y sea B escalonada reducida equivalente a A. Entonces $B = I = E_s \cdot \ldots \cdot E_1 \cdot A$ y por el teorema 15.1.24, $A = E_1^{-1} \cdot \ldots \cdot E_s^{-1}$ donde por cada $i = 1, \ldots, s$, E_i^{-1} es elemental ya que es la inversa de una matriz elemental. ∎

Conclusión. Si $A \in M_{n\times n}(\mathbb{R})$ es una matriz invertible, para encontrar su matriz inversa basta llevarla, mediante operaciones elementales, a la matriz identidad y realizando estas mismas operaciones sobre $I_{n\times n}$, obtenemos la matriz inversa de A (teorema 15.1.24).

Ejemplo 15.1.26. Sea $A = \begin{pmatrix} -1 & 1 & 0 \\ 0 & 1 & -1 \\ 3 & 2 & 1 \end{pmatrix}$

$$\begin{pmatrix} -1 & 1 & 0 \\ 0 & 1 & -1 \\ 3 & 2 & 1 \end{pmatrix} \xrightarrow[(-1)R_1]{} \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 3 & 2 & 1 \end{pmatrix} \xrightarrow[R_3-3R_1]{} \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 5 & 1 \end{pmatrix} \xrightarrow[\substack{R_1+R_2 \\ R_3-5R_2}]{} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 6 \end{pmatrix}$$

$$\xrightarrow[(\frac{1}{6})R_3]{} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow[\substack{R_1+R_3 \\ R_2+R_3}]{} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Ahora realizamos las mismas operaciones elementales sobre $I_{3\times 3}$:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow[(-1)R_1]{} \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow[R_3-3R_1]{} \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 3 & 0 & 1 \end{pmatrix} \xrightarrow[\substack{R_1+R_2 \\ R_3-5R_2}]{} \begin{pmatrix} -1 & 1 & 0 \\ 0 & 1 & 0 \\ 3 & -5 & 1 \end{pmatrix}$$

$$\xrightarrow[(\frac{1}{6})R_3]{} \begin{pmatrix} -1 & 1 & 0 \\ 0 & 1 & 0 \\ \frac{1}{2} & -\frac{5}{6} & \frac{1}{6} \end{pmatrix} \xrightarrow[\substack{R_1+R_3 \\ R_2+R_3}]{} \begin{pmatrix} -\frac{1}{2} & \frac{1}{6} & \frac{1}{6} \\ \frac{1}{2} & \frac{1}{6} & \frac{1}{6} \\ \frac{1}{2} & -\frac{5}{6} & \frac{1}{6} \end{pmatrix}$$

Entonces $A^{-1} = \begin{pmatrix} -\frac{1}{2} & \frac{1}{6} & \frac{1}{6} \\ \frac{1}{2} & \frac{1}{6} & \frac{1}{6} \\ \frac{1}{2} & -\frac{5}{6} & \frac{1}{6} \end{pmatrix}$.

Ejemplo 15.1.27. Sea $A = \begin{pmatrix} 1 & 0 & 1 & -1 \\ 2 & -1 & 3 & 2 \\ 1 & 7 & -4 & -5 \\ 3 & 5 & 0 & 1 \end{pmatrix}$

$$\begin{pmatrix} 1 & 0 & 1 & -1 \\ 2 & -1 & 3 & 2 \\ 1 & 7 & -4 & -5 \\ 3 & 5 & 0 & 1 \end{pmatrix} \overset{\substack{R_2-2R_1 \\ R_3-R_1 \\ R_4-3R_1}}{\sim} \begin{pmatrix} 1 & 0 & 1 & -1 \\ 0 & -1 & 1 & 4 \\ 0 & 7 & -5 & -4 \\ 0 & 5 & -3 & 4 \end{pmatrix} \overset{\substack{R_3+7R_2 \\ R_4+5R_2}}{\sim} \begin{pmatrix} 1 & 0 & 1 & -1 \\ 0 & -1 & 1 & 4 \\ 0 & 0 & 2 & 24 \\ 0 & 0 & 2 & 24 \end{pmatrix} \overset{(-1)\cdot R_2}{\sim}$$

$$\begin{pmatrix} 1 & 0 & 1 & -1 \\ 0 & 1 & -1 & -4 \\ 0 & 0 & 2 & 24 \\ 0 & 0 & 2 & 24 \end{pmatrix} \overset{\left(\frac{1}{2}\right)\cdot R_3}{\sim} \begin{pmatrix} 1 & 0 & 1 & -1 \\ 0 & 1 & -1 & -4 \\ 0 & 0 & 1 & 12 \\ 0 & 0 & 2 & 24 \end{pmatrix} \overset{\substack{R_1-R_3 \\ R_2+R_3 \\ R_4-2R_3}}{\sim} \begin{pmatrix} 1 & 0 & 0 & -13 \\ 0 & 1 & 0 & 8 \\ 0 & 0 & 1 & 12 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Al llevar a la matriz A a la forma escalonada reducida mediante operaciones elementales por renglones la matriz resultante tiene un renglón que consta únicamente de ceros, razón por la cual no es invertible y por lo tanto A tampoco lo es.

Es importante mencionar que el trabajo aquí ha sido únicamente con operaciones elementales sobre renglones, lo mismo puede hacerse con operaciones elementales sobre columnas con la adecuación que corresponde y los resultados serán básicamente los mismos como por ejemplo que cada matriz puede ser llevada a una matriz escalonada reducida mediante operaciones elementales sobre columnas lo que es equivalente a multiplicar por la derecha la matriz original por las matrices elementales correspondientes. La razón por la cual trabajamos con operaciones elementales por renglones es debido a nuestro objetivo inicial que es el de estudiar sistemas de ecuaciones lineales y que en este caso no nos es de utilidad hacer el trabajo con columnas.

§ 15.2. Transformaciones lineales

En esta sección introduciremos las así llamadas transformaciones lineales (cierto tipo de funciones) entre espacios vectoriales y cuyo estudio nos permitirá obtener un panorama de los sistemas de ecuaciones lineales desde este punto de vista. Comenzamos entonces dando la definición de este concepto general para espacios vectoriales sobre $\mathbb{R}$ (ver definición de espacio vectorial sobre $\mathbb{R}$ en el ejercicio 14.2.3)

Sean V y W espacios vectoriales sobre $\mathbb{R}$ y $T : V \longrightarrow W$ una función

Definición 15.2.1. *Diremos que T es una* **transformación lineal** *si para cualesquiera $\overline{s}, \overline{s}' \in V$ y $\alpha \in \mathbb{R}$*

(*i*) $T(\overline{s}+\overline{s}') = T(\overline{s}) + T(\overline{s}')$ *y*
(*ii*) $T(\alpha \cdot \overline{s}) = \alpha \cdot T(\overline{s})$.

Las transformaciones lineales serán entonces aquellas funciones que respetan la estructura de espacios vectoriales.

Ejemplo 15.2.2. La función identidad $1_{\mathbb{R}^n} : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ es evidentemente una transformación lineal:

i) $1_{\mathbb{R}^n}(\overline{s}+\overline{s}') = \overline{s}+\overline{s}' = 1_{\mathbb{R}^n}(\overline{s}) + 1_{\mathbb{R}^n}(\overline{s}')$ y
ii) $1_{\mathbb{R}^n}(\alpha \cdot \overline{s}) = \alpha \cdot \overline{s} = \alpha \cdot 1_{\mathbb{R}^n}(\overline{s})$.

Ejemplo 15.2.3. La función constante $\widetilde{0} : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ con $\widetilde{0}(\overline{s}) = \overline{0} \in \mathbb{R}^n$ para toda $\overline{s} \in \mathbb{R}^n$ es una transformación lineal:

i) $\widetilde{0}(\overline{s}+\overline{s}') = \overline{0} = \overline{0}+\overline{0} = \widetilde{0}(\overline{s}) + \widetilde{0}(\overline{s}')$ y
ii) $\widetilde{0}(\alpha \cdot \overline{s}) = \overline{0} = \alpha \cdot \overline{0} = \alpha \cdot \widetilde{0}(\overline{s})$.

Ejemplo 15.2.4. Sea $T : \mathbb{R}^3 \longrightarrow \mathbb{R}^4$ definida por

$$T((x,y,z)) = (x+y+z, x+y, x+z, y+z)$$

es una función lineal:

$$\begin{array}{l} T((x_1,y_1,z_1)+(x_2,y_2,z_2)) = \\ T(x_1+x_2, y_1+y_2, z_1+z_2) = \\ (x_1+x_2+y_1+y_2+z_1+z_2, x_1+x_2+y_1+y_2, x_1+x_2+z_1+z_2, y_1+y_2+z_1+z_2) = \\ (x_1+y_1+z_1, x_1+y_1, x_1+z_1, y_1+z_1)+(x_2+y_2+z_2, x_2+y_2, x_2+z_2, y_2+z_2) = \\ T((x_1,y_1,z_1)) + T((x_2,y_2,z_2)). \end{array}$$

y

$$\begin{array}{rcl} T(\alpha \cdot (x,y,z)) = & T((\alpha x, \alpha y, \alpha z)) \\ & = & (\alpha x+\alpha y+\alpha z, \alpha x+\alpha y, \alpha x+\alpha z, \alpha y+\alpha z) \\ & = & (\alpha(x+y+z), \alpha(x+y), \alpha(x+z), \alpha(y+z)) \\ & = & \alpha \cdot (x+y+z, x+y, x+z, y+z) \\ & = & \alpha \cdot T((x,y,z)) \end{array}$$

Ejemplo 15.2.5. La función $T : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ dada por $T(x,y) = (x,1)$ no es lineal puesto que $T((x_1+y_1)+(x_2+y_2)) = T(x_1+x_2, y_1+y_2) = (x_1+x_2, 1)$ y por otro lado

$$T((x_1+y_1)) + T((x_2+y_2)) = (x_1,1)+(x_2,1) = (x_1+x_2, 2) \neq (x_1+x_2, 1).$$

Con el fin de presentar le siguiente ejemplo que es sumamente importante y que en realidad forma parte de la teoría convendremos en lo siguiente.
Cada vector $(x_1, \ldots, x_n) \in \mathbb{R}^n$ lo podemos representar también como una matriz de orden $n \times 1$ $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ y esta representación no da lugar a ningún problema puesto que su comportamiento en ambos casos es exactamente el mismo, es decir,

(1) $(x_1, \ldots, x_n) = (y_1, \ldots, y_n)$ si y sólo si $x_i = y_i$ para toda $i = 1, \ldots, n$.
$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$ si y sólo si $x_i = y_i$ para toda $i = 1, \ldots, n$.
(2) $(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$.
$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix}$.
(3) $\alpha \cdot (x_1, \ldots, x_n) = (\alpha x_1, \ldots, \alpha x_n)$.
$\alpha \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \alpha x_1 \\ \vdots \\ \alpha x_n \end{pmatrix}$.

Ejemplo 15.2.6. Sea $A \in M_{m\times n}(\mathbb{R})$. Definimos $L_A : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ de la siguiente manera $L_A((x_1, \ldots, x_n)) = A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^m$. Esta función está bien definida ya que por ser A de orden $m \times n$ y $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ de orden $n \times 1$, el producto de ellas está definido y es de orden $m \times 1$.
Afirmamos que L_A es una transformación lineal. Sean

$$(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in \mathbb{R}^n$$

y $\alpha \in \mathbb{R}$. Entonces

(i)

$$\begin{aligned}
L_A((x_1,\ldots,x_n)+(y_1,\ldots,y_n)) &= L_A((x_1+y_1,\ldots,x_n+y_n)) \\
&= A\cdot\begin{pmatrix} x_1+y_1 \\ \vdots \\ x_n+y_n \end{pmatrix} \\
&= A\cdot\left[\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}+\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}\right] \\
&= A\cdot\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}+A\cdot\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \\
&= L_A((x_1,\ldots,x_n))+L_A((y_1,\ldots,y_n))
\end{aligned}$$

(ii)

$$\begin{aligned}
L_A(\alpha\cdot(x_1,\ldots,x_n)) &= L_A((\alpha x_1,\ldots,\alpha x_n)) \\
&= A\cdot\begin{pmatrix} \alpha x_1 \\ \vdots \\ \alpha x_n \end{pmatrix} \\
&= A\cdot\left(\alpha\cdot\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}\right) \\
&= \alpha\cdot\left(A\cdot\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}\right) \\
&= \alpha\cdot L_A((x_1,\ldots,x_n)).
\end{aligned}$$

Entonces cada matriz $A \in M_{m\times n}(\mathbb{R})$ determina una transformación lineal $L_A : \mathbb{R}^n \longrightarrow \mathbb{R}^m$. Más adelante veremos la gran importancia que tiene este ejemplo.

Veamos las consecuencias inmediatas de la definición de transformación lineal.

Proposición 15.2.7. *Sean V y W espacios vectoriales sobre $\mathbb{R}$ y $T : V \longrightarrow W$ transformación lineal. Entonces*

(1) $T\left(\overline{0}\right) = \overline{0}'$;

(2) $T(-v) = -T(v)$,
donde $\overline{0}$ *es el neutro aditivo de* V *y* $\overline{0}'$ *el neutro aditivo de* W, $-v$ *el inverso aditivo de* v *y* $-T(v)$ *el inverso aditivo de* $T(v)$.

Demostración.
(1) $\overline{0}' + T\left(\overline{0}\right) = T\left(\overline{0}\right) = T\left(\overline{0} + \overline{0}\right) = T\left(\overline{0}\right) + T\left(\overline{0}\right)$. Cancelando $T\left(\overline{0}\right)$ en ambos lados de la igualdad obtenemos $T\left(\overline{0}\right) = \overline{0}'$.
(2) $\overline{0}' = T\left(\overline{0}\right) = T(v + (-v)) = T(v) + T(-v)$. Como el inverso aditivo es único entonces $T(-v) = -T(v)$. ∎

Como las transformaciones lineales son funciones, podemos considerar la composición de éstas cuando ésta esté definida.

Teorema 15.2.8*. Sean* V, W *y* U *espacios vectoriales sobre* $\mathbb{R}$ *y* $T : V \longrightarrow W$, $G : W \longrightarrow U$ *transformaciones lineales. Entonces* $G \circ T : V \longrightarrow U$ *es una transformación lineal.*

Demostración. Sean $\overline{s}, \overline{s}' \in V$ y $\alpha \in \mathbb{R}$. Entonces
(*i*)

$$\begin{aligned}(G \circ T)(\overline{s} + \overline{s}') &= G(T(\overline{s} + \overline{s}')) \\ &= G(T(\overline{s}) + T(\overline{s}')) \\ &= G(T(\overline{s})) + G(T(\overline{s}')) \\ &= (G \circ T)(\overline{s}) + (G \circ T)(\overline{s}').\end{aligned}$$

(*ii*) $(G \circ T)(\alpha\overline{s}) = G(T(\alpha\overline{s})) = G(\alpha T(\overline{s})) = \alpha G(T(\overline{s})) = \alpha(G \circ T)(\overline{s})$. ∎

De aquí en adelante cuando hablemos de una transformación lineal $T : V \longrightarrow W$ daremos por hecho que V y W son espacios vectoriales sobre $\mathbb{R}$; además $\overline{0}$ denotarán al neutro aditivo de un espacio vectorial V, sin importar quién es V. Dada una transformación lineal $T : V \longrightarrow W$ ésta determina un subespacio de V que denotamos por $\boldsymbol{N(T)}$ y su definición es

Definición 15.2.9*. El* **núcleo** *de una transformación lineal* $T : V \longrightarrow W$ *es*

$$N(T) = \left\{ \overline{s} \in V \mid T(\overline{s}) = \overline{0} \right\}.$$

Proposición 15.2.10*. Si* $T : V \longrightarrow W$ *es una transformación lineal, entonces* $N(T)$ *es un subespacio de* V *y su imagen* $Im(T)$ *es un subespacio de* W.

Demostración. $N(T)$ es un subespacio de V
(*i*) $\overline{0} \in N(T)$ por la proposición 15.2.7.

(*ii*) si $\overline{s}, \overline{s}' \in N(T)$, entonces $T(\overline{s}) = \overline{0} = T(\overline{s}')$ y por lo tanto

$$T(\overline{s} + \overline{s}') = T(\overline{s}) + T(\overline{s}') = \overline{0} + \overline{0} = \overline{0}$$

y así $\overline{s} + \overline{s}' \in N(T)$.

(*iii*) si $\alpha \in \mathbb{R}$ y $\overline{s} \in N(T)$, entonces $T(\alpha\overline{s}) = \alpha \cdot T(\overline{s}) = \alpha \cdot \overline{0} = \overline{0}$. Luego $\alpha \cdot \overline{s} \in N(T)$.

$Im(T)$ es un subespacio de W

(*i*) $\overline{0} \in Im(T)$ ya que $T(\overline{0}) = \overline{0}$.

(*ii*) Si $\overline{t}, \overline{t}' \in Im(T)$, por definición $\overline{t} = T(\overline{s})$ y $\overline{t}' = T(\overline{s}')$ para alguna $\overline{s} \in V$ y alguna $\overline{s}' \in V$. Entonces $\overline{t} + \overline{t}' = T(\overline{s}) + T(\overline{s}') = T(\overline{s} + \overline{s}')$ por lo tanto $\overline{t} + \overline{t}' \in Im(T)$.

(*iii*) Si $\alpha \in \mathbb{R}$ y $\overline{t} \in Im(T)$, entonces $\overline{t} = T(\overline{s})$. Luego $\alpha \cdot \overline{t} = \alpha \cdot T(\overline{s}) = T(\alpha\overline{s})$ y así $\alpha \cdot \overline{t} \in Im(T)$. ∎

Como función, una transformación lineal $T : V \longrightarrow W$ podría se inyectiva o suprayectiva. Sabemos que T será suprayectiva si y sólo si $Im(T) = W$. De manera similar, el núcleo de T, $N(T)$, nos indica si T es inyectiva.

Proposición 15.2.11. *Sea $T : V \longrightarrow W$ es una transformación lineal. T es inyectiva si y sólo si $N(T) = \{\overline{0}\}$.*

Demostración.

$\Longrightarrow$) Supongamos que T es inyectiva y sea $v \in N(T)$. Entonces, por definición, $T(v) = \overline{0}$. Pero también $T(\overline{0}) = \overline{0}$. Luego debe ser $v = \overline{0}$ y por lo tanto $N(T) = \{\overline{0}\}$.

$\Longleftarrow$) Supongamos que $N(T) = \{\overline{0}\}$ y supongamos $v, v' \in V$ tales que $T(v) = T(v')$. Entonces $\overline{0} = T(v) - T(v') = T(v - v')$. Luego $v - v' \in N(T) = \{\overline{0}\}$. Esto es $v - v' = \overline{0}$ que es $v = v'$. ∎

Proposición 15.2.12. *Si $T : V \longrightarrow W$ es una transformación lineal y $\{v_1, \ldots, v_n\}$ una base de V, entonces $\{T(v_1), \ldots, T(v_n)\}$ genera a $Im(T)$.*

Demostración. Sea S el espacio generado por $T(v_1), \ldots, T(v_n)$.

1°/ Sea $w \in S$.Entonces $w = \alpha_1 T(v_1) + \cdots + \alpha_n T(v_n) = T(\alpha_1 v_1 + \cdots + \alpha_n v_n)$. Luego $w \in Im(T)$.

2°/ Sea $w \in Im(T)$. Entonces $w = T(v)$ para algún $v \in V$. Como $\{v_1, \ldots, v_n\}$ una base de V, tenemos que $v = \alpha_1 v_1 + \cdots + \alpha_n v_n$ y

$$\begin{aligned} w = T(v) &= T(\alpha_1 v_1 + \cdots + \alpha_n v_n) \\ &= \alpha_1 T(v_1) + \cdots + \alpha_n T(v_n). \end{aligned}$$

Y por consiguiente $w \in S$. ∎

Definición 15.2.13. *Una transformación lineal $T : V \longrightarrow W$ se llama* **isomorfismo** *si T es biyectiva. Diremos que V y W son espacios vectoriales isomorfos y lo denotaremos por $\boldsymbol{V \cong W}$ si existe un isomorfismo de V en W.*

Entonces una transformación lineal $T : V \longrightarrow W$ es un isomorfismo si y sólo si $N(T) = \left\{\overline{0}\right\}$ y $Im(T) = W$. Un isomorfismo entre dos espacios vectoriales nos lleva a considerarlos iguales desde el punto de vista estructural y esto significará que la única diferencia entre ellos puede ser la naturaleza de los elementos pero como espacios vectoriales tendrán ambos las mismas características.

Proposición 15.2.14. *Si $T : V \longrightarrow W$ es un isomorfismo de espacios vectoriales sobre $\mathbb{R}$. Entonces*

(*i*) *$\{v_1, \ldots, v_n\}$ genera a V si y sólo si $\{T(v_1), \ldots, T(v_n)\}$ genera a W.*
(*ii*) *$\{v_1, \ldots, v_n\}$ es linealmente independiente V si y sólo si $\{T(v_1), \ldots, T(v_n)\}$ es linealmente independiente.*
(*iii*) *$\{v_1, \ldots, v_n\}$ es base de V si y sólo si $\{T(v_1), \ldots, T(v_n)\}$ es base de W.*

Demostración.

(*i*)
$\Longrightarrow$) Supongamos que $\{v_1, \ldots, v_n\}$ genera a V y sea $w \in W$. Como T es isomorfismo, entonces existe $v \in V$ tal que $T(v) = w$. Luego, por hipótesis, existen $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$ tales que $v = \alpha_1 v_1 + \cdots + \alpha_n v_n$ y entonces

$$w = T(v) = T(\alpha_1 v_1 + \cdots + \alpha_n v_n) = \alpha_1 T(v_1) + \cdots + \alpha_n T(v_n).$$

Puesto que w fue arbitrario, concluimos que $T(v_1), \ldots, T(v_n)$ generan a W.
$\Longleftarrow$) Supongamos que $T(v_1), \ldots, T(v_n)$ generan a W y sea $v \in V$. Entonces $T(v) \in W$ y por hipótesis, existen $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$ tales que

$$T(v) = \alpha_1 T(v_1) + \cdots + \alpha_n T(v_n) = T(\alpha_1 v_1 + \cdots + \alpha_n v_n).$$

Ahora por ser T inyectiva debe ser $v = \alpha_1 v_1 + \cdots + \alpha_n v_n$.
(*ii*)
$\Longrightarrow$) Supongamos que $v_1, \ldots, v_n$ son linealmente independientes y sea

$$\alpha_1 T(v_1) + \cdots + \alpha_n T(v_n) = \overline{0}.$$

Entonces $T(\alpha_1 v_1 + \cdots + \alpha_n v_n) = \overline{0}$ y por ser T inyectiva debe ser

$$\alpha_1 v_1 + \cdots + \alpha_n v_n = \overline{0}.$$

Esta última igualdad implica, por hipótesis, que $\alpha_1 = \cdots = \alpha_n = 0$. Luego $T(v_1), \ldots, T(v_n)$ son linealmente independientes.
$\Longleftarrow$) Supongamos $T(v_1), \ldots, T(v_n)$ linealmente independientes y supongamos que $\alpha_1 v_1 + \cdots + \alpha_n v_n = \overline{0}$. Entonces

$$\overline{0} = T\left(\overline{0}\right) = T(\alpha_1 v_1 + \cdots + \alpha_n v_n) = \alpha_1 T(v_1) + \cdots + \alpha_n T(v_n).$$

Luego, por hipótesis, $\alpha_1 = \cdots = \alpha_n = 0$.
(*iii*) Es inmediato de (*i*) y (*ii*).∎

Corolario 15.2.15. *Si $T : V \longrightarrow V$ es un isomorfismo, entonces*

$$\dim_{\mathbb{R}} V = \dim_{\mathbb{R}} W.$$

Como consecuencia de la demostración de éste último teorema tenemos la siguiente

Corolario 15.2.16. *Sea $T : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ una transformación lineal inyectiva. Entonces* $\dim_{\mathbb{R}} Im(T) = n$

Demostración. Si $T : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ es inyectiva, $T' : \mathbb{R}^n \longrightarrow Im(T)$ definida por $T'(v) = T(v)$ es un isomorfismo y así $n = \dim_{\mathbb{R}} \mathbb{R}^n = \dim_{\mathbb{R}} Im(T)$. ∎

Corolario 15.2.17. *$\mathbb{R}^n$ y $\mathbb{R}^m$ son isomorfismos si y sólo si $n = m$.*

Demostración.

$\Longrightarrow$) Sabemos que cualquier base de $\mathbb{R}^n$ tiene n elementos y cualquier base de $\mathbb{R}^m$ tiene m elementos. Si T es un isomorfismo; por la proposición 15.2.14, $\{v_1, \ldots, v_n\}$ es base de $\mathbb{R}^n$ si y sólo si $\{T(v_1), \ldots, T(v_n)\}$ es base de $\mathbb{R}^m$ y por lo tanto $m = n$.
$\Longleftarrow$) Si $n = m$, $1_{\mathbb{R}^n} : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ es un isomorfismo. ∎

Teorema 15.2.18. *Si $T : V \longrightarrow W$ es un isomorfismo y $T^{-1} : W \longrightarrow V$ es la función inversa de T, entonces T^{-1} es lineal y por lo tanto también un isomorfismo.*

Demostración. Por ser T biyectiva, existe su función inversa $T^{-1} : W \longrightarrow V$ y está definida como sigue para cada $w \in W$; $T^{-1}(w) = v$ donde v es el único elemento de V tal que $T(v) = w$.
Sean $w, w' \in W$ y $v, v' \in V$ tales que $T(v) = w$ y $T(v') = w'$. Entonces

$$T(v + v') = T(v) + T(v') = w + w'$$

y por lo tanto $T^{-1}(w + w') = v + v' = T^{-1}(w) + T^{-1}(w')$.

Ahora si $\alpha \in \mathbb{R}$, $w \in W$ y $v \in V$ tal que $T(v) = w$, entonces $T(\alpha \cdot v) = \alpha \cdot T(v) = \alpha \cdot w$ y de aquí tenemos que $T^{-1}(\alpha \cdot w) = \alpha \cdot v = \alpha \cdot T^{-1}(w)$.
Por lo tanto T es lineal y por ser T^{-1} biyectiva, entonces T^{-1} es un isomorfismo.∎

Teorema 15.2.19. *Sea $T : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ una transformación lineal. Entonces*

$$\dim_{\mathbb{R}} N(T) + \dim_R Im(T) = n.$$

Demostración. Sea $\{v_1, \ldots, v_k\}$ una base de $N(T)$. Por la proposición 14.2.36 podemos extender este conjunto linealmente independiente a una base de $\mathbb{R}^n$, es decir existen $v_{k+1}, \ldots, v_n \in \mathbb{R}^n$ tales que $\{v_1, \ldots, v_k, v_{k+1}, \ldots, v_n\}$ es una base de $\mathbb{R}^n$ (recordamos que cualquier base de $\mathbb{R}^n$ tiene n elementos). Si demostramos que $\{T(v_{k+1}), \ldots, T(v_n)\}$ es una base de $Im(T)$, entonces $\dim_{\mathbb{R}} Im(T) = n - k$ y tendremos el resultado.

$1°/$ $\{T(v_{k+1}), \ldots, T(v_n)\}$ genera a $Im(T)$
Sea $w \in Im(T)$. Entonces $w = T(v)$ para alguna $v \in V$. Como $\{v_1, \ldots, v_k, v_{k+1}, \ldots, v_n\}$ es una base de $\mathbb{R}^n$, existen $\alpha_1, \ldots, \alpha_k, \alpha_{k+1}, \ldots, \alpha_n \in \mathbb{R}$ tales que

$$v = \alpha_1 v_1 + \cdots + \alpha_k v_k + \alpha_{k+1} v_{k+1} + \cdots + \alpha_n v_n.$$

Luego

$$\begin{aligned} w &= T(v) \\ &= T(\alpha_1 v_1 + \cdots + \alpha_k v_k + \alpha_{k+1} v_{k+1} + \cdots + \alpha_n v_n) \\ &= \alpha_1 T(v_1) + \cdots + \alpha_k T(v_k) + \alpha_{k+1} T(v_{k+1}) + \cdots + \alpha_n T(v_n) \\ &= \alpha_{k+1} T(v_{k+1}) + \cdots + \alpha_n T(v_n) \end{aligned}$$

donde la última igualdad es porque $\alpha_1 v_1 + \cdots + \alpha_k v_k \in N(T)$.
$2°/$ $\{T(v_{k+1}), \ldots, T(v_n)\}$ es linealmente independiente
Sea $\alpha_{k+1} T(v_{k+1}) + \cdots + \alpha_n T(v_n) = \overline{0}$. Entonces $T(\alpha_{k+1} v_{k+1} + \cdots + \alpha_n v_n) = \overline{0}$ y por lo tanto $\alpha_{k+1} v_{k+1} + \cdots + \alpha_n v_n \in N(T)$l Luego por ser $\{v_1, \ldots, v_k\}$ base de $N(T)$ existen $\alpha_1, \ldots, \alpha_k \in \mathbb{R}$ tales que $\alpha_{k+1} v_{k+1} + \cdots + \alpha_n v_n = \alpha_1 v_1 + \cdots + \alpha_k v_k$ y de aquí se tiene

$$(-\alpha_1) v_1 + \cdots + (-\alpha_k) v_k + \alpha_{k+1} v_{k+1} + \cdots + \alpha_n v_n = \overline{0},$$

lo que implica que $\alpha_1 = \cdots = \alpha_k = \alpha_{k+1} = \cdots = \alpha_n = 0$ por ser

$$\{v_1, \ldots, v_k, v_{k+1}, \ldots, v_n\}$$

base de $\mathbb{R}^n$. Luego $\{T(v_{k+1}), \ldots, T(v_n)\}$ es linealmente independiente.

Concluimos entonces que $\dim_{\mathbb{R}} n - k$.
Por último $n = k + (n-k) = \dim_{\mathbb{R}} N(T) + \dim_{\mathbb{R}} Im(T)$. ∎

Corolario 15.2.20. *Si $T : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ es una transformación lineal, entonces* $\dim_{\mathbb{R}} Im(T) \leq \text{mín}\{n, m\}$.

Corolario 15.2.21. *Sea $T : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ una transformación lineal. Las siguientes afirmaciones son equivalentes*

(1) *T es inyectiva.*
(2) *T es suprayectiva.*
(3) *T es isomorfismo.*

Demostración.

(1) $\Longrightarrow$ (2) Como T es inyectiva, $N(T) = \left\{\overline{0}\right\}$, así que por el teorema 15.2.19 $n = \dim_{\mathbb{R}} N(T) + \dim_{\mathbb{R}} Im(T) = \dim_{\mathbb{R}} Im(T)$ y por el teorema 14.2.44 $Im(T) = \mathbb{R}^n$. Luego T es suprayectiva.
(2) $\Longrightarrow$ (3) Como T es suprayectiva, entonces $\dim_{\mathbb{R}} Im(T) = n$. Luego por el teorema 15.2.19, $n = \dim_{\mathbb{R}} N(T) + \dim_{\mathbb{R}} Im(T) = \dim_{\mathbb{R}} N(T) + n$. Por lo tanto $\dim_{\mathbb{R}} N(T) = 0$ lo que significa que $N(T) = \left\{\overline{0}\right\}$. Entonces T es inyectiva.
(3) $\Longrightarrow$ (1) Inmediato. ∎

En el siguiente resultado veremos que para dar una transformación lineal $T : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ es suficiente conocer $T(v_1), \ldots, T(v_n)$ para alguna base $\{v_1, \ldots, v_n\}$ de $\mathbb{R}^n$. Esto es, cualquier transformación lineal está determinada por los valores que toma en una base.

Teorema 15.2.22. *Sea $\{v_1, \ldots, v_n\}$ una base de $\mathbb{R}^n$ y $w_1, \ldots, w_n$ vectores arbitrarios de $\mathbb{R}^m$. Entonces existe una única transformación lineal $T : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ tal que $T(v_i) = w_i$ para $i = 1, \ldots, n$.*

Demostración. Existencia: Definimos $T : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ como sigue: para $v \in \mathbb{R}^n$, si $v = \alpha_1 v_1 + \cdots + \alpha_n v_n$, $T(v) = \alpha_1 w_1 + \cdots + \alpha_n w_n$. Veamos que T está bien definida, T es lineal y $T(v_i) = w_i$ para $i = 1, \ldots, n$.

1°/ T esta bien definida porque al ser $\{v_1, \ldots, v_n\}$ una base de $\mathbb{R}^n$, los elementos $\alpha_1, \ldots, \alpha_n$ quedan determinados de manera única por v (véase el teorema 14.2.31).
2°/ T es lineal. Para ver esto sean $v = \alpha_1 v_1 + \cdots + \alpha_n v_n$ y $v' = \beta_1 v_1 + \cdots + \beta_n v_n$ vectores arbitrarios de $\mathbb{R}^n$ y $\gamma \in \mathbb{R}$.

(*i*)
$$\begin{aligned} T(v+v') &= T((\alpha_1+\beta_1)v_1+\cdots+(\alpha_n+\beta_n)v_n) \\ &= (\alpha_1+\beta_1)w_1+\cdots+(\alpha_n+\beta_n)w_n \\ &= (\alpha_1w_1+\cdots+\alpha_nw_n)+(\beta_1w_1+\cdots+\beta_nw_n) \\ &= T(v)+T(v'). \end{aligned}$$

(*ii*)
$$\begin{aligned} T(\gamma\cdot v) &= T(\gamma\alpha_1v_1+\cdots+\gamma\alpha_nv_n) \\ &= \gamma\alpha_1w_1+\cdots+\gamma\alpha_nw_n \\ &= \gamma\cdot(\alpha_1v_1+\cdots+\alpha_nv_n) \\ &= \gamma\cdot T(v). \end{aligned}$$

3°/ Para cada $i=1,\ldots,n$, $v_i = 0\cdot v_1+\cdots+0\cdot v_{i-1}+1\cdot v_i+0\cdot v_{i+1}+\cdots+0\cdot v_n$.
Entonces $T(v_i) = 0\cdot w_1+\cdots+0\cdot w_{i-1}+1\cdot w_i+0\cdot w_{i+1}+\cdots+0\cdot w_n = w_i$.

Unicidad: Supongamos que también $G:\mathbb{R}^n\longrightarrow\mathbb{R}^m$ es una transformación lineal tal que $G(v_i)=w_i$ para $i=1,\ldots,n$ y sea $v=\alpha_1v_1+\cdots+\alpha_nv_n$. Entonces

$$\begin{aligned} G(v) &= G(\alpha_1v_1+\cdots+\alpha_nv_n) &&= \alpha_1G(v_1)+\cdots+\alpha_nG(v_n) \\ &= \alpha_1w_1+\cdots+\alpha_nw_n &&= \alpha_1T(v_1)+\cdots+\alpha_nT(v_n) \\ &= T(\alpha_1v_1+\cdots+\alpha_nv_n) &&= T(v). \end{aligned}$$

Como esto es para cada $v\in\mathbb{R}^n$, entonces $G=T$. ∎

Es inmediato de este último teorema:

Corolario 15.2.23. *Sean $T,G:\mathbb{R}^n\longrightarrow\mathbb{R}^m$ transformaciones lineales y una base de $\mathbb{R}^n$ dada por los vectores $\{v_1,\ldots,v_n\}$. Entonces $T=G$ si y sólo si $T(v_i)=G(v_i)$ para toda $i=1,\ldots,n$.*

En el ejemplo 15.2.6 vimos que cada matriz $A\in M_{m\times n}(\mathbb{R})$ da lugar a una transformación lineal $L_A:\mathbb{R}^n\longrightarrow\mathbb{R}^m$ y mencionamos ahí que este ejemplo es de gran importancia. En lo que sigue veremos el por qué de esta afirmación.
Sea $T:\mathbb{R}^n\longrightarrow\mathbb{R}^m$ una transformación lineal y consideremos $S_0=\{\overline{e}_1,\ldots,\overline{e}_n\}$ y $S_1=\{\overline{e}'_1,\ldots,\overline{e}'_m\}$ las bases canónicas de $\mathbb{R}^n$ y $\mathbb{R}^m$ respectivamente (véase el ejemplo 14.2.32). Por el teorema 15.2.22 T queda determinada por los valores $T(\overline{e}_1),\ldots,T(\overline{e}_n)$ y como estos son elementos de $\mathbb{R}^m$ cada uno de ellos es combinación lineal de los elementos de la base S_1:

$$\begin{array}{ccccccccc} T(\overline{e}_1) & = & a_{11}\overline{e}'_1 & + & a_{21}\overline{e}'_2 & + & \cdots & + & a_{m1}\overline{e}'_m \\ T(\overline{e}_2) & = & a_{12}\overline{e}'_1 & + & a_{22}\overline{e}'_2 & + & \cdots & + & a_{m2}\overline{e}'_m \\ \vdots & & \vdots & & \vdots & & \vdots\vdots\vdots & & \vdots \\ T(\overline{e}_n) & = & a_{1n}\overline{e}'_1 & + & a_{2n}\overline{e}'_2 & + & \cdots & + & a_{mn}\overline{e}'_m \end{array}$$

Queda claro entonces que conociendo los escalares $a_{ij}, \ldots, a_{mj}$ obtenemos el valor de $T(\overline{e}_j)$ para cada $j = 1, \ldots, n$. Por lo tanto la información sobre T está dada en la siguiente matriz que denotamos $\boldsymbol{M(T)}$ y a la que llamamos la ***matriz asociada a T*** respecto a las bases canónicas de $\mathbb{R}^n$ y $\mathbb{R}^m$.

$$M(T) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots\vdots\vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \in M_{m\times n}(\mathbb{R})$$

Ejemplo 15.2.24. Sea $T = 1_{\mathbb{R}^n}$ la transformación lineal identidad de $\mathbb{R}^n$

$$\begin{array}{rcccccccccc} 1_{\mathbb{R}^n}(\overline{e}_1) & = & \overline{e}_1 & = & 1\cdot\overline{e}'_1 & + & 0\cdot\overline{e}'_2 & + & \cdots & + & 0\cdot\overline{e}'_m \\ 1_{\mathbb{R}^n}(\overline{e}_2) & = & \overline{e}_2 & = & 0\cdot\overline{e}'_1 & + & 1\cdot\overline{e}'_2 & + & \cdots & + & 0\cdot\overline{e}'_m \\ \vdots & & \vdots & & \vdots & & \vdots & & \vdots\vdots\vdots & & \vdots \\ 1_{\mathbb{R}^n}(\overline{e}_n) & = & \overline{e}_3 & = & 0\cdot\overline{e}'_1 & + & 0\cdot\overline{e}'_2 & + & \cdots & + & 1\cdot\overline{e}'_m \end{array}$$

Entonces

$$M(1_{\mathbb{R}^n}) = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots\vdots\vdots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} = I_{n\times n}$$

Luego la matriz asociada a la identidad en $\mathbb{R}^n$ es la matriz identidad $I_{n\times n}$

Ejemplo 15.2.25. Sea $T : \mathbb{R}^3 \longrightarrow \mathbb{R}^4$ definida por

$$T(a_1, a_2, a_3) = (a_1 + a_2, a_1 + a_3, a_2 + a_3, 2a_1).$$

Entonces T es lineal. Encontremos $M(T)$. Sean $\{\overline{e}_1 = (1,0,0),\ \overline{e}_2 = (0,1,0),\ \overline{e}_3 = (0,0,1)\}$ y $\{\overline{e}'_1 = (1,0,0,0),\ \overline{e}'_2 = (0,1,0,0),\ \overline{e}'_3 = (0,0,1,0),\ \overline{e}'_4 = (0,0,0,1)\}$ las bases canónicas de $\mathbb{R}^3$ y $\mathbb{R}^4$ respectivamente.

$$\begin{aligned} T(\overline{e}_1) = T(1,0,0) &= (1,1,0,2) = 1\cdot\overline{e}'_1 + 1\cdot\overline{e}'_2 + 0\cdot\overline{e}'_3 + 2\cdot\overline{e}'_4 \\ T(\overline{e}_2) = T(0,1,0) &= (1,0,1,0) = 1\cdot\overline{e}'_1 + 0\cdot\overline{e}'_2 + 1\cdot\overline{e}'_3 + 0\cdot\overline{e}'_4 \\ T(\overline{e}_3) = T(0,0,1) &= (0,1,1,0) = 0\cdot\overline{e}'_1 + 1\cdot\overline{e}'_2 + 1\cdot\overline{e}'_3 + 0\cdot\overline{e}'_4 \end{aligned}$$

Por lo tanto

$$M(T) = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 2 & 0 & 0 \end{pmatrix} \in M_{4\times 3}(\mathbb{R}).$$

Antes de continuar le damos estructura de espacio vectorial sobre $\mathbb{R}$ al conjunto de transformaciones lineales de $\mathbb{R}^n$ a $\mathbb{R}^m$ y que denotamos por $\mathscr{L}(\mathbb{R}^n, \mathbb{R}^m)$:
Sea $T, G \in \mathscr{L}(\mathbb{R}^n, \mathbb{R}^m)$ y $\alpha \in \mathbb{R}$. Definimos la suma $T + G$ y el producto por escalares $\alpha \cdot T$ como sigue
$(T + G)(v) = T(v) + G(v)$ y $(\alpha \cdot T)(v) = \alpha \cdot T(v)$ para toda $v \in \mathbb{R}^n$.
Veamos que esta suma y producto por escalares están bien definidas en $\mathscr{L}(\mathbb{R}^n, \mathbb{R}^m)$.

Proposición 15.2.26. *Si $T, G \in \mathscr{L}(\mathbb{R}^n, \mathbb{R}^m)$ y $\alpha \in \mathbb{R}$, entonces*

$$T + G \in \mathscr{L}(\mathbb{R}^n, \mathbb{R}^m) \ \ y \ \ \alpha \cdot T \in \mathscr{L}(\mathbb{R}^n, \mathbb{R}^m).$$

Demostración. Sean $v, v' \in \mathbb{R}^n$ y $\beta \in \mathbb{R}$.

$$\begin{aligned} (T + G)(v + v') &= T(v + v') + G(v + v') \\ &= T(v) + T(v') + G(v) + G(v') \\ &= (T(v) + G(v)) + (T(v') + G(v')) \\ &= (T + G)(v) + (T + G)(v'). \end{aligned}$$

y

$$\begin{aligned} (T + G)(\beta \cdot v) &= T(\beta \cdot v) + G(\beta \cdot v) \\ &= \beta \cdot T(v) + \beta \cdot G(v) \\ &= \beta \cdot (T(v) + G(v)) \\ &= \beta \cdot (T + G)(v). \end{aligned}$$

Luego $T + G$ es una transformación lineal.

$$\begin{aligned} (\alpha \cdot T)(v + v') &= \alpha \cdot T(v + v') \\ &= \alpha \cdot (T(v) + T(v')) \\ &= \alpha \cdot T(v) + \alpha \cdot T(v') \\ &= (\alpha \cdot T)(v) + (\alpha \cdot T)(v'). \end{aligned}$$

$$\begin{aligned} (\alpha \cdot T)(\beta \cdot v) &= \alpha \cdot T(\beta \cdot v) \\ &= \alpha \cdot (\beta \cdot T(v)) \\ &= (\alpha\beta) \cdot T(v) \\ &= (\beta\alpha) \cdot T(v) \\ &= \beta \cdot (\alpha \cdot T(v)). \end{aligned}$$

Por lo tanto $\alpha \cdot T$ es una transformación lineal. ∎

Por la manera en que se definió la suma y producto por escalares, la estructura de espacio vectorial de $\mathscr{L}(\mathbb{R}^n, \mathbb{R}^m)$ se "hereda" de la de $\mathbb{R}^m$. Por ejemplo para ver que para cualesquiera $T, G, H \in \mathscr{L}(\mathbb{R}^n, \mathbb{R}^m)$, $(T + G) + H = T + (G + H)$, debemos verificar que ambas funciones coinciden en cada elemento v de $\mathbb{R}^n$:

$$\begin{aligned}((T + G) + H)(v) &= (T + G)(v) + H(v)\\ &= (T(v) + G(v)) + H(v)\\ &= T(v) + (G(v) + H(v))\\ &= T(v) + (G + H)(v)\\ &= (T + (G + H))(v).\end{aligned}$$

De la misma manera se demuestra las otras propiedades por lo que tenemos entonces que

Proposición 15.2.27. *$(\mathscr{L}(\mathbb{R}^n, \mathbb{R}^m), +, \cdot_{\mathbb{R}})$ es un espacio vectorial sobre $\mathbb{R}$.*

Demostración. El neutro aditivo será la función $\widetilde{0} : \mathbb{R}^n \longrightarrow \mathbb{R}^m$, es decir la función idénticamente cero dada como $\widetilde{0}(v) = \overline{0}$ para todo $v \in \mathbb{R}^n$. Entonces para cualquier vector $v \in \mathbb{R}^n$, $(T + \widetilde{0})(v) = T(v) + \widetilde{0}(v) = T(v) + \overline{0} = T(v)$. Luego $T + \widetilde{0} = T$.
El inverso aditivo de T, que denotamos por $-T$ es la transformación lineal $-T : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ definida por $(-T)(v) = -T(v)$ para todo $v \in \mathbb{R}^n$.

$$(T + (-T))(v) = T(v) + (-T)(v) = T(v) - T(v) = \overline{0} = \widetilde{0}(v).$$

Luego $T + (-T) = \widetilde{0}$. ∎

Regresando a las transformaciones lineales L_A mencionadas en el ejemplo 15.2.6 y la matriz $M(T)$ asociada a una transformación lineal T introducida en la página 558, tenemos entonces definidas dos funciones

$$\mathscr{F} : \mathscr{L}(\mathbb{R}^n, \mathbb{R}^m) \longrightarrow M_{m\times n}(\mathbb{R}) \ \ y \ \ \mathscr{G} : M_{m\times n}(\mathbb{R}) \longrightarrow \mathscr{L}(\mathbb{R}^n, \mathbb{R}^m)$$

que resultan ser lineales y no sólo eso, cada una de ellas es inversa de la otra, con lo cual se tendrá que ambos espacios vectoriales son isomorfos. Esto nos dice entonces que las transformaciones lineales de $\mathbb{R}^n$ en $\mathbb{R}^m$ son exactamente las de la forma L_A para alguna $A \in M_{m\times n}(\mathbb{R})$.

Teorema 15.2.28. *Las funciones $\mathscr{F} : \mathscr{L}(\mathbb{R}^n, \mathbb{R}^m) \longrightarrow M_{m\times n}(\mathbb{R})$ dada por $\mathscr{F}(T) = M(T)$ y $\mathscr{G} : M_{m\times n}(\mathbb{R}) \longrightarrow \mathscr{L}(\mathbb{R}^n, \mathbb{R}^m)$ dada por $\mathscr{G}(A) = L_A$ son transformaciones lineales tales que $\mathscr{G} \circ \mathscr{F} = 1_{\mathscr{L}(\mathbb{R}^n, \mathbb{R}^m)}$ y $\mathscr{F} \circ \mathscr{G} = 1_{M_{m\times n}(\mathbb{R})}$. Esto es $\mathscr{F}$ es un isomorfismo y $\mathscr{F}^{-1} = \mathscr{G}$.*

Demostración.

(1) $\mathscr{F} : \mathscr{L}(\mathbb{R}^n, \mathbb{R}^m) \longrightarrow M_{m\times n}(\mathbb{R})$ es lineal.
Sean $T, G \in \mathscr{L}(\mathbb{R}^n, \mathbb{R}^m)$ y $\alpha \in \mathbb{R}$ y

$$\begin{array}{l} T(\overline{e}_1) = a_{11}\overline{e}'_1 + a_{21}\overline{e}'_2 + \cdots + a_{m1}\overline{e}'_m \\ T(\overline{e}_2) = a_{12}\overline{e}'_1 + a_{22}\overline{e}'_2 + \cdots + a_{m2}\overline{e}'_m \\ \vdots \quad\quad \vdots \quad\quad \vdots \quad\quad \vdots\vdots \quad\quad \vdots \\ T(\overline{e}_n) = a_{1n}\overline{e}'_1 + a_{2n}\overline{e}'_2 + \cdots + a_{mn}\overline{e}'_m \end{array} \quad \text{y} \quad \begin{array}{l} G(\overline{e}_1) = b_{11}\overline{e}'_1 + b_{21}\overline{e}'_2 + \cdots + b_{m1}\overline{e}'_m \\ G(\overline{e}_2) = b_{12}\overline{e}'_1 + b_{22}\overline{e}'_2 + \cdots + b_{m2}\overline{e}'_m \\ \vdots \quad\quad \vdots \quad\quad \vdots \quad\quad \vdots\vdots \quad\quad \vdots \\ G(\overline{e}_n) = b_{1n}\overline{e}'_1 + b_{2n}\overline{e}'_2 + \cdots + b_{mn}\overline{e}'_m \end{array}$$

Entonces

$$\begin{array}{l} (T+G)(\overline{e}_1) = T(\overline{e}_1)+G(\overline{e}_1) = (a_{11}+b_{11})\overline{e}'_1 + (a_{21}+b_{21})\overline{e}'_2 + \cdots + (a_{m1}+b_{m1})\overline{e}'_m \\ (T+G)(\overline{e}_2) = T(\overline{e}_2)+G(\overline{e}_2) = (a_{12}+b_{12})\overline{e}'_1 + (a_{22}+b_{22})\overline{e}'_2 + \cdots + (a_{m2}+b_{m2})\overline{e}'_m \\ \vdots \quad\quad\quad\quad \vdots \quad\quad\quad\quad \vdots \quad\quad\quad\quad \vdots \quad\quad \vdots\vdots \quad\quad \vdots \\ (T+G)(\overline{e}_n) = T(\overline{e}_n)+G(\overline{e}_n) = (a_{1n}+b_{1n})\overline{e}'_1 + (a_{2n}+b_{2n})\overline{e}'_2 + \cdots + (a_{mn}+b_{mn})\overline{e}'_m \end{array}$$

y

$$\begin{array}{l} (\alpha\cdot T)(\overline{e}_1) = \alpha\cdot T(\overline{e}_1) = \alpha\cdot a_{11}\overline{e}'_1 + \alpha\cdot a_{21}\overline{e}'_2 + \cdots + \alpha\cdot a_{m1}\overline{e}'_m \\ (\alpha\cdot T)(\overline{e}_2) = \alpha\cdot T(\overline{e}_2) = \alpha\cdot a_{12}\overline{e}'_1 + \alpha\cdot a_{22}\overline{e}'_2 + \cdots + \alpha\cdot a_{m2}\overline{e}'_m \\ \vdots \quad\quad\quad\quad \vdots \quad\quad\quad\quad \vdots \quad\quad\quad\quad \vdots \quad\quad \vdots\vdots \quad\quad \vdots \\ (\alpha\cdot T)(\overline{e}_n) = \alpha\cdot T(\overline{e}_n) = \alpha\cdot a_{1n}\overline{e}'_1 + \alpha\cdot a_{2n}\overline{e}'_2 + \cdots + \alpha\cdot a_{mn}\overline{e}'_m \end{array}$$

De aquí tenemos que

$$M(T) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots\vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}, \quad M(G) = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \vdots\vdots & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix}$$

$$M(T+G) = \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \cdots & a_{1n}+b_{1n} \\ a_{21}+b_{21} & a_{22}+b_{12} & \cdots & a_{2n}+b_{2n} \\ \vdots & \vdots & \vdots\vdots & \vdots \\ a_{m1}+b_{m1} & a_{m2}+b_{m2} & \cdots & a_{mn}+b_{mn} \end{pmatrix} \text{ y } M(\alpha\cdot T) = \begin{pmatrix} \alpha a_{11} & \alpha a_{12} & \cdots & \alpha a_{1n} \\ \alpha a_{21} & \alpha a_{22} & \cdots & \alpha a_{2n} \\ \vdots & \vdots & \vdots\vdots & \vdots \\ \alpha a_{m1} & \alpha a_{m2} & \cdots & \alpha a_{mn} \end{pmatrix}$$

Luego

$$\begin{aligned}
\mathscr{F}(T+G) &= M(T+G)\\
&= \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \cdots & a_{1n}+b_{1n} \\ a_{21}+b_{21} & a_{22}+b_{12} & \cdots & a_{2n}+b_{2n} \\ \vdots & \vdots & \vdots\!\vdots\!\vdots & \vdots \\ a_{m1}+b_{m1} & a_{m2}+b_{m2} & \cdots & a_{mn}+b_{mn} \end{pmatrix}\\
&= \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots\!\vdots\!\vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \vdots\!\vdots\!\vdots & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix}\\
&= M(T)+M(G)\\
&= \mathscr{F}(T)+\mathscr{F}(G).
\end{aligned}$$

$$\begin{aligned}
\mathscr{F}(\alpha\cdot T) &= M(\alpha\cdot T)\\
&= \begin{pmatrix} \alpha a_{11} & \alpha a_{12} & \cdots & \alpha a_{1n} \\ \alpha a_{21} & \alpha a_{22} & \cdots & \alpha a_{2n} \\ \vdots & \vdots & \vdots\!\vdots\!\vdots & \vdots \\ \alpha a_{m1} & \alpha a_{m2} & \cdots & \alpha a_{mn} \end{pmatrix}\\
&= \alpha\cdot \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots\!\vdots\!\vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}\\
&= \alpha\cdot M(T)\\
&= \alpha\cdot \mathscr{F}(T).
\end{aligned}$$

Por lo tanto $\mathscr{F}$ es lineal.

(2) $\mathscr{G}\circ\mathscr{F} = 1_{\mathscr{L}(\mathbb{R}^n,\mathbb{R}^m)}$:

Sea $T\in\mathscr{L}(\mathbb{R}^n,\mathbb{R}^m)$. Entonces $\mathscr{F}(T) = M(T) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots\!\vdots\!\vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$ donde

$$\begin{array}{rcccccccc}
T(\overline{e}_1) &=& a_{11}\overline{e}'_1 &+& a_{21}\overline{e}'_2 &+& \cdots &+& a_{m1}\overline{e}'_m \\
T(\overline{e}_2) &=& a_{12}\overline{e}'_1 &+& a_{22}\overline{e}'_2 &+& \cdots &+& a_{m2}\overline{e}'_m \\
\vdots && \vdots && \vdots && \vdots\!\vdots\!\vdots && \vdots \\
T(\overline{e}_n) &=& a_{1n}\overline{e}'_1 &+& a_{2n}\overline{e}'_2 &+& \cdots &+& a_{mn}\overline{e}'_m
\end{array}$$

Apliquemos $\mathscr{G}$ a la matriz $M(T) = \mathscr{F}(T)$ y veamos que $\mathscr{G}(\mathscr{F}(T)) = T$
$\mathscr{G}(\mathscr{F}(T)) = \mathscr{G}(M(T)) = L_{M(T)}$. Para mostrar que $L_{M(T)} = T$ basta ver que ambas funciones coinciden en la base $\{\overline{e}_1,\ldots,\overline{e}_n\}$ de R^n. Para cada $i = 1,\ldots,n$ tenemos

$$
\begin{aligned}
L_{M(T)}(\overline{e}_i) = L_{M(T)} \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} &= M(T) \cdot \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \\
&= \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots\vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \\
&= \begin{pmatrix} a_{11}\cdot 0 + a_{12}\cdot 0 + \cdots + a_{1i}\cdot 1 + \cdots + a_{1n}\cdot 0 \\ a_{21}\cdot 0 + a_{22}\cdot 0 + \cdots + a_{2i}\cdot 1 + \cdots + a_{2n}\cdot 0 \\ \vdots \quad\quad \vdots \quad\quad \vdots\vdots \quad\quad \vdots \quad\quad \vdots\vdots \quad\quad \vdots \\ a_{m1}\cdot 0 + a_{m2}\cdot 0 + \cdots + a_{mi}\cdot 1 + \cdots + a_{mn}\cdot 0 \end{pmatrix} \\
&= \begin{pmatrix} a_{1i} \\ a_{2i} \\ \vdots \\ a_{mi} \end{pmatrix} \\
&= a_{1i}\overline{e}'_1 + \cdots + a_{mi}\overline{e}'_m \\
&= T(\overline{e}_i).
\end{aligned}
$$

Luego $\mathscr{G}(\mathscr{F}(T)) = L_{M(T)} = T$ y por lo tanto $\mathscr{G} \circ \mathscr{F} = 1_{\mathscr{L}(\mathbb{R}^n, \mathbb{R}^m)}$.

(3) $\mathscr{F} \circ \mathscr{G} = 1_{M_{m\times n}(\mathbb{R})}$

Si $A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots\vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \in M_{m\times n}(\mathbb{R})$, entonces $\mathscr{G}(A) = L_A$. Encontremos $\mathscr{F}(L_A)$

$$
\begin{aligned}
L_A(\overline{e}_1) = L_A \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = A\cdot \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix} &= a_{11}\overline{e}'_1 + a_{21}\overline{e}'_2 + \cdots + a_{m1}\overline{e}'_m \\
L_A(\overline{e}_2) = L_A \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} = A\cdot \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{pmatrix} &= a_{12}\overline{e}'_1 + a_{22}\overline{e}'_2 + \cdots + a_{m2}\overline{e}'_m \\
\vdots \qquad\quad \vdots \qquad\quad \vdots \qquad\quad \vdots \qquad\quad \vdots \qquad\quad \vdots \qquad\quad \vdots\vdots \qquad\quad \vdots & \\
L_A(\overline{e}_n) = L_A \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} = A\cdot \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{pmatrix} &= a_{1n}\overline{e}'_1 + a_{2n}\overline{e}'_2 + \cdots + a_{mn}\overline{e}'_m
\end{aligned}
$$

Entonces $M(L_A) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots\vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} = A$, es decir,

$$(\mathscr{F} \circ \mathscr{G})(A) = \mathscr{F}(\mathscr{G}(A)) = \mathscr{F}(L_A) = A$$

y por lo tanto $\mathscr{F} \circ \mathscr{G} = 1_{M_{m\times n}(\mathbb{R})}$.

Por último $\mathscr{G}$ es lineal por el teorema 15.2.18. ∎

Corolario 15.2.29. $\dim_{\mathbb{R}} \mathscr{L}(\mathbb{R}^n, \mathbb{R}^m) = m \cdot n$.

Demostración. Como $\mathscr{L}(\mathbb{R}^n, \mathbb{R}^m) \cong M_{m\times n}(\mathbb{R})$ y $\dim_{\mathbb{R}} M_{m\times n}(\mathbb{R}) = m \cdot n$ (véase ejercicio 15.1.4), entonces $\dim_{\mathbb{R}} \mathscr{L}(\mathbb{R}^n, \mathbb{R}^m) = m \cdot n$ (corolario 15.2.15). ∎

Cada transformación lineal $T : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ tiene asociada una matriz $M(T) \in M_{m\times n}(\mathbb{R})$ y cada matriz $A \in M_{m\times n}(\mathbb{R})$ tiene asociada una transformación lineal $L_A : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ donde $M(L_A) = A$ y $L_{M(T)} = T$ con lo cual se tiene que cada matriz es la matriz asociada a una transformación lineal y cada transformación lineal es de la forma L_A para alguna matriz A. Tenemos aún más:

Teorema 15.2.30. (1) *Sean $T : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ y $G : \mathbb{R}^m \longrightarrow \mathbb{R}^k$ transformaciones lineales. Entonces $M(G \circ F) = M(G) \cdot M(F)$.*
(2) *Si $A \in M_{m\times n}(\mathbb{R})$ y $B \in M_{m\times k}(\mathbb{R})$, entonces $L_{B\cdot A} = L_B \circ L_A$.*

Demostración.

(1) Sean $\{\overline{e}_1, \ldots, \overline{e}_n\}, \{\overline{e}'_1, \ldots, \overline{e}'_m\}$ y $\{\overline{e}''_1, \ldots, \overline{e}''_k\}$ las bases canónicas de $\mathbb{R}^n, \mathbb{R}^m$ y $\mathbb{R}^k$ respectivamente y

$$\begin{array}{llll} T(\overline{e}_1) = a_{11}\overline{e}'_1 + \cdots + a_{m1}\overline{e}'_m & & G(\overline{e}'_1) = b_{11}\overline{e}''_1 + \cdots + b_{k1}\overline{e}''_m \\ T(\overline{e}_2) = a_{12}\overline{e}'_1 + \cdots + a_{m2}\overline{e}'_m & & G(\overline{e}'_2) = b_{12}\overline{e}''_1 + \cdots + b_{k2}\overline{e}''_m \\ \vdots \quad\quad \vdots \quad\quad \vdots\vdots \quad\quad \vdots & \text{y} & \vdots \quad\quad \vdots \quad\quad \vdots\vdots \quad\quad \vdots \\ T(\overline{e}_n) = a_{1n}\overline{e}'_1 + \cdots + a_{mn}\overline{e}'_m & & G(\overline{e}'_m) = b_{1m}\overline{e}''_1 + \cdots + b_{km}\overline{e}''_m \end{array}$$

Para cada $i = 1, \ldots, n$ se tiene que

$$\begin{aligned} (G \circ T)(\overline{e}_i) &= G(T(\overline{e}_i)) \\ &= G(a_{1i}\overline{e}'_1 + \cdots + a_{mi}\overline{e}'_m) \\ &= a_{1i}G(\overline{e}'_1) + \cdots + a_{mi}G(\overline{e}'_m) \\ &= a_{1i}(b_{11}\overline{e}''_1 + b_{21}\overline{e}''_2 + \cdots + b_{k1}\overline{e}''_m) + \cdots + a_{mi}(b_{1m}\overline{e}''_1 + b_{2m}\overline{e}''_2 + \cdots + b_{km}\overline{e}''_m) \\ &= (a_{1i}b_{11} + \cdots + a_{mi}b_{1m})\overline{e}''_1 + \cdots + (a_{1i}b_{k1} + \cdots + a_{mi}b_{km})\overline{e}''_k \\ &= \left(\sum_{j=1}^{m} b_{1j}a_{ji}\right)\overline{e}''_1 + \cdots + \left(\sum_{j=1}^{m} b_{kj}a_{ji}\right)\overline{e}''_k \end{aligned}$$

Entonces

$$
\begin{aligned}
(G\circ T)(\overline{e}_1) &= (a_{11}b_{11}+\cdots+a_{m1}b_{1m})\overline{e}_1'' + \cdots + (a_{11}b_{k1}+\cdots+a_{m1}b_{km})\overline{e}_k'' = \left(\sum_{j=1}^{m} b_{1j}a_{j1}\right)\overline{e}_1''+\cdots+\left(\sum_{j=1}^{m} b_{kj}a_{j1}\right)\overline{e}_k''\\
(G\circ T)(\overline{e}_2) &= (a_{12}b_{11}+\cdots+a_{m2}b_{1m})\overline{e}_1'' + \cdots + (a_{12}b_{k1}+\cdots+a_{m2}b_{km})\overline{e}_k'' = \left(\sum_{j=1}^{m} b_{1j}a_{j2}\right)\overline{e}_1''+\cdots+\left(\sum_{j=1}^{m} b_{kj}a_{j2}\right)\overline{e}_k''\\
&\ \ \vdots \qquad\qquad \vdots \qquad\qquad \vdots\vdots\vdots \qquad\qquad \vdots \qquad\qquad\qquad\qquad \vdots\\
(G\circ T)(\overline{e}_n) &= (a_{1n}b_{11}+\cdots+a_{mn}b_{1m})\overline{e}_1'' + \cdots + (a_{1n}b_{k1}+\cdots+a_{mn}b_{km})\overline{e}_k'' = \left(\sum_{j=1}^{m} b_{1j}a_{jn}\right)\overline{e}_1''+\cdots+\left(\sum_{j=1}^{m} b_{kj}a_{jn}\right)\overline{e}_k''
\end{aligned}
$$

Así pues $M(G \circ T)$ es la matriz

$$
M(G\circ T) = \begin{pmatrix}
\sum_{j=1}^{m} b_{1j}a_{j1} & \sum_{j=1}^{m} b_{1j}a_{j2} & \cdots & \sum_{j=1}^{m} b_{1j}a_{jn}\\
\sum_{j=1}^{m} b_{2j}a_{j1} & \sum_{j=1}^{m} b_{2j}a_{j2} & \cdots & \sum_{j=1}^{m} b_{2j}a_{jn}\\
\vdots & \vdots & \vdots\vdots\vdots & \vdots\\
\sum_{j=1}^{m} b_{kj}a_{j1} & \sum_{j=1}^{m} b_{kj}a_{j2} & \cdots & \sum_{j=1}^{m} b_{kj}a_{jn}
\end{pmatrix}
$$

Luego

$$
M(G\circ T) = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1m}\\ b_{21} & b_{22} & \cdots & b_{2m}\\ \vdots & \vdots & \vdots\vdots & \vdots\\ b_{k1} & b_{k2} & \cdots & b_{km}\end{pmatrix}\cdot\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n}\\ a_{21} & a_{22} & \cdots & a_{2n}\\ \vdots & \vdots & \vdots\vdots & \vdots\\ a_{m1} & a_{m2} & \cdots & a_{mn}\end{pmatrix} = M(G)\cdot M(T)
$$

(2) Para demostrar que $L_{B\cdot A} = L_B \circ L_A$ debemos ver que tienen el mismo dominio, mismo codominio y misma regla de correspondencia: como $B \cdot A \in M_{k\times n}(\mathbb{R})$, entonces $L_{B\cdot A} : \mathbb{R}^n \longrightarrow \mathbb{R}^k$ y como $L_A : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ y $L_B : \mathbb{R}^m \longrightarrow \mathbb{R}^k$, entonces $L_B \circ L_A : \mathbb{R}^n \longrightarrow \mathbb{R}^k$. Ahora veamos que tienen la misma regla de correspondencia y para esto sea $\begin{pmatrix} a_1\\ a_2\\ \vdots\\ a_n\end{pmatrix} \in \mathbb{R}^n$.

$$
\begin{aligned}
(L_B \circ L_A)\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} &= L_B\left(L_A\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}\right) \\
&= L_B\left(A \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}\right) \\
&= B \cdot \left(A \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}\right) \\
&= (B \cdot A) \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \\
&= L_{B\cdot A}\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}.
\end{aligned}
$$

Concluimos entonces que $L_{B\cdot A} = L_B \circ L_A$. ∎

En el ejercicio 15.2.1 se pide demostrar que $L_{I\times I} = 1_{\mathbb{R}^n}$ y $M_{(1_{\mathbb{R}^n})} = I_{n\times n}$. Usaremos este hecho para demostrar el siguiente:

Teorema 15.2.31. *Sea $A \in M_{n\times n}(\mathbb{R})$. Si A tiene inverso izquierdo o inverso derecho, entonces A es invertible.*

Demostración. Supongamos que A tiene inverso izquierdo y sea $B \in M_{n\times n}(\mathbb{R})$ tal que $B \cdot A = I_n$. Entonces $L_B \circ L_A = L_{BA} = L_{I_n} = 1_{\mathbb{R}^n}$. Luego L_A es inyectiva y por el corolario 15.2.20, L_A es isomorfismo, por lo que $L_B \circ L_A = 1_{\mathbb{R}^n} = L_A \circ L_B$. ∎

Corolario 15.2.32. *Si $A \in M_{m\times n}(\mathbb{R})$ no es invertible, entonces $A\cdot B$ no es invertible para toda $B \in M_{n\times n}(\mathbb{R})$.*

Demostración. Si $A \cdot B$ fuera invertible, entonces $(A \cdot B) \cdot C = I_{n\times n}$ para alguna $C \in M_{n\times n}(\mathbb{R})$. Luego A tendría inverso derecho y esto implicaría, por el teorema 15.2.31, que A es invertible, lo que no es cierto por hipótesis. Por lo tanto $A \cdot B$ no es invertible. ∎

En el caso $m = n$, tanto $M_{n\times n}(\mathbb{R})$ como $\mathscr{L}(\mathbb{R}^n, \mathbb{R}^n)$ son anillos donde en el primero el producto es el producto de matrices y su elemento identidad, es $I_{n\times n}$ y en el segundo el producto es la composición y su elemento identidad es la transformación

lineal identidad, además las transformaciones lineales que tienen inverso multiplicativo son precisamente las que son isomorfismo y por esta razón las llamaremos ***invertibles***

Por el teorema 15.2.30 los isomorfismos $\mathscr{F}$ y $\mathscr{G}$ satisfacen

$$\mathscr{F}(G \circ F) = \mathscr{F}(G) \cdot \mathscr{F}(T) \;\; y \;\; \mathscr{G}(A \cdot B) = \mathscr{G}(A) \circ \mathscr{G}(B),$$

es decir, $M(G \circ T) = M(G) \cdot M(T)$ y $L_{A \cdot B} = L_A \circ L_B$ esto para cualesquiera $T, G \in \mathscr{L}(\mathbb{R}^n, \mathbb{R}^n)$ y cualesquiera $A, B \in M_{n\times n}(\mathbb{R})$.

Hemos visto en el corolario 15.2.17 que $\mathbb{R}^n \cong \mathbb{R}^m$ si y sólo si $m = n$.

Teorema 15.2.33*. Sea $T : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ una transformación lineal. T es invertible (isomorfismo) si y sólo si $M(T)$ es invertible. Es más $M(T)^{-1} = M\left(T^{-1}\right)$.*

Demostración.

$\Longrightarrow$) Supongamos que T es invertible, es decir, $T : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ es isomorfismo. Entonces

$T \circ T^{-1} = 1_{\mathbb{R}^n} = T^{-1} \circ T$.

$M\left(T \circ T^{-1}\right) = M(1_{\mathbb{R}^n}) = M\left(T^{-1} \circ T\right)$

$M(T) \cdot M\left(T^{-1}\right) = I_{n\times n} = M\left(T^{-1}\right) \cdot M(T)$

Entonces $M(T)$ es invertible y $M(T)^{-1} = M\left(T^{-1}\right)$.

$\Longleftarrow$) Supongamos que $M(T) \in M_{n\times n}(\mathbb{R})$ es invertible. Entonces existe $M(T)^{-1} \in M_{n\times n}(\mathbb{R})$ tal que $M(T) \cdot M(T)^{-1} = I_{n\times n} = M(T)^{-1} \cdot M(T)$.

$L_{M(T)\cdot M(T)^{-1}} = L_{I_{n\times n}} = L_{M(T)^{-1}\cdot M(T)}$

$L_{M(T)} \circ L_{M(T)^{-1}} = 1_{\mathbb{R}^n} = L_{M(T)^{-1}} \circ L_{M(T)}$

$T \circ L_{M(T)^{-1}} = 1_{\mathbb{R}^n} = L_{M(T)^{-1}} \circ T$

Por lo tanto T es invertible y $T^{-1} = L_{M(T)^{-1}}$. ∎

§ 15.3. Rango de una matriz

Dado un sistema de m ecuaciones lineales en n indeterminadas, su conjunto de soluciones es un subespacio de $\mathbb{R}^n$ (véase la proposición 14.2.10) y como tal tiene una base (finita), así que este conjunto puede ser descrito mediante un número finito de soluciones, esto es, las soluciones del sistema son el conjunto de combinaciones lineales de una base.En el caso de un sistema de ecuaciones no-homogéneo de m ecuaciones lineales en n indeterminadas cada solución (si existe) se expresa como la suma de una solución particular fija y una solución del sistema homogéneo

asociado, teorema 14.3.8. Esto significa que aún cuando el conjunto de soluciones de un sistema no-homogéneo no es un subespacio, igualmente se le puede describir a través de de un número finito de vectores. Pero ¿cuál es la dimensión del subespacio de soluciones de un sistema homogéneo? Esta respuesta se dará a través de lo que definiremos como *rango de una matriz* está dada mediante las transformación lineal asociada a la matriz.

Definición 15.3.1. *Sea $A \in M_{m\times n}(\mathbb{R})$. El* **rango de *A*** *es la dimensión de $Im(L_A)$, donde $L_A : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ es la transformación lineal asociada a A.*

Ejemplo 15.3.2. Sea $A = \begin{pmatrix} 1 & 1 & 0 \\ 2 & 0 & 1 \\ 0 & 1 & -1 \\ 1 & -1 & 3 \end{pmatrix} \in M_{4\times 3}(\mathbb{R})$. Encontremos el rango de A. La transformación lineal asociada a A, $L_A : \mathbb{R}^3 \longrightarrow \mathbb{R}^4$ está dada por

$$L_A \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = A \cdot \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} a_1+a_2 \\ 2a_1+a_3 \\ a_1-a_2+3a_3 \end{pmatrix}.$$

Esto es $L_A(a_1, a_2, a_3) = (a_1 + a_2, 2a_1 + a_3, a_1 - a_2 + 3a_3)$. Para determinar la dimensión de $Im(L_A)$ debemos encontrar una base de $Im(L_A)$. Por la proposición 15.2.12

$$\{L_A((1,0,0)), L_A((0,1,0)), L_A((0,0,1))\}$$

genera a $Im(L_A)$ ya que $\{(1,0,0),(0,1,0),(0,0,1)\}$ es una base de $\mathbb{R}^3$. En este caso

$$L_A((1,0,0)) = (1,2,0,1), \quad L_A((0,1,0)) = (1,0,1,-1) \ y \ L_A((0,0,1)) = (0,1,-1,3).$$

Si este conjunto es linealmente independiente habremos obtenido una base de $Im(L_A)$. En caso contrario algún subconjunto de él será una base (véase el teorema 14.2.39).

Sea $\alpha(1,2,0,1) + \beta(1,0,1,-1) + \gamma(0,1,-1,3) = \overline{0} = (0,0,0,0)$. Entonces

$$\alpha + \beta = 0, \quad 2\alpha + \gamma = 0, \quad \beta - \gamma = 0 \ y \ \alpha - \beta + \gamma = 0$$

y no es difícil ver que la única posibilidad de que se cumplan estas igualdades es que $\alpha = \beta = \gamma = 0$. Luego $\{(1,2,0,1),(1,0,1,-1),(0,1,-1,3)\}$ es una base de $Im(L_A)$ y por lo tanto rango de $A = \dim_{\mathbb{R}} L_A = 3$.

Proposición 15.3.3. *Sea $A \in M_{m\times n}(\mathbb{R})$. Entonces el rango de A es igual a la dimensión del subespacio generado por las columnas de A.*

Demostración. Sea $A = (a_{ij})$. Por el teorema 15.2.28 $M(L_A) = A$, es decir,

$$\begin{array}{ccccccccccc}
L_A(\overline{e}_1) & = & a_{11}\overline{e}'_1 & + & a_{21}\overline{e}'_2 & + & \cdots & + & a_{m1}\overline{e}'_m & = & (a_{11}, a_{21}, \ldots, a_{m1}) \\
L_A(\overline{e}_2) & = & a_{12}\overline{e}'_1 & + & a_{22}\overline{e}'_2 & + & \cdots & + & a_{m2}\overline{e}'_m & = & (a_{12}, a_{22}, \ldots, a_{m2}) \\
\vdots & & \vdots & & \vdots & & \vdots\vdots & & \vdots & & \vdots \\
L_A(\overline{e}_n) & = & a_{1n}\overline{e}'_1 & + & a_{2n}\overline{e}'_2 & + & \cdots & + & a_{mn}\overline{e}'_m & = & (a_{1n}, a_{2n}, \ldots, a_{mn})
\end{array}$$

Por lo tanto

$$\dim_{\mathbb{R}} Im(L_A) = \dim_{\mathbb{R}} \langle\{(a_{11}, a_{21}, \ldots, a_{m1}), (a_{12}, a_{22}, \ldots, a_{m2}), \ldots, (a_{1n}, a_{2n}, \ldots, a_{mn})\}\rangle = rango\ A. \blacksquare$$

Teorema 15.3.4. *Sean $A \in M_{m\times n}(\mathbb{R})$ y $B \in M_{n\times k}(\mathbb{R})$. Si A es invertible, entonces rango $A \cdot B$ = rango B. Igualmente si B es invertible, entonces*

$$rango\ A \cdot B = rango\ A.$$

Demostración. Sea $\{v_1, \ldots, v_s\}$ base de $N(L_B)$ y $v_{s+1}, \ldots, v_k \in \mathbb{R}^k$ tales que $\{v_1, \ldots, v_s, v_{s+1}, \ldots, v_k\}$ es una base de $\mathbb{R}^k$. Como se vio en la demostración del teorema 15.2.19 $\{L_B(v_{s+1}), \ldots, L_B(v_k)\}$ es base de $Im(L_B)$ y por la, proposición 15.2.14, por ser L_A isomorfismo (ya que A es invertible), entonces

$$\{L_A L_B(v_{s+1}), \ldots, L_A L_B(v_k)\}$$

es base de $Im(L_A \circ L_B) = Im(L_{A\cdot B})$. Luego

$$\begin{aligned} rango\ A \cdot B &= \dim_{\mathbb{R}} \langle\{L_{A\cdot B}(v_{s+1}), \ldots, L_{A\cdot B}(v_k)\}\rangle \\ &= \dim_{\mathbb{R}} \langle\{L_B(v_{s+1}), \ldots, L_B(v_k)\}\rangle \\ &= rango\ B \blacksquare \end{aligned}$$

Corolario 15.3.5. *Si $A, B \in M_{m\times n}(\mathbb{R})$ y A es equivalente a B mediante operaciones elementales sobre renglones (columnas), entonces rango A = rango B.*

Demostración. Por el teorema 15.1.21, $B = E_r \cdot \ldots \cdot E_1 \cdot A$, donde las matrices E_i $(i = 1, \ldots, r)$ son elementales y por lo tanto, por el corolario 15.1.22 son invertibles. Al ser $E_r \cdot \ldots \cdot E_1$ invertible por el teorema 15.3.4 *rango* B = *rango* $(E_r \cdot \ldots \cdot E_1 \cdot A)$ = *rango* A. Similarmente para operaciones elementales sobre columnas, $B = A \cdot E_1 \cdot \ldots \cdot E_r$ y por el ejercicio 15.3.1, por ser $E_1 \cdot \ldots \cdot E_r$ invertible, *rango* A = *rango* B. ∎

Sea $A \in M_{m\times n}(\mathbb{R})$ y sea $\{\overline{e}_1, \ldots, \overline{e}_n\}$ la base canónica de $\mathbb{R}^n$. Entonces *rango* $A = \dim_{\mathbb{R}} Im(L_A) = \dim_{\mathbb{R}} \langle\{L_A(\overline{e}_1), \ldots, L_A(\overline{e}_n)\}\rangle$ y como $L_A(\overline{e}_j)$ es precisamente la columna j de A a la cual denotamos por A^j. Entonces *rango* $A = \dim_{\mathbb{R}} \left\langle A^1, \ldots, A^n \right\rangle$.

Teorema 15.3.6. *Sea $A \in M_{m\times n}(\mathbb{R})$ una matriz escalonada reducida. Entonces el rango de A es igual al número de renglones distintos de cero de A.*

Demostración. Supongamos que A tiene r renglones distintos de cero, los cuales por la forma que tiene A, deben ser los renglones 1 hasta r y esto significa que todos los renglones de A son 0 del lugar $r+1$ al m. Para $j = 1, \ldots, n$, sea A^j la j-ésima columna de A y para $k = 1, \ldots, r$ sea A^{i_k} la columna i_k correspondiente al primer elemento distinto de cero del renglón k. Entonces

$$A^{i_k} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \longleftarrow \text{renglón } k, \quad k = 1, \ldots, r$$

Es claro que $A^{i_1}, \ldots, A^{i_r}$ son linealmente independientes (forman parte de la base canónica de $\mathbb{R}^m$). Además como cada columna A^j de A es de la forma

$$A^j = \begin{pmatrix} b_1 \\ \vdots \\ b_r \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

entonces$A^j = b_1 A^{i_1} + \cdots + b_r A^{i_r}$. Luego $\{A^{i_1}, \ldots, A^{i_r}\}$ es una base del subespacio $\left\langle \{A^1, \ldots, A^n\} \right\rangle$. Por último

$$\begin{aligned} \textit{rango } A &= \dim_{\mathbb{R}} Im(L_A) = \dim_{\mathbb{R}} \langle \{L_A(\overline{e}_1), \ldots, L_A(\overline{e}_n)\} \rangle \\ &= \dim_{\mathbb{R}} \left\langle \{A^1, \ldots, A^n\} \right\rangle = r \\ &= \#\text{ renglones } \neq 0. \end{aligned}$$

∎

Basándonos en el corolario 15.3.5 y el teorema 15.3.6, una manera para encontrar el rango de una matriz A es llevándola a una matriz escalonada reducida y entonces contar en ésta última cuántos renglones tiene distintos de cero y ese será precisamente el rango de A, es decir, no tenemos que recurrir a encontrar una base de $Im(L_A)$.

Corolario 15.3.7. *Sea $A \in M_{m\times n}(\mathbb{R})$ una matriz escalonada reducida. Entonces el rango de A es igual a la dimensión del subespacio generado por los renglones.*

Demostración. Como la matriz A es escalonada reducida, por el teorema 15.3.6 *rango* A = # renglones distintos de cero. Sean $B_1, \ldots, B_r$ estos renglones y sean $C_{i_1}, \ldots, C_{i_r}$ las columnas donde están los primeros elementos distintos de cero de $B_1, \ldots, B_r$ respectivamente. Entonces para cada $j = 1, \ldots, r$ la coordenada i_j de B_j es 1 y la coordenada i_j de B_k es cero para $k = 1, \ldots, r$ y $k \neq j$. Por esta razón $B_1, \ldots, B_r$ son linealmente independientes ya que si $\alpha_1 B_1 + \cdots + \alpha_r B_r = \overline{0}$, entonces el vector de la izquierda tiene a $\alpha_1, \ldots, \alpha_r$ como las coordenadas $i_1, \ldots, i_r$ respectivamente y por lo tanto deben ser cero. Luego $\dim_{\mathbb{R}} \langle\{B_1, \ldots, B_r\}\rangle = r =$ *rango* A. ∎

Corolario 15.3.8. *Si A es una matriz escalonada, entonces rangoA =dimensión del subespacio generado por las columnas = dimensión del subespacio generado por los renglones.*

Definición 15.3.9. *Sea $A = (a_{ij}) \in M_{m\times n}(\mathbb{R})$. La* **transpuesta** *de A es la matriz $\boldsymbol{A^t} = (a'_{ji}) \in M_{n\times m}(\mathbb{R})$ donde $a'_{ji} = a_{ij}$ para $i = 1, \ldots, m$ y $j = 1, \ldots, n$.*

En otras palabras, la transpuesta de A es la matriz que resulta de A al intercambiar en A renglones por columnas, es decir, los renglones de A^t son las columnas de A en el mismo orden.

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots\vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}, \; A^t = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \vdots & \vdots & \vdots\vdots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{nm} \end{pmatrix}$$

Proposición 15.3.10. *Sean $A = (a_{ij}) \in M_{m\times n}(\mathbb{R})$ y $B = (b_{s\ell}) \in M_{n\times k}(\mathbb{R})$. Entonces*

(1) $(A^t)^t = A$ *y*
(2) $(A \cdot B)^t = B^t \cdot A^t$.

Demostración.

(1) $A^t = (a'_{ji})$ donde $a'_{ji} = a_{ij}$ y $(A^t)^t = (a''_{ij})$ donde $a''_{ij} = a'_{ji}$. Entonces $a''_{ij} = a'_{ji} = a_{ij}$ (Nota: Por definición $A, (A^t)^t \in M_{m\times n}(\mathbb{R})$).

(2) $A^t = (a'_{ji})$, $B^t = (b'_{\ell s})$, $A \cdot B = (c_{pq})$, $(A \cdot B)^t = (c'_{qp})$ donde $a'_{ji} = a_{ij}, b'_{\ell s} = b_{s\ell}$ y $c'_{qp} = c_{pq}$ para $i = 1, \ldots, m$; $j = 1, \ldots, n$; $\ell = 1, \ldots, k$ y $p = 1, \ldots, m$; $q = 1, \ldots, k$.
Es claro que $B^t \cdot A^t, (A \cdot B)^t \in M_{k\times m}(\mathbb{R})$. Veamos entonces que las entradas correspondientes en ambas matrices son iguales: $B^t \cdot A^t = (d_{qp})$ donde $d_{qp} = \sum_{r=1}^{n} b'_{qr} \cdot a'_{rp}$. Entonces

$$d_{qp} = \sum_{r=1}^{n} b'_{qr} \cdot a'_{rp} = \sum_{r=1}^{n} b_{rq} \cdot a_{pr} = \sum_{r=1}^{n} a_{pr} \cdot b_{rq} = c_{pq}.$$

Como la entrada qp de $B^t \cdot A^t$ es precisamente la entrada pq de $A \cdot B$, entonces $(A \cdot B)^t = B^t \cdot A^t$. ∎

Proposición 15.3.11. *Si E es una matriz elemental, entonces E^t es una matriz elemental del mismo tipo.*

Demostración. Lo demostraremos considerando los tres tipos de operaciones elementales. Sea E una matriz elemental.

1°/ Supongamos que E se obtiene de $I_{n\times n}$ al intercambiar el renglón k por el renglón ℓ. Entonces $E = (a_{ij})$ donde $a_{ij} = \begin{cases} 1 & \text{si } i = j,\ i \neq k, \ell \\ 1 & \text{si } i = k,\ j = \ell \text{ o } i = \ell,\ j = k \\ 0 & \text{en cualquier otro caso} \end{cases}$

$E^t = (a'_{ji})$ donde $a'_{ji} = a_{ij}$, así que $a'_{ji} = \begin{cases} 1 & \text{si } i = j,\ i \neq k, \ell \\ 1 & \text{si } i = \ell,\ j = k \text{ o } i = k,\ j = \ell \\ 0 & \text{en cualquier otro caso} \end{cases}$

Entonces $E^t = E$ y por lo tanto E^t es una matriz elemental.

2°/ Supongamos que E se obtiene de $I_{n\times n}$ al multiplicar por α el renglón k. Entonces

$E = (a_{ij})$ donde $a_{ij} = \begin{cases} 1 & \text{si } i = j,\ i \neq k \\ \alpha & \text{si } i = j = k \\ 0 & \text{en cualquier otro caso} \end{cases}$

$E^t = (a'_{ji})$ donde $a'_{ji} = a_{ij}$, así que $a'_{ji} = \begin{cases} 1 & \text{si } i = j,\ i \neq k \\ \alpha & \text{si } i = j = k \\ 0 & \text{en cualquier otro caso} \end{cases}$

y concluimos que $E^t = E$ y por lo tanto E^t es una matriz elemental.

3°/ Supongamos que E se obtiene de $I_{n\times n}$ de sumar al renglón k α veces el renglón ℓ,

$E = (a_{ij})$ donde $a_{ij} = \begin{cases} 1 & \text{si } i = j \\ \alpha & \text{si } i = k,\ j = \ell \\ 0 & \text{en cualquier otro caso} \end{cases}$

$E^t = (a'_{ji})$ donde $a'_{ji} = a_{ij}$, y entonces $a'_{ji} = \begin{cases} 1 & \text{si } i = j \\ \alpha & \text{si } i = \ell,\ j = k \\ 0 & \text{en cualquier otro caso} \end{cases}$

Luego E^t es la matriz elemental que resulta de $I_{n\times n}$ de sumar al renglón ℓ α veces el renglón k y por lo tanto es elemental. ∎

Habiendo introducido la transpuesta de una matriz tenemos entonces

Proposición 15.3.12. *Si A es una matriz escalonada reducida, entonces*

$$\textit{rango } A^t = \textit{rango } A.$$

Demostración. Se obtiene del corolario 15.3.8. ∎

Proposición 15.3.13. *Sea $A \in M_{m\times n}(\mathbb{R})$. Entonces rango A = rango A^t.*

Demostración. Sea A' una matriz escalonada reducida equivalente, mediante operaciones elementales sobre renglones, a A, esto es, $A' = E_k \cdot \ldots \cdot E_1 \cdot A$ donde $E_1, \ldots, E_k$ son elementales. Luego $A'^t = A^t \cdot E_1^t \cdot \ldots \cdot E_k^t$

$$\begin{array}{lcll} \textit{rango } A & = & \textit{rango } A' & \text{(corolario 15.3.5)} \\ \textit{rango } A' & = & \textit{rango } A'^t & \text{(proposición 15.3.12)} \\ \textit{rango } A'^t & = & \textit{rango } A^t & \text{(corolario 15.3.5)} \end{array}$$

Concluimos que *rango* A = *rango* A^t. ∎

Aunque el siguiente resultado es consecuencia inmediata de la proposición 15.3.13, la presentamos como teorema debido a su importancia.

Teorema 15.3.14. *Sea $A \in M_{m\times n}(\mathbb{R})$. Entonces rango A = dimensión del subespacio de $\mathbb{R}^m$ generado por las columnas de A = dimensión del subespacio de $\mathbb{R}^n$ generado por los renglones de A.*

Corolario 15.3.15. *Sea $A \in M_{m\times n}(\mathbb{R})$. Entonces rango $A \leq \min\{m, n\}$.*

Ejemplo 15.3.16. Sea $A = \begin{pmatrix} 2 & 3 & 1 & 0 \\ -1 & 2 & 1 & -1 \\ 3 & -6 & -3 & 3 \end{pmatrix}$

$$\begin{pmatrix} 2 & 3 & 1 & 0 \\ -1 & 2 & 1 & -1 \\ 3 & -6 & -3 & 3 \end{pmatrix} \xrightarrow[R_1 \longleftrightarrow R_2]{} \begin{pmatrix} -1 & 2 & 1 & -1 \\ 2 & 3 & 1 & 0 \\ 3 & -6 & -3 & 3 \end{pmatrix} \xrightarrow{(-1)R_1} \begin{pmatrix} 1 & -2 & -1 & 1 \\ 2 & 3 & 1 & 0 \\ 3 & -6 & -3 & 3 \end{pmatrix} \xrightarrow[R_3-3R_1]{R_2-2R_1}$$

$$\begin{pmatrix} 1 & -2 & -1 & 1 \\ 0 & 7 & 3 & -2 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow[(\frac{1}{7})\cdot R_2]{} \begin{pmatrix} 1 & -2 & -1 & 1 \\ 0 & 1 & \frac{3}{7} & -\frac{2}{7} \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{R_1+2R_2} \begin{pmatrix} 1 & 0 & -\frac{1}{7} & \frac{3}{7} \\ 0 & 1 & \frac{3}{7} & -\frac{2}{7} \\ 0 & 0 & 0 & 0 \end{pmatrix} = A'$$

Entonces *rango* A = *rango* A' = 2.

§ 15.4. Aplicación a sistemas de ecuaciones

En esta sección aplicaremos los resultados vistos hasta ahora para estudiar los sistemas de ecuaciones desde el punto de vista de espacios vectoriales.
Consideramos el sistema de m ecuaciones lineales en n indeterminadas con coeficientes en $\mathbb{R}$

$$(*) \quad \begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + \cdots + a_{2n}x_n = b_2 \\ \vdots \quad \vdots \quad \vdots \quad \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{cases}$$

La matriz de coeficientes de este sistema, como se definió en la página 486, es

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{pmatrix} \in M_{m\times n}(\mathbb{R})$$

Recordamos que los vectores en $\mathbb{R}^n$ podemos expresarlos en forma de columna, así que, si $X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ y $B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$, podemos presentar el sistema $(*)$ como una ecuación vectorial

$$(**) \quad A \cdot X = B$$

Interpretemos lo visto anteriormente.

Una solución del sistema $(**)$ es un vector $\overline{s} \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} = \in \mathbb{R}^n$ tal que $A \cdot \overline{s} = B$.

Pero esta igualdad es lo mismo que $L_A(\overline{s}) = B$ donde, recordamos,

$$L_A : \mathbb{R}^n \longrightarrow \mathbb{R}^m.$$

Entonces una solución de $(*)$ es un vector $\overline{s} \in \mathbb{R}^n$ cuya imagen bajo L_A es precisamente $B \in \mathbb{R}^m$. Empecemos estudiando los sistemas homogéneos, es decir, cuando $B = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \overline{0} \in \mathbb{R}^m$.

Teorema 15.4.1. *El conjunto de soluciones del sistema $A \cdot X = \overline{0}$ es $N(L_A)$, por lo que es un subespacio de $\mathbb{R}^n$ y su dimensión es n – rango A.*

Demostración. Evidentemente las soluciones del sistema son aquellos vectores $\overline{s} \in \mathbb{R}^n$ tal que $L_A(\overline{s}) = \overline{0}$ que son precisamente los elementos del núcleo de L_A que ya hemos visto que es un subespacio de $\mathbb{R}^n$. Además, por el teorema 15.2.19,

$$\dim_{\mathbb{R}} N(L_A) = n - \dim_{\mathbb{R}} Im(L_A) = n - \textit{rango } A.$$

■

Corolario 15.4.2. *Si $m < n$, entonces el sistema $A \cdot X = \overline{0}$ tiene al menos una solución no trivial.*

Demostración. Basta ver que $\dim_{\mathbb{R}} N(L_A) > 0$. Pero esto se debe a que, como $\dim_{\mathbb{R}} Im(L_A) \leq m$, entonces $\dim_{\mathbb{R}} N(L_A) = n - \dim_{\mathbb{R}} Im(L_A) \geq n - m > 0$. ■

Pasemos ahora a estudiar los sistemas no-homogéneos.

Teorema 15.4.3. *El sistema no homogéneo $A \cdot X = B$ tiene solución si y sólo si $B \in Im(L_A)$.*

Teorema 15.4.4. *Supongamos que el sistema no homogéneo $A \cdot X = B$ tiene solución $\overline{s} \in \mathbb{R}^n$. Entonces el conjunto de soluciones del sistema es el conjunto*

$$\overline{s} + N(L_A) = \{\overline{s} + \overline{s}_0 \mid \overline{s}_0 \in N(L_A)\}.$$

Demostración. Si $\overline{s}'$ es una solución del sistema, entonces

$$L_A(\overline{s}') = B = L_A(\overline{s})$$

y por lo tanto $\overline{0} = L_A(\overline{s}) - L_A(\overline{s}') = L_A(\overline{s} - \overline{s}')$. Luego $\overline{s} - \overline{s}' \in N(L_A)$ y así $\overline{s}' = \overline{s} + (\overline{s}' - \overline{s}) \in \overline{s} + N(L_A)$. Ahora si $\overline{s}_0 \in N(L_A)$, entonces

$$L_A(\overline{s} + \overline{s}_0) = L_A(\overline{s}) + L_A(\overline{s}_0) = L_A(\overline{s}) + \overline{0} = L_A(\overline{s}) = B.$$

■

Teorema 15.4.5. *El sistema $A \cdot X = B$ tiene al menos una solución si y sólo si rango A = rango A', donde A' es la matriz aumentada del sistema.*

Demostración. Supongamos que el sistema tiene una solución $\overline{s} \in \mathbb{R}^n$, esto es, $L_A(\overline{s}) = B$. Entonces $B \in Im(L_A)$. Pero $Im(L_A)$ es el subespacio generado por las columnas $A_1, \ldots, A_n$ de A, luego el subespacio generado por $A_1, \ldots, A_n, B$ es de la misma dimensión puesto que $B \in Im(L_A)$. Entonces *rango* A = *rango* A'. ■

§ 15.5. Determinante

Sea $\delta : M_{1\times1}(\mathbb{R}) \longrightarrow \mathbb{R}$ definida por $\delta(A) = a$ si $A = (a) \in M_{1\times1}(\mathbb{R})$. δ tiene las siguientes propiedades:

(1) $\delta(I_{1\times1}) = 1$.
(2) $\delta(A + B) = \delta(A) + \delta(B)$.
(2) $\delta(\alpha \cdot A) = \alpha \cdot \delta(A)$.
(4) $\delta(A \cdot B) = \delta(A) \cdot \delta(B)$.
(5) A es invertible si y sólo si $\delta(A) \neq 0$ y en este caso $\delta(A^{-1}) = \delta(A)^{-1}$.

Ahora definimos $\delta : M_{2\times2}(\mathbb{R}) \longrightarrow \mathbb{R}$ por $\delta(A) = a_{11}a_{22} - a_{12}a_{21}$, donde

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}.$$

Dada la matriz $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$, denotamos por A_1 y A_2 al primero y segundo renglón de A, es decir, $A_1 = (a_{11}\ a_{12})$ y $A_2 = (a_{21}\ a_{22})$. Entonces

$$\delta(A) = \delta\begin{pmatrix} A_1 \\ A_2 \end{pmatrix}$$

satisface

Teorema 15.5.1. (1) $\delta(I_{2\times2}) = 1$.
(2) $\delta\begin{pmatrix} \alpha\cdot A_1 + A_1' \\ A_2 \end{pmatrix} = \alpha \cdot \delta\begin{pmatrix} A_1 \\ A_2 \end{pmatrix} + \delta\begin{pmatrix} A_1' \\ A_2 \end{pmatrix}$ *y* $\delta\begin{pmatrix} A_1 \\ \alpha\cdot A_2 + A_2' \end{pmatrix} = \alpha \cdot \delta\begin{pmatrix} A_1 \\ A_2 \end{pmatrix} + \delta\begin{pmatrix} A_1 \\ A_2' \end{pmatrix}$
(3) $\delta\left(\begin{pmatrix} A_1 \\ A_2 \end{pmatrix}\right) = 0$ *si* $A_1 = A_2$.

Demostración.

(1) $\delta(I_{1\times 1}) = \delta\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1 \cdot 1 + 0 \cdot 0 = 1.$

(2) Si $A_1 = (a_{11}\ a_{12}), A_2 = (a_{21}\ a_{22}), A_1' = (a_{11}'\ a_{12}')$ y $\alpha \in \mathbb{R}$, entonces

$$\begin{aligned}
\delta\begin{pmatrix} \alpha\cdot A_1 + A_1' \\ A_2 \end{pmatrix} &= \delta\begin{pmatrix} \alpha\cdot a_{11} + a_{11}' & \alpha\cdot a_{12} + a_{12}' \\ a_{21} & a_{22} \end{pmatrix} \\
&= (\alpha \cdot a_{11} + a_{11}')a_{22} - (\alpha \cdot a_{12} + a_{12}')a_{21} \\
&= \alpha \cdot (a_{11}a_{22} - a_{12}a_{21}) + (a_{11}'a_{22} - a_{12}'a_{21}) \\
&= \alpha \cdot \delta\begin{pmatrix} A_1 \\ A_2 \end{pmatrix} + \delta\begin{pmatrix} A_1' \\ A_2 \end{pmatrix}
\end{aligned}$$

Análogamente se demuestra la otra igualdad.

(3) Si $A_1 = A_2 = (a_{11}\ a_{12})$, entonces

$$\delta\begin{pmatrix} A_1 \\ A_2 \end{pmatrix} = \delta\begin{pmatrix} a_{11} & a_{12} \\ a_{11} & a_{12} \end{pmatrix} = a_{11}a_{12} - a_{11}a_{12} = 0.$$

■

Nota 15.5.2. A una función de $M_{2\times 2}(\mathbb{R}) \longrightarrow \mathbb{R}$ que satisface (2) del teorema 15.5.1 se le llama ***bilineal*** o **2-*lineal***.

Corolario 15.5.3. *Sea $d : M_{2\times 2}(\mathbb{R}) \longrightarrow \mathbb{R}$ cualquier función que satisface el teorema.15.5.1. Entonces $d\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = -1$.*

Demostración. Sea $d\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = 0$ ya que tiene sus dos renglones iguales. Entonces, puesto que d es bilineal,

$$\begin{aligned}
0 &= d\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \\
&= d\begin{pmatrix} 1+0 & 0+1 \\ 1 & 1 \end{pmatrix} \\
&= d\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} + d\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \\
&= d\begin{pmatrix} 1 & 0 \\ 1+0 & 0+1 \end{pmatrix} + d\begin{pmatrix} 0 & 1 \\ 1+0 & 0+1 \end{pmatrix} \\
&= d\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} + d\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + d\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + d\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \\
&= 0 + 1 + d\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + 0 \\
&= 1 + d\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}
\end{aligned}$$

Por lo tanto $d\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = -1$. ■

Aunque el teorema siguiente podemos demostrarlo de la definición que hemos dado de $\delta : M_{2\times 2}(\mathbb{R}) \to \mathbb{R}$, no lo haremos aquí, debido a que probaremos en general que para cualquier $n \geq 1$ y cualquier función $\delta : M_{n\times n}(\mathbb{R}) \longrightarrow \mathbb{R}$ que satisfaga propiedades similares a las dadas en el teorema 15.5.1 y que para el caso $n = 2$ coinciden con dicho teorema, es verdadero el resultado. Este es

Teorema 15.5.4. *Si* $\delta : M_{2\times 2}(\mathbb{R}) \to \mathbb{R}$, *definida por*

$$\delta \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = a_{11} \cdot a_{22} - a_{12} \cdot a_{21}.$$

(1) $\delta(A \cdot B) = \delta(A) \cdot \delta(B)$.
(2) *A es invertible si y sólo si* $\delta(A) \neq 0$ *y en este caso* $\delta(A^{-1}) = \delta(A)^{-1}$.

Demostraremos ahora que en realidad δ es la única función de $M_{n\times n}$ en $\mathbb{R}$ que satisface las propiedades del teorema 15.5.1

Teorema 15.5.5. *Si* $d : M_{2\times 2} \longrightarrow \mathbb{R}$ *satisface las siguientes propiedades*

(1) $d(I_{2\times 2}) = 1$,
(2) *d es bilineal*,
(3) $d \begin{pmatrix} A_1 \\ A_2 \end{pmatrix} = 0$ *si* $A_1 = A_2$,

entonces $d = \delta$.

Demostración. Sea $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in M_{2\times 2}(\mathbb{R})$. Usando las propiedades de d tenemos

$$\begin{aligned}
d \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} &= d \begin{pmatrix} 0+a_{11} & a_{12}+0 \\ a_{21} & a_{22} \end{pmatrix} \\
&= d \begin{pmatrix} 0 & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + d \begin{pmatrix} a_{11} & 0 \\ a_{21} & a_{22} \end{pmatrix} && \text{por (2)} \\
&= d \begin{pmatrix} 0 & a_{12} \\ 0+a_{21} & a_{22}+0 \end{pmatrix} + d \begin{pmatrix} a_{11} & 0 \\ 0+a_{21} & a_{22}+0 \end{pmatrix} \\
&= d \begin{pmatrix} 0 & a_{12} \\ 0 & a_{22} \end{pmatrix} + d \begin{pmatrix} 0 & a_{12} \\ a_{21} & 0 \end{pmatrix} + d \begin{pmatrix} a_{11} & 0 \\ 0 & a_{22} \end{pmatrix} + d \begin{pmatrix} a_{11} & 0 \\ a_{21} & 0 \end{pmatrix} && \text{por (2)} \\
&= d \begin{pmatrix} a_{12}\cdot 0 & a_{12}\cdot 1 \\ a_{22}\cdot 0 & a_{22}\cdot 1 \end{pmatrix} + d \begin{pmatrix} a_{12}\cdot 0 & a_{12}\cdot 1 \\ a_{21}\cdot 1 & a_{21}\cdot 0 \end{pmatrix} + d \begin{pmatrix} a_{11}\cdot 1 & a_{11}\cdot 0 \\ a_{22}\cdot 0 & a_{22}\cdot 1 \end{pmatrix} + d \begin{pmatrix} a_{11}\cdot 1 & a_{11}\cdot 0 \\ a_{21}\cdot 1 & a_{21}\cdot 0 \end{pmatrix} \\
&= a_{12}a_{22} d \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} + a_{12}a_{21} d \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + a_{11}a_{22} d \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + a_{11}a_{21} d \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} && \text{por (2)} \\
&= 0 + a_{12}a_{21} d \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + a_{11}a_{22} d \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + 0 && \text{por (3)} \\
&= a_{12}a_{21} \cdot (-1) + a_{11}a_{22} \cdot 1 && \text{por (1) y corolario 15.5.3} \\
&= a_{11}a_{22} - a_{12}a_{21} = \delta \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}
\end{aligned}$$

Luego $d = \delta$. ∎

Nuestra intención ahora es generalizar lo que hemos hecho para $n = 1$ y $n = 2$. Definimos el concepto de determinante y de aquí desarrollaremos la teoría. Además demostraremos que, en caso de existir, éste es único. Para terminar, demostraremos la existencia del determinante para cada $n \geq 1$.

Empezamos definiendo *función n-lineal*. De la misma manera que hicimos para $n = 2$, si $A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots\vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$, denotaremos $A_i = \begin{pmatrix} a_{i1} & a_{i2} & \cdots & a_{in} \end{pmatrix}$ el i-ésimo renglón de A, así que $A = \begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_m \end{pmatrix}$

Definición 15.5.6. *Una función* $\delta : M_{n\times n}(\mathbb{R}) \longrightarrow \mathbb{R}$ *es* ***n*-lineal** *si para cada* $i = 1, \ldots, n$ *y* $\alpha \in \mathbb{R}$

$$\delta\begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ \alpha\cdot A_i + A_i' \\ \vdots \\ A_n \end{pmatrix} = \alpha \cdot \delta\begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_i \\ \vdots \\ A_n \end{pmatrix} + \delta\begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_i' \\ \vdots \\ A_n \end{pmatrix}.$$

Ejemplo 15.5.7. Sea $\delta : M_{n\times n}(\mathbb{R}) \longrightarrow \mathbb{R}$ definida como

$$\delta(A) = a_{11}a_{22} \cdot \ldots \cdot a_{nn},$$

donde $A_i = \begin{pmatrix} a_{i1} & a_{i2} & \cdots & a_{in} \end{pmatrix}$. Para cada $i = 1, \ldots, n$, si $A_i' = \begin{pmatrix} a_{i1}' & a_{i2}' & \cdots & a_{in}' \end{pmatrix}$, entonces

$$\begin{aligned} \delta\begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ \alpha\cdot A_i + A_i' \\ \vdots \\ A_n \end{pmatrix} &= a_{11}a_{22} \cdot \ldots (\alpha \cdot a_{ii} + a_{ii}') \cdot \ldots \cdot a_{nn} \\ &= \alpha \cdot a_{11}a_{22} \cdot \ldots \cdot a_{ii} \cdot \ldots \cdot a_{nn} + a_{11}a_{22} \cdot \ldots \cdot a_{ii}' \cdot \ldots \cdot a_{nn} \\ &= \alpha \cdot \delta\begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_i \\ \vdots \\ A_n \end{pmatrix} + \delta\begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_i' \\ \vdots \\ A_n \end{pmatrix} \end{aligned}$$

Luego δ es n-lineal.

Ejemplo 15.5.8. Para cada $j = 1, \ldots, n$, sea $\delta_j : M_{n\times n}(\mathbb{R}) \longrightarrow \mathbb{R}$ definida por $\delta_j(A) = a_{1j}a_{2j} \cdot \ldots \cdot a_{nj}$. δ_j es n-lineal. Sea $A_i\,' = (a_{i1}', a_{i2}', \ldots, a_{in}')$. Entonces

$$\alpha A_i + A_i\,' = (\alpha a_{i1} + a_{i1}' \cdots \alpha a_{ij} + a_{ij}' \cdots \alpha a_{in} + a_{in}')$$

y

$$\delta_j\begin{pmatrix} A_1 \\ \vdots \\ \alpha\cdot A_i+A_i' \\ \vdots \\ A_n \end{pmatrix} = a_{ij}a_{2j}\cdot\ldots\cdot(\alpha a_{ij}+a_{ij}')\cdot\ldots\cdot a_{nj}$$

$$= \alpha a_{ij}a_{2j}\cdot\ldots\cdot a_{ij}\cdot\ldots\cdot a_{nj} + a_{ij}a_{2j}\cdot\ldots\cdot a_{(i-1)j}\cdot a_{ij}'\cdot a_{(i+1)j}\ldots\cdot a_{nj}$$

$$= \alpha\delta_j\begin{pmatrix} A_1 \\ \vdots \\ A_i \\ \vdots \\ A_n \end{pmatrix} + \delta_j\begin{pmatrix} A_1 \\ \vdots \\ A_i' \\ \vdots \\ A_n \end{pmatrix}.$$

Proposición 15.5.9. *Si $\delta_1,\ldots,\delta_m : M_{n\times n}(\mathbb{R}) \longrightarrow \mathbb{R}$ son n-lineales, entonces para cualesquiera $\alpha_1,\ldots,\alpha_m \in \mathbb{R}$, $\alpha_1\delta_1,\ldots,\alpha_m\delta_m$ es n-lineal. Esto es, toda combinación lineal de funciones n-lineales es n-lineal.*

Demostración. Para cada $i = 1,\ldots,n$ se tiene

$$(\alpha_1\cdot\delta_1+\cdots+\alpha_m\cdot\delta_m)\begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ \alpha\cdot A_i+A_i' \\ \vdots \\ A_n \end{pmatrix} =$$

$$\alpha_1\cdot\delta_1\begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ \alpha\cdot A_i+A_i' \\ \vdots \\ A_n \end{pmatrix} + \cdots + \alpha_m\cdot\delta_m\begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ \alpha\cdot A_i+A_i' \\ \vdots \\ A_n \end{pmatrix} =$$

$$\alpha_1\cdot\left(\alpha\delta_1\begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_i \\ \vdots \\ A_n \end{pmatrix} + \delta_1\begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_i' \\ \vdots \\ A_n \end{pmatrix}\right) + \cdots + \alpha_m\cdot\left(\alpha\delta_m\begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_i \\ \vdots \\ A_n \end{pmatrix} + \delta_m\begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_i' \\ \vdots \\ A_n \end{pmatrix}\right) =$$

$$\alpha\cdot(\alpha_1\cdot\delta_1+\cdots+\alpha_m\cdot\delta_m)\begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_i \\ \vdots \\ A_n \end{pmatrix} + (\alpha_1\cdot\delta_1+\cdots+\alpha_m\cdot\delta_m)\begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_i' \\ \vdots \\ A_n \end{pmatrix}$$

Por lo tanto $\alpha_1 \cdot \delta_1 + \cdots + \alpha_m \cdot \delta_m$ es n-lineal. ∎

Para definir un determinante necesitamos introducir el concepto de función alternante.

Definición 15.5.10. *Una función $\delta : M_{n\times n}(K) \longrightarrow K$ es* **alternante** *si para toda matriz A que tiene dos renglones consecutivos iguales, $\delta(A) = 0$.*

Definición 15.5.11. *Una función $\delta : M_{n\times n}(K) \longrightarrow K$ es un determinante si*

(1) *δ es n-lineal.*
(2) *δ es alternante.*
(3) $\delta(I_{n\times n}) = 1$.

Ejemplo 15.5.12. En el teorema 15.5.1 demostramos precisamente que

$$\delta : M_{2\times 2}(\mathbb{R}) \longrightarrow \mathbb{R}$$

definida por $\delta \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = a_{11}a_{22} - a_{12}a_{21}$ es un determinante.

Las funciones n-lineales dadas en los ejemplos 15.5.7 y 15.5.8 no son determinantes ya que de acuerdo con su regla de correspondencia, en el primero la función no es alternante y en el segundo $\delta_j(I_{n\times n}) = 0$ (en realidad tampoco es alternante). Verifique ambas afirmaciones.
Veamos las propiedades inmediatas que se obtienen de la definición de determinante.

Teorema 15.5.13. *Sea $\delta : M_{n\times n}(\mathbb{R}) \longrightarrow \mathbb{R}$ un determinante y $A, B \in M_{n\times n}(\mathbb{R})$. Entonces*

(1) *Si B se obtiene de A al intercambiar dos renglones, entonces $\delta(B) = -\delta(A)$.*
(2) *Si A tiene dos renglones iguales, entonces $\delta(A) = 0$.*
(3) *Si un renglón de A consta únicamente de ceros, entonces $\delta(A) = 0$.*
(4) *Si B se obtiene de A al sumar un renglón α veces otro renglón, entonces $\delta(B) = \delta(A)$.*

Demostración.

(1) (i) Demostraremos primero el caso en que los renglones intercambiados son consecutivos.

Sea $A = \begin{pmatrix} A_1 \\ \vdots \\ A_i \\ A_{i+1} \\ \vdots \\ A_n \end{pmatrix}$. Entonces $B = \begin{pmatrix} A_1 \\ \vdots \\ A_{i+1} \\ A_i \\ \vdots \\ A_n \end{pmatrix}$. Luego, como δ es un determinante,

$$
\begin{aligned}
0 &= \delta \begin{pmatrix} A_1 \\ \vdots \\ A_i + A_{i+1} \\ A_i + A_{i+1} \\ \vdots \\ A_n \end{pmatrix} \\
&= \delta \begin{pmatrix} A_1 \\ \vdots \\ A_i \\ A_i \\ \vdots \\ A_n \end{pmatrix} + \delta \begin{pmatrix} A_1 \\ \vdots \\ A_i \\ A_{i+1} \\ \vdots \\ A_n \end{pmatrix} + \delta \begin{pmatrix} A_1 \\ \vdots \\ A_{i+1} \\ A_i \\ \vdots \\ A_n \end{pmatrix} + \delta \begin{pmatrix} A_1 \\ \vdots \\ A_{i+1} \\ A_{i+1} \\ \vdots \\ A_n \end{pmatrix} \\
&= \delta \begin{pmatrix} A_1 \\ \vdots \\ A_i \\ A_{i+1} \\ \vdots \\ A_n \end{pmatrix} + \delta \begin{pmatrix} A_1 \\ \vdots \\ A_{i+1} \\ A_i \\ \vdots \\ A_n \end{pmatrix} = \delta(A) + \delta(B)
\end{aligned}
$$

y por lo tanto $\delta(B) = -\delta(A)$.

(*ii*) Ahora, supongamos que intercambiamos en A el renglón i con el renglón j, donde $i < j$. Entonces $B = \begin{pmatrix} A_1 \\ \vdots \\ A_j \\ \vdots \\ A_i \\ \vdots \\ A_n \end{pmatrix}$ $\begin{matrix} \\ \\ -\text{renglón } i \\ \\ -\text{renglón } j \\ \\ \\ \end{matrix}$. Utilizando el caso (*i*), primero bajamos el renglón i renglón por renglón hasta llegar al renglón j, con lo cual la matriz obtenida será $C = \begin{pmatrix} A_1 \\ \vdots \\ A_{i+1} \\ \vdots \\ A_j \\ A_i \\ \vdots \\ A_n \end{pmatrix}$ $\begin{matrix} \\ -\text{renglón } i \\ \\ \\ -\text{renglón } (j-1) \\ -\text{renglón } j \\ \\ \end{matrix}$. Esto es,

$$\delta\begin{pmatrix} A_1 \\ \vdots \\ A_i \\ \vdots \\ A_j \\ \vdots \\ A_n \end{pmatrix} = (-1)\delta\begin{pmatrix} A_1 \\ \vdots \\ A_{i+1} \\ A_i \\ \vdots \\ A_j \\ \vdots \\ A_n \end{pmatrix} \begin{matrix} \\ \\ \\ -\text{renglón } i \\ -\text{renglón } (i{+}1) \\ \\ \\ \\ \end{matrix}$$

$$= (-1)^2\delta\begin{pmatrix} A_1 \\ \vdots \\ A_{i+1} \\ A_{i+2} \\ A_i \\ \vdots \\ A_j \\ \vdots \\ A_n \end{pmatrix} \begin{matrix} \\ \\ -\text{renglón } i \\ -\text{renglón } (i+1) \\ -\text{renglón } (i+2) \\ \\ -\text{renglón } j \\ \\ \end{matrix}$$

$$\vdots$$

$$= (-1)^{j-i}\delta\begin{pmatrix} A_1 \\ \vdots \\ A_{i+1} \\ \vdots \\ A_j \\ A_i \\ \vdots \\ A_n \end{pmatrix} \begin{matrix} \\ \\ -\text{renglón } i \\ \\ -\text{renglón } (j-1) \\ -\text{renglón } j \\ \\ \\ \end{matrix}$$

$$= (-1)^{j-i}\delta(C)$$

Ahora de manera similar, subiendo el renglón $(j-1)$ de C al renglón i, obtenemos B

$$\delta(C) = (-1)\delta\begin{pmatrix} A_1 \\ \vdots \\ A_{i+1} \\ \vdots \\ A_j \\ A_{j-1} \\ A_i \\ \vdots \\ A_n \end{pmatrix} \begin{matrix} \\ -\text{renglón } i \\ \\ -\text{renglón } (j{-}2) \\ -\text{renglón } (j{-}1) \\ -\text{renglón } j \\ \\ \\ \end{matrix} = \cdots = (-1)^{j-i-1}\delta\begin{pmatrix} A_1 \\ \vdots \\ A_j \\ \vdots \\ A_i \\ \vdots \\ A_n \end{pmatrix} = (-1)^{j-i-1}\delta(B)$$

Entonces $\delta(A) = (-1)^{j-i}\delta(C) = (-1)^{2(j-i)-1}\delta(B) = -\delta(B)$.
Por lo tanto $\delta(B) = -\delta(A)$.

(2) Supongamos que $A_i = A_j$ en A. Por (1) si intercambiamos el renglón i y el renglón j, la matriz B resultante satisface $\delta(B) = -\delta(A)$ y como $A_i = A_j$, entonces $B = A$ y así tenemos $\delta(A) = -\delta(A)$, lo que implica $\delta(A) = 0$.

(3) Suponemos que el renglón i, $A_i = \overline{0}$. Entonces por ser δ n-lineal, tenemos que

$$\delta\begin{pmatrix} A_1 \\ \vdots \\ 0 \\ \vdots \\ A_n \end{pmatrix} = \delta\begin{pmatrix} A_1 \\ \vdots \\ 0 \\ \vdots \\ A_n \end{pmatrix} = 0 \cdot \delta\begin{pmatrix} A_1 \\ \vdots \\ 0 \\ \vdots \\ A_n \end{pmatrix} = 0$$

(4) Supongamos que B se obtiene de A al sumar al renglón i α veces el renglón j. Entonces

$$\delta(B) = \delta\begin{pmatrix} A_1 \\ \vdots \\ A_i+\alpha A_j \\ \vdots \\ A_j \\ \vdots \\ A_n \end{pmatrix} = \delta\begin{pmatrix} A_1 \\ \vdots \\ A_i \\ \vdots \\ A_j \\ \vdots \\ A_n \end{pmatrix} + \alpha \cdot \delta\begin{pmatrix} A_1 \\ \vdots \\ A_j \\ \vdots \\ A_j \\ \vdots \\ A_n \end{pmatrix} = \delta\begin{pmatrix} A_1 \\ \vdots \\ A_i \\ \vdots \\ A_j \\ \vdots \\ A_n \end{pmatrix} = \delta(A).$$

∎

Para cualquier determinante δ definido en $M_{n\times n}(\mathbb{R})$, nuestra idea ahora será probar que $\delta(A \cdot B) = \delta(A) \cdot \delta(B)$ para matrices arbitrarias $A, B \in M_{n\times n}(\mathbb{R})$. Lo haremos paso a paso y para esto veremos los posibles valores que pueden tener $\delta(E)$ cuando E es una matriz elemental.

Corolario 15.5.14. *Sea $\delta : M_{n\times n}(\mathbb{R}) \longrightarrow \mathbb{R}$ un determinante y $A \in M_{n\times n}(\mathbb{R})$ de rango $k < n$. Entonces $\delta(A) = 0$.*

Demostración. Como $k = rang\ A = \dim_{\mathbb{R}} \langle\{A_1, \ldots, A_n\}\rangle < n$, donde $A_1, \ldots, A_n$ son los renglones de A, entonces $A_1, \ldots, A_n$ son linealmente dependientes, luego

$$\alpha_1 A_1 + \cdots + \alpha_n A_n = \overline{0}$$

donde algún $\alpha_i \neq 0$. Multiplicando por α_i^{-1} obtenemos

$$(\alpha_i^{-1}\alpha_1)A_1 + \cdots + A_i + \cdots + (\alpha_i^{-1}\alpha_n)A_n = \overline{0},$$

así que si sumamos al renglón i de A, $(\alpha_i^{-1}\alpha_j)A_j$ para cada $j = 1, \ldots, n$, $j \neq i$, por (3) y (4) del teorema 15.5.13, para la matriz B resultante cuyo renglón i consta de ceros, se tendrá $0 = \delta(B) = \delta(A)$. ∎

Corolario 15.5.15. *Sea $\delta : M_{n\times n}(\mathbb{R}) \longrightarrow \mathbb{R}$ un determinante y $E \in M_{n\times n}(\mathbb{R})$ una matriz elemental. Entonces*

$$\delta(E) = \begin{cases} -1 & \text{si } E \text{ es de tipo (I)} \\ \alpha & \text{si } E \text{ es de tipo (II)} \\ 1 & \text{si } E \text{ es de tipo (III)} \end{cases}$$

(véase la página 544)

Demostración.

(1) Supongamos que E resulta de $I_{n\times n}$ al intercambiar dos renglones (tipo (I)). Entonces, por el teorema 15.5.13 (1), $\delta(E) = -\delta(I_{n\times n}) = -1$.
(2) Supongamos que E resulta de $I_{n\times n}$ al multiplicar el renglón i por $\alpha \neq 0$ (tipo (II)). Entonces por ser δ n-lineal, $\delta(E) = \alpha\delta(I_{n\times n}) = \alpha$.
(3) Si E resulta de $I_{n\times n}$ al sumar al renglón i α veces el renglón j (tipo (III)), entonces por el teorema 15.5.13 (4), $\delta(E) = \delta(I_{n\times n}) = 1$. ∎

Corolario 15.5.16. *Si δ y δ' son determinantes en $M_{n\times n}(\mathbb{R})$, entonces $\delta(E) = \delta'(E)$ para toda matriz elemental E.*

Corolario 15.5.17. *Sea $\delta : M_{n\times n}(\mathbb{R}) \longrightarrow \mathbb{R}$ un determinante y $E \in M_{n\times n}(\mathbb{R})$ una matriz elemental. Entonces $\delta(E) = \delta(E^t)$.*

Demostración. Es inmediato del corolario 15.5.15 puesto que E^t es una matriz elemental del mismo tipo que E (véase la proposición 15.3.11). ∎

Teorema 15.5.18. *Sea $\delta : M_{n\times n}(\mathbb{R}) \longrightarrow \mathbb{R}$ un determinante y $A \in M_{n\times n}(\mathbb{R})$. Entonces para cualquier matriz elemental E se tiene que $\delta(E \cdot A) = \delta(E)\delta(A)$.*

Demostración.

(*i*) Si E es del tipo (I), entonces $E \cdot A$ resulta de A al intercambiar los respectivos renglones y por lo tanto

$$\delta(E \cdot A) = -\delta(A) = \delta(E)\delta(A).$$

(*ii*) Si E es del tipo (II), entonces $E \cdot A$ resulta de A al multiplicar el correspondiente renglón por $\alpha \neq 0$ y por lo tanto

$$\delta(E \cdot A) = \alpha \cdot \delta(A) = \delta(E)\delta(A).$$

(*iii*) Si E es del tipo (III), entonces $E \cdot A$ resulta de A al realizar la misma operación elemental, luego $\delta(E \cdot A) = \delta(A) = 1 \cdot \delta(A) = \delta(E)\delta(A)$. ∎

El siguiente corolario se puede demostrar, sin ninguna dificultad, por inducción sobre $s \geq 1$ y queda como ejercicio (véase e ejercicio 15.5.1).

Corolario 15.5.19. *Sea δ un determinante en $M_{n\times n}(\mathbb{R})$ y $B \in M_{n\times n}(\mathbb{R})$. Entonces $\delta(E_1 \cdot \ldots \cdot E_s \cdot B) = \delta(E_1) \cdot \ldots \cdot \delta(E_s) \cdot \delta(B)$ para cualesquiera matrices elementales $E_1, \ldots, E_s \in M_{n\times n}(\mathbb{R})$. En particular $\delta(E_1 \cdot \ldots \cdot E_s) = \delta(E_1) \cdot \ldots \cdot \delta(E_s)$.*

Teorema 15.5.20. *Si δ es un determinante en $M_{n\times n}(\mathbb{R})$ y $A \in M_{n\times n}(\mathbb{R})$ es invertible, entonces $\delta(A) \neq 0$.*

Demostración. Si A es invertible, por el corolario 15.1.25, A es entonces producto de matrices elementales: $A = E_1 \cdot \ldots \cdot E_s$ y aplicando el corolario 15.5.19 cuando $B = I_{n\times n}$, obtenemos $\delta(A) = \delta(E_1) \cdot \ldots \cdot \delta(E_s)$. Por último, como $\delta(E_i) \neq 0$ para toda $i = 1, \ldots, s$, entonces $\delta(A) \neq 0$. ∎

Tenemos en general que para cualquier determinante δ en $M_{n\times n}(\mathbb{R})$ A invertible implica $\delta(A) \neq 0$ y A no invertible implica $\delta(A) = 0$. Esto es,

Corolario 15.5.21. *Sea δ un determinante en $M_{n\times n}(\mathbb{R})$ y $A \in M_{n\times n}(\mathbb{R})$. Entonces A es invertible si y sólo si $\delta(A) \neq 0$.*

Estamos ahora en condiciones de demostrar:

Teorema 15.5.22. *Sea δ un determinante en $M_{n\times n}(\mathbb{R})$ y sean $A, B \in M_{n\times n}(\mathbb{R})$. Entonces $\delta(A \cdot B) = \delta(A) \cdot \delta(B)$.*

Demostración. Consideramos por separado cuando A es invertible o no lo es.

1°/ Supongamos A invertible. Entonces $A = E_1 \cdot \ldots \cdot E_s$, donde E_i es elemental para cada $i = 1, \ldots, s$. Por el corolario 15.5.19,

$$\delta(A \cdot B) = \delta(E_1) \cdot \ldots \cdot \delta(E_s)\delta(B) = \delta(A) \cdot \delta(B).$$

2°/ Si A no es invertible, entonces $A \cdot B$ no es invertible (corolario 15.2.32) y por lo tanto $\delta(A) = 0 = \delta(A \cdot B)$, así se cumple $\delta(A \cdot B) = \delta(A) \cdot \delta(B)$. ∎

Proposición 15.5.23. *Si δ es un determinante en $M_{n\times n}(\mathbb{R})$, entonces*

$$\delta(A) = \delta(A^t).$$

Demostración.

1°/ $rango A < n$. Entonces $\delta(A) = 0$ (corolario 15.5.14) y como

$$rango A = rango A^t$$

por la proposición 15.3.13 , entonces $\delta(A^t) = 0$.
2°/ *rango*$A = n$. En este caso A es invertible y por lo tanto $A = E_1 \cdot \ldots \cdot E_k$ donde cada E_i es una matriz elemental. Luego $A^t = E_k^t \cdot \ldots \cdot E_1^t$ y

$$\delta(A^t) = \delta(E_k^t \cdot \ldots \cdot E_1^t) = \delta(E_k^t) \cdot \ldots \cdot \delta(E_1^t) = \delta(E_1) \cdot \ldots \cdot \delta(E_k) = \delta(E_1 \cdot \ldots \cdot E_k) = \delta(A).$$

■

Con este último teorema podemos demostrar que, en caso de existir un determinante en $M_{n\times n}(\mathbb{R})$, éste es único.

Teorema 15.5.24. *Si δ y δ' son determinantes en $M_{n\times n}(\mathbb{R})$, entonces $\delta = \delta'$.*

Demostración. Sea $A \in M_{n\times n}(\mathbb{R})$.

1°/ Si A es invertible, entonces $A = E_1 \cdot \ldots \cdot E_s$, donde E_i es elemental para cada $i = 1, \ldots, s$.

$$\begin{aligned} \delta(A) &= \delta(E_1) \cdot \ldots \cdot \delta(E_s) && \text{(corolario 15.5.19)} \\ &= \delta'(E_1) \cdot \ldots \cdot \delta'(E_s) && \text{(corolario 15.5.16)} \\ &= \delta'(E_1 \cdot \ldots \cdot E_s) && \text{(corolario 15.5.19)} \\ &= \delta'(A) \end{aligned}$$

2°/ Si A no es invertible, entonces para cualquier determinante $\delta(A) = 0$ (corolario 15.5.14). Luego $\delta(A) = 0 = \delta'(A)$.

■

Lo único que falta para terminar con nuestro estudio de determinantes es mostrar que efectivamente, para cada $n \geq 1$, siempre existe un determinante y daremos la definición recursivamente, esto es, definiremos un determinante en $M_{1\times 1}(\mathbb{R})$ y suponiendo que se tiene definido un determinante en $M_{n\times n}(\mathbb{R})$ para $n \geq 1$ definiremos uno en $M_{(n+1)\times(n+1)}(\mathbb{R})$.

Definición 15.5.25. (1) $\delta_1 : M_{1\times 1}(R) \longrightarrow \mathbb{R}$, $\delta_1(A) = a$ *si* $A = (a)$.
(2) *Supongamos que se tiene definido el determinante* $\delta_n : M_{n\times n}(\mathbb{R}) \longrightarrow \mathbb{R}$ $(n \geq 1)$ *y sea* $A = (a_{ij}) \in M_{(n+1)\times(n+1)}(\mathbb{R})$*;* $\delta_{n+1}(A) = \sum_{i=1}^{n+1}(-1)^{i+j} a_{ij}\delta_n(A_{ij})$ *donde* j *es fijo con* $1 \leq j \leq n+1$ *y* A_{ij} *es la matriz que resulta de* A *al eliminar el renglón* i *y la columna* j *y por lo cual es de orden* $n \times n$.

Debemos verificar que esta última definición que hemos dado tiene sentido, es decir, para cada $n \geq 1$ la función $\delta_{(n+1)} : M_{(n+1)\times(n+1)}(\mathbb{R}) \longrightarrow \mathbb{R}$ es efectivamente un determinante.

Teorema 15.5.26. *Si $\delta : M_{n\times n}(\mathbb{R}) \longrightarrow \mathbb{R}$ es un determinante, entonces para cada j fijo $1 \leq j \leq n+1$, la función $\delta_j : M_{(n+1)\times(n+1)}(\mathbb{R}) \longrightarrow \mathbb{R}$ definida por la expresión $\delta_j(A) = \sum_{i=1}^{n+1}(-1)^{i+j}a_{ij}\delta(A_{ij})$ es un determinante.*

Demostración.

(1) δ_j es $(n+1)$-lineal

Debemos demostrar que δ_j es lineal en cada renglón $k = 1, \ldots, (n+1)$. Para esto sea $A = \begin{pmatrix} A_1 \\ \vdots \\ A_k \\ \vdots \\ A_{n+1} \end{pmatrix}$ y supongamos que $A_k = A'_k + A''_k$. Sean $A' = \begin{pmatrix} A_1 \\ \vdots \\ A'_k \\ \vdots \\ A_{n+1} \end{pmatrix}$ y $A'' = \begin{pmatrix} A_1 \\ \vdots \\ A''_k \\ \vdots \\ A_{n+1} \end{pmatrix}$ y para $i \neq k$ escribimos $A'_{ij} = \begin{pmatrix} A_1 \\ \vdots \\ A'_k \\ \vdots \\ A_{n+1} \end{pmatrix}$ y $A''_{ij} = \begin{pmatrix} A_1 \\ \vdots \\ A''_k \\ \vdots \\ A_{n+1} \end{pmatrix}$ donde en A'_{ij} y A''_{ij} se han suprimido el renglón i y la columna j de A'y A'' respectivamente. Entonces en estas matrices aparece el renglón k. Teniendo en cuenta que δ es un determinante, $\delta(A_{ij}) = \delta(A'_{ij}) + \delta(A''_{ij})$, para $i \neq k$.

$$\begin{aligned}
\delta_j(A) &= (-1)^{1+j}a_{1j}\delta(A_{1j}) + \cdots + (-1)^{k+j}(a'_{kj} + a''_{kj})\delta(A_{kj}) + \cdots + (-1)^{(n+1)+j}a_{(n+1)j}\delta(A_{(n+1)j}) \\
&= (-1)^{1+j}a_{1j}(\delta(A'_{1j}) + \delta(A''_{1j})) + \cdots + (-1)^{k+j}(a'_{kj} + a''_{kj})\delta(A_{kj}) + \cdots + \\
&\quad (-1)^{(n+1)+j}a_{(n+1)j}(\delta(A'_{(n+1)j}) + \delta(A''_{(n+1)j})) \\
&= [(-1)^{1+j}a_{1j}\delta(A'_{1j}) + \cdots + (-1)^{k+j}a'_{kj}\delta(A_{kj}) + \cdots + (-1)^{(n+1)+j}a_{(n+1)j}\delta(A'_{(n+1)j})] + \\
&\quad [(-1)^{1+j}a_{1j}\delta(A''_{1j}) + \cdots + (-1)^{k+j}a''_{kj}\delta(A_{kj}) + \cdots + (-1)^{(n+1)+j}a_{(n+1)j}\delta(A''_{(n+1)j})] \\
&= \delta_j(A') + \delta_j(A'').
\end{aligned}$$

Ahora sea $A = \begin{pmatrix} A_1 \\ \vdots \\ \alpha A_k \\ \vdots \\ A_{n+1} \end{pmatrix}$. Entonces, para cada $i \neq k$, en A_{ij} aparece el renglón k. Sea $A' = \begin{pmatrix} A_1 \\ \vdots \\ A_k \\ \vdots \\ A_{n+1} \end{pmatrix}$ y A'_{ij} la correspondiente matriz A'_{ij} (es decir, las matrices

que resultan de A' al eliminar el renglón i y la columna j). Como δ es un determinante, para estas matrices, $\delta(A_{ij}) = \alpha\delta(A'_{ij})$ debido a que $i \neq k$ y el renglón k está multiplicado por α.

$$\begin{aligned}
\delta_j(A) &= (-1)^{1+j}a_{1j}\delta(A_{1j}) + \cdots + (-1)^{k+j}(\alpha a_{kj})\delta(A_{kj}) + \cdots + \\
&\quad (-1)^{(n+1)+j}a_{(n+1)j}\delta(A_{(n+1)j}) \\
&= (-1)^{1+j}a_{1j}\alpha\cdot\delta(A'_{1j})+\cdots+(-1)^{k+j}\alpha a_{kj}\delta(A_{kj})+\cdots+(-1)^{(n+1)+j}a_{(n+1)j}\alpha\cdot \\
&\quad \delta(A'_{(n+1)j}) \\
&= \alpha \cdot ((-1)^{1+j}a_{1j}\delta(A'_{1j}) + \cdots + (-1)^{k+j}a_{kj}\delta(A_{kj}) + \cdots + \\
&\quad (-1)^{(n+1)+j}a_{(n+1)j}\delta(A'_{(n+1)j})) \\
&= \alpha \cdot \delta_j(A').
\end{aligned}$$

Concluimos entonces que δ_j es $(n+1)$-lineal.

(2) δ_j es alternante.

Supongamos que en A el renglón k es igual al renglón $k+1$, es decir, $A_k = A_{k+1}$. Entonces para $i \neq k$ y $i \neq k+1$, A_{ij} tiene los renglones correspondientes a los renglones k y $k+1$ de A iguales y por lo tanto $\delta(A_{ij}) = 0$. Luego

$$\begin{aligned}
\delta_j(A) &= (-1)^{1+j}a_{1j}\delta(A_{1j})+\cdots+(-1)^{k+j}a_{kj}\delta(A_{kj})+(-1)^{(k+1)+j}a_{(k+1)j}\delta(A_{(k+1)j})+ \\
&\quad \cdots + (-1)^{(n+1)+j}a_{(n+1)j}\delta(A_{(n+1)j}) \\
&= (-1)^{k+j}a_{kj}\delta(A_{kj}) + (-1)^{(k+1)+j}a_{(k+1)j}\delta(A_{(k+1)j}) \\
&= (-1)^{k+j}(a_{kj}\delta(A_{kj}) - a_{(k+1)j}\delta(A_{(k+1)j})) \\
&= 0.
\end{aligned}$$

ya que $a_{kj} = a_{(k+1)j}$ y $\delta(A_{kj}) = \delta(A_{(k+1)j})$.

(3) $\delta_j(I_{(n+1)\times(n+1)}) = 1$.

$$\begin{aligned}
\delta_j(I_{(n+1)\times(n+1)}) &= (-1)^{1+j}0\cdot\delta((I_{(n+1)\times(n+1)})_{1j}) + \cdots + (-1)^{j+j}1\cdot\delta((I_{(n+1)\times(n+1)})_{jj}) + \\
&\quad \cdots + (-1)^{(n+1)+j}0\cdot\delta(A_{(n+1)j}) \\
&= (-1)^{2j}\delta((I_{(n+1)\times(n+1)})_{jj}) \\
&= \delta(I_{(n+1)\times(n+1)}) \\
&= 1.
\end{aligned}$$

puesto que al eliminar el renglón j y la columna j en $I_{(n+1)\times(n+1)}$ obtenemos $I_{n\times n}$.

Luego δ_j es un determinante. ∎

Tenemos entonces, para cada $n \geq 1$, definido un determinante y por lo tanto es el único por el teorema 15.5.24. Por esta razón y debido a que la definición es

completamente similar para cada $n \geq 1$, usaremos **det** en lugar de δ, sin importar quién es n.

Corolario 15.5.27. *Para cualesquiera j y k, $1 \leq j, k, s \leq n$,*

$$\begin{aligned}\sum_{i=1}^{n}(-1)^{i+j}a_{ij}\det(A_{ij}) &= \sum_{i=1}^{n}(-1)^{i+k}a_{ik}\det(A_{ik}) \\ &= \sum_{s=1}^{n}(-1)^{j+s}a_{js}\det(A_{js}) \\ &= \sum_{s=1}^{n}(-1)^{k+s}a_{ks}\det(A_{ks}).\end{aligned}$$

Demostración. Es inmediato de la unicidad del determinante y del hecho de que $\det(A) = \det(A^t)$ (proposición 15.5.23). ∎

En la definición del determinante de A, $\det(A) = \sum_{i=1}^{n}(-1)^{i+j}a_{ij}\det(A_{ij})$ donde j es fijo, lo llamaremos ***la expansión de* det(A) *a través de la columna j*** o si $\det(A) = \sum_{j=1}^{n}(-1)^{i+j}a_{ij}\det(A_{ij})$ lo llamaremos ***la expansión de* det(A) *a través del renglón i***. A $\det(A_{ij})$ y a $(-1)^{i+j}\det(A_{ij})$ se les llama el ***menor de a_{ij}*** y el ***cofactor de a_{ij}***, respectivamente.

Decimos que una matriz $A = (a_{ij}) \in M_{n\times n}(\mathbb{R})$ es ***triangular superior*** (***inferior***) si $a_{ij} = 0$ para $i > j$ ($a_{ij} = 0$ para $i < j$).

Proposición 15.5.28. *Sea $A = (a_{ij}) \in M_{n\times n}(\mathbb{R})$ triangular superior (inferior). Entonces*

$$\det(A) = a_{11} \cdot a_{22} \cdot \ldots \cdot a_{nn}.$$

Demostración.

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1i} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2i} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots\vdots & \vdots & \vdots\vdots & \vdots \\ 0 & 0 & \cdots & a_{ii} & \cdots & a_{in} \\ \vdots & \vdots & \vdots\vdots & \vdots & \vdots\vdots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & a_{mn} \end{pmatrix}$$

Demostraremos el resultado por inducción sobre n:

1°/ $n = 1$, $A = (a)$ y $\det(A) = a$.

2°/ Supongamos cierto el resultado para n y sea una matriz triangular superior $A = (a_{ij}) \in M_{(n+1)\times(n+1)}(\mathbb{R})$. Si desarrollamos el determinante de A a través de la primera columna tenemos
$\det(A) = \sum_{i=1}^{n}(-1)^{i+1}a_{i1}\det(A_{i1}) = (-1)^{1+1}a_{11}\det(A_{11})$ ya que para $i > 1$, $a_{i1} = 0$.
Pero A_{11} es una matriz triangular superior, por lo que por hipótesis de inducción, $\det(A) = a_{22} \cdot \ldots \cdot a_{nn}$. Luego $\det(A_{11}) = a_{11} \cdot a_{22} \cdot \ldots \cdot a_{nn}$. ∎

Como se verá en el ejemplo 15.5.30 aplicar la propiedad para calcular un determinante resulta ser de gran utilidad. Antes de dar estos ejemplos, enlistamos todas las propiedades del determinante.

(1) $\det(I_{n\times n}) = 1$.

(2) $\det\begin{pmatrix} A_1 \\ \vdots \\ A_i + A_i' \\ \vdots \\ A_n \end{pmatrix} = \det\begin{pmatrix} A_1 \\ \vdots \\ A_i \\ \vdots \\ A_n \end{pmatrix} + \det\begin{pmatrix} A_1 \\ \vdots \\ A_i' \\ \vdots \\ A_n \end{pmatrix}$, y

$\det\begin{pmatrix} A^1 & \cdots & A^i + A^{i'} & \cdots & A^n \end{pmatrix} = \det\begin{pmatrix} A^1 & \cdots & A^i & \cdots & A^n \end{pmatrix} + \det\begin{pmatrix} A^1 & \cdots & A^{i'} & \cdots & A^n \end{pmatrix}$, donde A^j denota la j-ésima columna de A para $j = 1, \ldots, n$.

(3)
$$\det\begin{pmatrix} A_1 \\ \vdots \\ \alpha \cdot A_i' \\ \vdots \\ A_n \end{pmatrix} = \alpha \cdot \det\begin{pmatrix} A_1 \\ \vdots \\ A_i \\ \vdots \\ A_n \end{pmatrix},$$

y

$$\det\begin{pmatrix} A^1 & \cdots & \alpha \cdot A^i & \cdots & A^n \end{pmatrix} = \alpha \cdot \det\begin{pmatrix} A^1 & \cdots & A^i & \cdots & A^n \end{pmatrix}.$$

(4) $\det(A) = 0$ si A tiene dos renglones (columnas) iguales.

(5) Si B se obtiene de A al intercambiar dos renglones (columnas), entonces $\det(B) = -\det(A)$.

(6) Si A tiene un renglón (columna) de ceros, entonces $\det(A) = 0$.

(7) Si B se obtiene de A al sumar a un renglón (columna) α veces otro renglón (columna) entonces $\det(B) = \det(A)$.

(8) A es invertible si y sólo si $\det(A) \neq 0$.

(9) $\det(A \cdot B) = \det(A) \cdot \det(B)$.

(10) $\det(A) = \det(A^t)$.

(11) Si $A = (a_{ij})$ es una matriz triangular superior (inferior), entonces

$$\det(A) = a_{11} \cdot a_{22} \cdot \ldots \cdot a_{nn}.$$

Ejemplo 15.5.29. Sea $A = \begin{pmatrix} 3 & 1 & 1 \\ -2 & -1 & 0 \\ 1 & 2 & 1 \end{pmatrix}$. Desarrollaremos el determinante a través de la columna 3.

$$\begin{aligned} \det \begin{pmatrix} 3 & 1 & 1 \\ -2 & -1 & 0 \\ 1 & 2 & 1 \end{pmatrix} &= \\ & (-1)^{1+3} \cdot 1 \cdot \det \begin{pmatrix} -2 & -1 \\ 1 & 2 \end{pmatrix} + (-1)^{2+3} \cdot 0 \cdot \det \begin{pmatrix} 3 & 1 \\ 1 & 2 \end{pmatrix} + (-1)^{3+3} \cdot 1 \cdot \det \begin{pmatrix} 3 & 1 \\ -2 & -1 \end{pmatrix} \\ &= \det \begin{pmatrix} -2 & -1 \\ 1 & 2 \end{pmatrix} + \det \begin{pmatrix} 3 & 1 \\ -2 & -1 \end{pmatrix} \\ &= (-2) \cdot 2 - (-1) \cdot 1 + 3 \cdot (-1) - (-2) \cdot 1 = -4. \end{aligned}$$

Entonces $\det(A) = -4 \neq 0$ y con esto podemos afirmar que A es invertible.

Ejemplo 15.5.30. Calculemos ahora el $\det(A)$ del ejemplo 15.5.29 usando las propiedades del determinante.

$$\begin{aligned} \det \begin{pmatrix} 3 & 1 & 1 \\ -2 & -1 & 0 \\ 1 & 2 & 1 \end{pmatrix} &= -\det \begin{pmatrix} 1 & 1 & 3 \\ 0 & -1 & -2 \\ 1 & 2 & 1 \end{pmatrix} \\ &= -\det \begin{pmatrix} 1 & 1 & 3 \\ 0 & -1 & -2 \\ 0 & 1 & -2 \end{pmatrix} \\ &= -\det \begin{pmatrix} -1 & -2 \\ 1 & -2 \end{pmatrix} \\ &= -\det \begin{pmatrix} -1 & -2 \\ 0 & -4 \end{pmatrix} \\ &= -4. \end{aligned}$$

Volviendo ahora a un sistema de n ecuaciones lineales en n indeterminadas presentada como una ecuación matricial $A \cdot \overline{x} = \overline{b}$ no es difícil ver que en el caso en que A es invertible tiene una única solución que es $\overline{x} = A^{-1}\overline{b}$, así que todo consiste en encontrar A^{-1} que por cierto tenemos un método para encontrarla (véase el teorema 15.1.24). Sin embargo existe otra manera de obtener esta inversa y es mediante el uso del determinante. Para esto definimos la adjunta (clásica) de una matriz.

Sea $A = (a_{ij}) \in M_{n\times n}(\mathbb{R})$ y para cada i, j, $1 \leq i, j \leq n$ sea $\widetilde{A}_{ij}$ el cofactor de a_{ij}, es decir, $\widetilde{A}_{ij} = (-1)^{i+j} \cdot \det(A_{ij})$, donde A_{ij} se obtiene de A al eliminar el renglón i y la columna j.

Definición 15.5.31. *Dada $A = (a_{ij}) \in M_{n\times n}(\mathbb{R})$, la* **adjunta A^a** *de A es la matriz $A^a = \left(\widetilde{A}_{ij}\right)^t$. Esto es, la entrada ij de A^a es $(-1)^{j+i} \det(A_{ij})$.*

Ejemplo 15.5.32. Sea $A = \begin{pmatrix} -1 & 0 & 1 \\ 1 & 1 & -1 \\ 2 & 3 & 0 \end{pmatrix}$. Para obtener A^a debemos encontrar los valores de $\widetilde{A}_{ij}$, $1 \leq i, j \leq 3$.

$\widetilde{A}_{11} = (-1)^{1+1}\det\begin{pmatrix} 1 & -1 \\ 3 & 0 \end{pmatrix} = 3$, $\widetilde{A}_{12} = (-1)^{1+2}\det\begin{pmatrix} 1 & -1 \\ 2 & 0 \end{pmatrix} = -2$,
$\widetilde{A}_{13} = (-1)^{1+3}\det\begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix} = 1$, $\widetilde{A}_{21} = (-1)^{2+1}\det\begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix} = 3$,
$\widetilde{A}_{22} = (-1)^{2+2}\det\begin{pmatrix} -1 & 1 \\ 2 & 0 \end{pmatrix} = -2$, $\widetilde{A}_{23} = (-1)^{2+3}\det\begin{pmatrix} -1 & 0 \\ 2 & 3 \end{pmatrix} = 3$,
$\widetilde{A}_{31} = (-1)^{3+1}\det\begin{pmatrix} 0 & 1 \\ 1 & -0 \end{pmatrix} = -1$, $\widetilde{A}_{32} = (-1)^{3+2}\det\begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix} = 0$,
$\widetilde{A}_{33} = (-1)^{3+3}\det\begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} = -1$.

Entonces $A^a = \begin{pmatrix} 3 & -2 & 1 \\ 3 & -2 & 3 \\ -1 & 0 & -1 \end{pmatrix}^t = \begin{pmatrix} 3 & 3 & -1 \\ -2 & -2 & 0 \\ 1 & 3 & -1 \end{pmatrix}$

$$A \cdot A^a = \begin{pmatrix} -1 & 0 & 1 \\ 1 & 1 & -1 \\ 2 & 3 & 0 \end{pmatrix} \cdot \begin{pmatrix} 3 & 3 & -1 \\ -2 & -2 & 0 \\ 1 & 3 & -1 \end{pmatrix} = \begin{pmatrix} -2 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -2 \end{pmatrix} = (-2) \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (-2) \cdot I_{3\times 3}.$$

Como veremos en el siguiente teorema, no es casualidad la forma de $A \cdot A^a$ en este ejemplo.

Teorema 15.5.33. *Sea $A \in M_{n\times n}(\mathbb{R})$. Entonces $A \cdot A^a = \det(A) \cdot I_{n\times n}$.*

Demostración. Sean $A = (a_{ij})$ y $A^a = \left(\widetilde{A}_{ij}\right)^t$. Luego $A \cdot A^a = (c_{ij})$ donde

$$c_{ij} = \sum_{k=1}^{n} a_{ik}(A^a)_{kj} = \sum_{k=1}^{n} (-1)^{j+k} a_{ik} \cdot \det(A_{jk}).$$

Para $i \neq j$, sea A'_{ij} la matriz que resulta de A al sustituir el renglón j por el renglón i. Entonces $A'_{ij} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \vdots & \vdots & \vdots & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$ $\begin{matrix} \\ \\ -\text{renglón } i \\ \\ -\text{renglón } j \\ \\ \\ \end{matrix}$ y como tiene dos renglones iguales, $\det(A'_{ij}) = 0$.

Ahora, desarrollando $\det(A'_{ij})$ a través del renglón j tenemos

$$\det(A'_{ij}) = \sum_{k=1}^{n} (-1)^{j+k} a_{ik} \det(A_{jk}) = c_{ij}$$

con lo cual $c_{ij} = 0$ para cualesquiera i, j con $i \neq j$.

Veamos qué pasa cuando $i = j$.

$c_{ii} = \sum_{k=1}^{n} a_{ik}\widetilde{A}_{ik} = \sum_{k=1}^{n} (-1)^{i+k} a_{ik} \det(A_{ik}) = \det(A)$.

Por lo tanto $A \cdot A^a = \begin{pmatrix} \det(A) & 0 & \cdots & 0 \\ 0 & \det(A) & \cdots & 0 \\ \vdots & \vdots & \vdots\vdots\vdots & \vdots \\ 0 & 0 & \cdots & \det(A) \end{pmatrix} = \det(A) \cdot I_{n\times n}$. ■

Corolario 15.5.34. *Si A es invertible, entonces* $A^{-1} = \frac{1}{\det(A)} \cdot A^a$.

Demostración. Como A es invertible, entonces $\det(A) \neq 0$ y por el teorema 15.5.33, $A \cdot \left(\frac{1}{\det(A)} \cdot A^a\right) = I_{n\times n}$. y entonces $A^{-1} = \frac{1}{\det(A)} \cdot A^a$. ■

Ejemplo 15.5.35. La matriz A del ejemplo 15.5.32 es invertible con $\det(A) = -2$, así que $A^{-1} = -\frac{1}{2}\begin{pmatrix} 3 & 3 & -1 \\ -2 & -2 & 0 \\ 1 & 3 & -1 \end{pmatrix} = \begin{pmatrix} \frac{3}{2} & -\frac{3}{2} & \frac{1}{2} \\ 1 & 1 & 0 \\ -\frac{1}{2} & -\frac{3}{2} & \frac{1}{2} \end{pmatrix}$.

Sea $A \cdot \overline{x} = \overline{b}$ un sistema de n ecuaciones en n indeterminadas. En el caso en que $\det(A) \neq 0$, es decir A invertible, existe una manera de obtener la solución (la cual sabemos que es única) mediante el uso de determinantes y a este método se le llama la *regla de Cramer*. En realidad la importancia de este método es fundamentalmente teórico puesto que en la práctica debemos encontrar el valor de $n+1$ determinantes, lo que resulta un proceso largo en comparación con escalonar la matriz. Por cierto, lo mismo se puede decir de la matriz adjunta, en donde debemos encontrar el valor de n^2 determinantes.

Teorema 15.5.36. *Sea* $A \cdot \overline{x} = \overline{b}$ *un sistema de n ecuaciones en n indeterminadas. Si* $\det(A) \neq 0$, *entonces la única solución del sistema está dada por* $x_j = \frac{\det(B_j)}{\det(A)}$ *donde* B_j *es la matriz obtenida de A al sustituir la columna* j *de A por* $\overline{b} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$ *para* $j = 1, \ldots, n$.

Demostración. Multiplicando el sistema por A^a a la izquierda, tenemos $A^a \cdot A \cdot \overline{x} = A^a \cdot \overline{b}$ y como $A^a \cdot A = \det(A) \cdot I_{n\times n}$, entonces $\det(A) \cdot I_{n\times n} \cdot \overline{x} = A^a \cdot \overline{b}$. El renglón j de $A^a \cdot \overline{b}$ se obtiene de multiplicar el renglón j de A^a por $\overline{b}$ que es $\sum_{i=1}^{n} \widetilde{A}_{ij} \cdot b_j = \sum_{i=1}^{n} (-1)^{i+j} \cdot b_j \cdot \det(A_{ij}) = \det(B_j)$ donde B_j es como en el enunciado del teorema. Luego, para cada $j = 1, \ldots, n$, se tiene la igualdad $\det(A) \cdot x_j = \sum_{i=1}^{n} (-1)^{i+j} \cdot b_i \cdot \det(A_{ij}) = \det(B_j)$ y por lo tanto $x_j = \frac{\det(B_j)}{\det(A)}$. ■

Ejemplo 15.5.37. Consideramos el siguiente sistema de ecuaciones

$$\begin{cases} x_1 - 2x_2 + x_3 = -1 \\ x_1 + x_2 - x_3 = 2 \\ x_1 - x_2 + 3x_3 = -2 \end{cases}$$

Como $\det(A) = \det\begin{pmatrix} 1 & -2 & 1 \\ 1 & 1 & -1 \\ 1 & -1 & 3 \end{pmatrix} = 1 \cdot \det\begin{pmatrix} 1 & -1 \\ -1 & 3 \end{pmatrix} - (-2) \cdot \det\begin{pmatrix} 1 & -1 \\ 1 & 3 \end{pmatrix} + 1 \cdot \det\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = 2 + 8 - 2 = 8$, la solución del sistema está dada como en el teorema 15.5.36

$\det(B_1) = \det\begin{pmatrix} -1 & -2 & 1 \\ 2 & 1 & -1 \\ -2 & -1 & 3 \end{pmatrix} = (-1)\cdot\det\begin{pmatrix} 1 & -1 \\ -1 & 3 \end{pmatrix} - (-2)\cdot\det\begin{pmatrix} 2 & -1 \\ -2 & 3 \end{pmatrix} + 1\cdot\det\begin{pmatrix} 2 & 1 \\ -2 & -1 \end{pmatrix} = -2 + 8 = 6$

$\det(B_2) = \det\begin{pmatrix} 1 & -1 & 1 \\ 1 & 2 & -1 \\ 1 & -2 & 3 \end{pmatrix} = 1 \cdot \det\begin{pmatrix} 2 & -1 \\ -2 & 3 \end{pmatrix} - (-1) \cdot \det\begin{pmatrix} 1 & -1 \\ 1 & 3 \end{pmatrix} + 1 \cdot \det\begin{pmatrix} 1 & 2 \\ 1 & -2 \end{pmatrix} = 4 + 4 - 4 = 4$

$\det(B_3) = \det\begin{pmatrix} 1 & -2 & -1 \\ 1 & 1 & 2 \\ 1 & -1 & -2 \end{pmatrix} = 1 \cdot \det\begin{pmatrix} 1 & 2 \\ -1 & -2 \end{pmatrix} - 1 \cdot \det\begin{pmatrix} -2 & -1 \\ -1 & -2 \end{pmatrix} + 1 \cdot \det\begin{pmatrix} -2 & -1 \\ 1 & 2 \end{pmatrix} = -3 - 3 = -6$

Luego la solución del sistema es $x_1 = \frac{6}{8} = \frac{3}{4}$, $x_2 = \frac{4}{8} = \frac{1}{2}$, $x_3 = \frac{-6}{8} = -\frac{3}{4}$.

§§ Ejercicios sección 15.1.

15.1.1. Demuestre que si $A, B \in M_{n\times n}(\mathbb{R})$ y $A \cdot B$ no es invertible, entonces A no es invertible o B no es invertible.

15.1.2. Determine los valores x, y, z tales que

$$\begin{pmatrix} 0 & 2 & -3 \\ 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} x+y & 2 & x+z \\ x & 0 & 1 \end{pmatrix}$$

en $M_{2\times 3}(\mathbb{R})$.

15.1.3. Sean

$$A = \begin{pmatrix} 2 & 1 & 4 \\ -1 & 0 & 3 \end{pmatrix}, B = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \end{pmatrix}, C = \begin{pmatrix} 0 & 1 & 2 \\ 5 & 4 & -3 \end{pmatrix}.$$

Encuentre lo siguiente

(a) $A + B$ (b) $(A + B) + C$ (c) $B - C$
(d) $2A$ (e) $2A + 3B$ (f) $2B - 4C$
(g) $A + 2B - 3C$ (h) $2\,(3B)$

15.1.4. [1] Para cada $i \in \{1,\dots,m\}$ y $j \in \{1,\dots,n\}$ sea e_{ij} la matriz en $M_{m\times n}\mathbb{R}$ que tiene 1 en el lugar ij y cero en los demás. Demuestre que

$$\{e_{ij} \mid i = 1,\dots,m \text{ y } j = 1,\dots,n\}$$

es una base de $M_{m\times n}\mathbb{R}$.

15.1.5. Realice los siguientes productos de matrices.

1) $\begin{pmatrix} 1 & 3 & 3 \end{pmatrix} \cdot \begin{pmatrix} -2 & 0 \\ 0 & -1 \\ 2 & 1 \end{pmatrix}$

2) $\begin{pmatrix} 1 & 1 & 2 \\ 1 & 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}$

3) $\begin{pmatrix} 1 & -2 \\ 0 & 3 \end{pmatrix} \cdot \begin{pmatrix} 2 & 6 \\ 6 & 8 \end{pmatrix}$

4) $\begin{pmatrix} 1 & 1 & -1 \\ 2 & -2 & 3 \\ 4 & 0 & -5 \\ 1 & 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 3 & 0 & 4 \\ -1 & 0 & 6 \\ 7 & 7 & 2 \end{pmatrix}$

5) $\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & \pi \\ 0 & \sqrt{2} & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \\ e & f \end{pmatrix}$

6) $\begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & -\frac{1}{2} \\ \frac{1}{2} & 1 \\ 1 & 1 \end{pmatrix}$

7) $\begin{pmatrix} 2 & -3 & -5 \\ -1 & 4 & 5 \\ 1 & -3 & -4 \end{pmatrix} \cdot \begin{pmatrix} 1 & -3 & -4 \\ 2 & -3 & -5 \\ -1 & 4 & 5 \end{pmatrix}$

8) $\begin{pmatrix} -1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix}$

9) $\begin{pmatrix} x & y \end{pmatrix} \cdot \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}$

15.1.6. Realice todas las multiplicaciones que estén definidas entre las siguientes matrices:

$$A = \begin{pmatrix} 5 & -1 & 2 \\ 0 & 7 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ -2 & 3 \\ 5 & 4 \\ 0 & 1 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & -1 & 1 \\ 2 & 0 & 1 \\ 3 & 0 & 1 \end{pmatrix},$$

$$E = \begin{pmatrix} 2 & -2 \\ 1 & 3 \\ 4 & 4 \end{pmatrix}.$$

[1] Parte del corolario 15.2.29 pág. 564.

15.1.7. Sean A y B matrices ¿Qué puede concluir acerca de los órdenes de A y B, si los productos $A \cdot B$ y $B \cdot A$ están definidos?

15.1.8. Explique por qué no es válida, en general, la siguiente fórmula, en donde A y B son matrices cuadradas del mismo orden:

$$(A + B)^2 = A^2 + 2 \cdot AB + B^2.$$

Dé un contraejemplo.

15.1.9. Pruebe que las matrices $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ y $B = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$ en $M_{2\times2}(\mathbb{R})$ conmutan.

15.1.10. Obtener todas las matrices en $M_{3\times3}(\mathbb{R})$ que conmutan con la matriz $A = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}$.

15.1.11. Sea la matriz $A = \begin{pmatrix} 2 & 1 \\ 1 & a \end{pmatrix}$ en $M_{2\times2}(\mathbb{R})$. Decir la condición que ha de verificar el número real a para que existan matrices $B \in M_{2\times2}(\mathbb{R})$, $B \neq \widetilde{0}$, verificando que $A \cdot B = \widetilde{0}$

15.1.12. Dé ejemplos de matrices A y B en $M_{3\times3}(\mathbb{R})$ tales que $A \cdot B = \widetilde{0}$, pero $A \neq \widetilde{0}$ y $B \neq \widetilde{0}$.

15.1.13. Demuestre que no hay matrices A y B en $M_{2\times2}(\mathbb{R})$ tales que

$$A \cdot B - B \cdot A = I_{2\times2}.$$

Definición. Si $A \in M_{n\times n}(\mathbb{R})$, se define A^k, para $k \in \mathbb{N}$, por recursión.

(1) Para $k = 0$, definimos $A^0 = I_{n\times n}$;
(2) Si A^k está definido, definimos $A^{k+1} = A^k \cdot A$.

15.1.14. Calcule A^2, A^3, A^4 y A^5 donde $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$.

15.1.15. Sea $A \in M_{n\times n}(\mathbb{R})$, y sean $r, s \in \mathbb{N}$. Demuestre que

(*a*) $A^r \cdot A^s = A^{r+s}$;
(*b*) $(A^r)^s = A^{rs}$.

15.1.16. Sean $A, B \in M_{n\times n}(\mathbb{R})$. Demuestre que si $A\cdot B = B\cdot A$, entonces $(A\cdot B)^n = A^n\cdot B^n$ para todo $n \in \mathbb{N}$. Mediante un ejemplo muestre que esto no ocurre con todas las matrices en $M_{n\times n}(\mathbb{R})$.

15.1.17. Sea $A = \begin{pmatrix} 7 & 4 \\ -9 & -5 \end{pmatrix}$. Compruebe que $A^n = \begin{pmatrix} 1+6n & 4n \\ -9n & 1-6n \end{pmatrix}$, para $n \in \mathbb{N}$.

15.1.18. Sea $A = \begin{pmatrix} \cos(\theta) & -\operatorname{sen}(\theta) \\ \operatorname{sen}(\theta) & \cos(\theta) \end{pmatrix}$.

(1) Demuestre que $A^2 = \begin{pmatrix} \cos(2\theta) & -\operatorname{sen}(2\theta) \\ \operatorname{sen}(2\theta) & \cos(2\theta) \end{pmatrix}$.

(2) Demuestre, mediante inducción matemática, que

$$A^n = \begin{pmatrix} \cos(n\theta) & -\operatorname{sen}(n\theta) \\ \operatorname{sen}(n\theta) & \cos(n\theta) \end{pmatrix}$$

para $n \geq 1$.

15.1.19. Sea $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$. Encuentre una fórmula para A^n $(n \in \mathbb{N})$ y verifique su fórmula usando inducción matemática.

Matriz inversa

15.1.20. Mediante inducción, demuestre que si $A_1, A_2, \ldots, A_s \in M_{n\times n}(\mathbb{R})$ son matrices invertibles, entonces el producto $A_1A_2\cdots A_s$ es invertible y

$$(A_1A_2\cdots A_s)^{-1} = A_1^{-1}A_2^{-1}\cdots A_s^{-1}.$$

15.1.21.

(*a*) Proporcione un contraejemplo para demostrar que $(AB)^{-1} \neq A^{-1}B^{-1}$ en general.

(*b*) ¿En que condiciones de A y B, $(AB)^{-1} = A^{-1}B^{-1}$? Pruebe su afirmación.

15.1.22. Demuestre que si $A, B \in M_{n\times n}(\mathbb{R})$ y $A\cdot B$ no es invertible, entonces A no es invertible o B no es invertible.

15.1.23. Sean $A, B \in M_{n\times n}(\mathbb{R})$ matrices invertibles. ¿Es invertible $A + B$?

15.1.24. Sea $A \in M_{n\times n}(\mathbb{R})$. Probar que si $A^2 = A\cdot A = \widetilde{0}$ y $A \neq I_{n\times n}$, entonces A no es invertible.

15.1.25.

(*a*) Sean $A, B, C \in M_{n\times n}(\mathbb{R})$. Demuestre que si A es invertible y $BA = CA$, entonces $B = C$.
(*b*) Ofrezca un contraejemplo para mostrar que el resultado en el inciso (*a*) puede fallar si A no es invertible.

15.1.26. Sean $A, B \in M_{n\times n}(\mathbb{R})$. Pruébese que si $I_{n\times n} - A \cdot B$ es invertible, entonces $I_{n\times n} - B \cdot A$ también es invertible y que

$$(I_{n\times n} - B \cdot A)^{-1} = I_{n\times n} + B \cdot (I_{n\times n} - A \cdot B)^{-1} \cdot A.$$

15.1.27. Determinar, en cada uno de los siguientes pares de matrices A y B, si la matriz B es la inversa de la matriz A.

$$(a)\ A = \begin{pmatrix} 5 & 0 & 0 \\ 0 & \frac{1}{3} & 0 \\ 0 & 0 & -2 \end{pmatrix}, B = \begin{pmatrix} \frac{1}{5} & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & -\frac{1}{2} \end{pmatrix};$$

$$(b)\ A = \begin{pmatrix} 1 & 1 & -1 \\ -3 & 2 & -1 \\ 3 & -3 & 2 \end{pmatrix}, B = \begin{pmatrix} 1 & 1 & 1 \\ 3 & 5 & 4 \\ 3 & 6 & 5 \end{pmatrix};$$

$$(c)\ A = \begin{pmatrix} 0 & 1 & -1 \\ 2 & -2 & 1 \\ -1 & 1 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 1 & 1 \end{pmatrix}.$$

15.1.28. Sea

$$A = \begin{pmatrix} -1 & 1 & 2 & 1 \\ 1 & 1 & 0 & 1 \\ 2 & 1 & -1 & 2 \end{pmatrix}.$$

Comprobar que realizar sobre ella cada una de las siguientes operaciones elementales por renglones equivale a multiplicar por la izquierda por la matriz resultante de aplicar a $I_{3\times 3}$ la misma operación.

(1) Intercambiar los renglones 1 y 3.
(2) Multiplicar el renglón 2 por el número real $3 \neq 0$.
(3) Sumar al renglón 2 el renglón 1 multiplicado por -2.

15.1.29. Sean

$$A = \begin{pmatrix} 1 & 2 & -1 \\ 1 & 1 & 1 \\ 1 & -1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & -1 & 0 \\ 1 & 1 & 1 \\ 1 & 2 & -1 \end{pmatrix},$$
$$C = \begin{pmatrix} 1 & 2 & -1 \\ 1 & 1 & 1 \\ 2 & 1 & -1 \end{pmatrix}, \quad D = \begin{pmatrix} 1 & 2 & -1 \\ -3 & -1 & 3 \\ 2 & 1 & -1 \end{pmatrix}.$$

En cada inciso, encuentre una matriz elemental E que satisfaga la ecuación dada.

(a) $EA = B$ (b) $EB = A$ (c) $EA = C$
(d) $EC = A$ (e) $EC = D$ (f) $ED = C$

15. 1.30. En los siguientes incisos, encuentre la inversa de la matriz elemental dada.

(a) $\begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}$ (b) $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ (c) $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ (d) $\begin{pmatrix} 1 & 0 \\ -\frac{1}{2} & 1 \end{pmatrix}$

(e) $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, c \neq 0$(f) $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ (g) $\begin{pmatrix} 1 & 0 & 0 \\ 0 & c & 0 \\ 0 & 0 & 1 \end{pmatrix}, c \neq 0$

15. 1.31. Para cada una de las siguientes matrices A, encuentre una secesión de matrices elementales $E_1, E_2, \ldots, E_s$ tal que $E_1E_2 \cdots E_sA = I_{2\times 2}$; use esta sucesión para escribir A y A^{-1} como producto de matrices elementales.

(a) $A = \begin{pmatrix} 1 & 0 \\ -1 & -2 \end{pmatrix}$ (b) $A = \begin{pmatrix} 2 & 4 \\ 1 & 1 \end{pmatrix}$

(c) $A = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 2 & 0 \\ 0 & 1 & 3 \end{pmatrix}$ (d) $A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 3 & 4 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 4 & 5 \end{pmatrix}$

15.1.32. Sea

$$A = \begin{pmatrix} a_{11} & 0 & 0 & \cdots & 0 \\ 0 & a_{22} & 0 & \cdots & 0 \\ 0 & 0 & a_{33} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & a_{nn} \end{pmatrix} \in M_{n\times n}(\mathbb{R}).$$

Demuestre que A es invertible si y sólo si $a_{ii} \neq 0$, para $i = 1, \ldots, n$. Si A es invertible calcule A^{-1}.

15.1.33. Sean A y B matrices equivalentes. Demuestre que A es invertible si y sólo si B es invertible.

15.1.34. Pruebe que una matriz en $M_{n\times n}(\mathbb{R})$ no tiene inversa si

(*a*) tiene dos renglones iguales;
(*b*) tiene dos columnas iguales.

15.1.35. Sea $A \in M_{n\times n}(\mathbb{R})$ una matrix invertible. Describa los cambios que ocurren en A^{-1} si en la matriz A

(1) se intercambian dos de sus renglones;
(2) se multiplica uno de sus renglones por el número real $\alpha \neq 0$;
(3) al renglón i se le suma α veces el renglón j.

15.1.36. Para cada una de las siguientes matrices calcular su inversa, si ésta existe.

a) $\begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix}$ *b*) $\begin{pmatrix} 3 & 2 \\ 6 & 4 \end{pmatrix}$ *c*) $\begin{pmatrix} 1 & 2 & 1 \\ -1 & 1 & 2 \\ 1 & 0 & 1 \end{pmatrix}$

d) $\begin{pmatrix} 0 & -2 & 4 \\ 1 & 1 & -1 \\ 2 & 4 & -5 \end{pmatrix}$ *e*) $\begin{pmatrix} 1 & 2 & 8 \\ 0 & 6 & 9 \\ 0 & 2 & 3 \end{pmatrix}$ *f*) $\begin{pmatrix} -\frac{1}{3} & -\frac{7}{3} & 2 \\ 1 & -2 & 1 \\ -\frac{1}{3} & \frac{5}{3} & -1 \end{pmatrix}$

g) $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 10 & 20 & -1 & 0 \\ 5 & -8 & 0 & -1 \end{pmatrix}$ *h*) $\begin{pmatrix} 2 & 3 & 1 & 2 \\ 1 & 1 & 1 & -1 \\ 1 & 2 & 2 & 4 \\ 1 & 0 & -2 & -6 \end{pmatrix}$ *i*) $\begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & -1 & 2 \\ 2 & 0 & 1 & 0 \\ 0 & 1 & -1 & -3 \end{pmatrix}$

j) $\begin{pmatrix} 1 & 0 & 0 & -1 \\ -1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 2 \\ -2 & 2 & -1 & 1 \end{pmatrix}$ *k*) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$ *l*) $\begin{pmatrix} -1 & 2 & 0 & 3 & 1 \\ 1 & 0 & 3 & -2 & 2 \\ 2 & 0 & 0 & -4 & -2 \\ 0 & 1 & 0 & 2 & -3 \\ 0 & -1 & 2 & 1 & 1 \end{pmatrix}$

15.1.37. Sea

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2\times 2}(\mathbb{R}).$$

Demostrar, usando operaciones elementales de renglón, que A es invertible si y sólo si $ad - bc \neq 0$.

15.1.38. Sea

$$A = \begin{pmatrix} a & b \\ c & 0 \end{pmatrix} \in M_{2\times 2}(\mathbb{R}).$$

Encontrar todos los posibles valores de a, b y c tales que A es invertible y $A^{-1} = A$.

15.1.39. Para cada una de las siguientes matrices A, encontrar una matriz P tal que $P \cdot A$ es una matriz escalonada:

(a) $A = \begin{pmatrix} \frac{1}{2} & -2 & 0 \\ 1 & 3 & 2 \\ 6 & 12 & -1 \end{pmatrix}$, (b) $A = \begin{pmatrix} 1 & -1 & 1 & -2 \\ 0 & 3 & 3 & 1 \\ 3 & 0 & 0 & 5 \end{pmatrix}$, (c) $A = \begin{pmatrix} 1 & 2 & 2 & 2 \\ 1 & 2 & 2 & 2 \\ 1 & 2 & 2 & 2 \end{pmatrix}$,

(d) $A = \begin{pmatrix} -2 & -1 & -4 \\ -1 & 1 & 3 \\ 3 & 1 & 5 \end{pmatrix}$ (e) $A = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$.

15.1.40. Encuentre matrices $P, Q \in M_{3\times 3}(\mathbb{R})$ que satisfagan la identidad:

$$P \cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & -2 & 1 \\ 3 & 0 & 4 \end{pmatrix} \cdot Q = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

15.1.41. Hallar todos los inversos

(1) izquierdos de la matriz

$$A = \begin{pmatrix} 1 & -1 \\ 1 & 2 \\ 0 & 1 \end{pmatrix};$$

(2) derechos de la matriz

$$B = \begin{pmatrix} 1 & -1 & 1 \\ 1 & 1 & 2 \end{pmatrix}.$$

§§ Ejercicios sección 15.2.

15.2.1. Demuestre que $L_{I\times I} = 1_{\mathbb{R}^n}$ y $M_(1_{\mathbb{R}^n}) = I_{n\times n}$.

15.2.2. Determine cuáles de las siguientes funciones son transformaciones lineales y estudiar para las que lo sean su inyectividad y suprayectividad.

(1) $T : \mathbb{R}^2 \longrightarrow \mathbb{R}$; $T(x, y) = 2x - y$.
(2) $T : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$; $T(x, y) = (xy, x + y)$.
(3) $T : \mathbb{R}^2 \longrightarrow \mathbb{R}^3$; $T(x, y) = (2x - 3y, x + 4, 5x)$.
(4) $T : \mathbb{R}^3 \longrightarrow \mathbb{R}^2$; $T(x, y, z) = (2x + 3y - 4z, x + 2y + z)$.
(5) $T : \mathbb{R}^2 \longrightarrow \mathbb{R}^3$; $T(x, y) = (x + y, 0)$.
(6) $T : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$; $T(x, y, z) = (-x, y, -z)$.

15.2.3. Considere la transformación lineal $T : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ definida por

$$T(x, y, z) = (2x + y, -z, 0).$$

(1) ¿Pertenece $(6, -2, 0)$ a $N(T)$?
(2) Determinar $N(T)$ y hallar una base de dicho subespacio.
(3) Hallar $\dim_{\mathbb{R}} Im(T)$.

15.2.4. ¿Existe una transformación lineal $T : \mathbb{R}^3 \longrightarrow \mathbb{R}^2$ tal que:

$$T(1, 0, 0) = (1, 1), \quad T(0, 1, 0) = (1, -1),$$
$$T(1, 0, 0) = (1, 0), \quad T(-1, 1, 2) = (-2, 2)?$$

15. 2.5. Encuentre una transformación lineal $T : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ tal que $N(T) = \{(x, y, z) \in \mathbb{R}^3 \mid 2x - y + z = 0\}$.

15.2.6. Determinar una transformación lineal $T : \mathbb{R}^4 \longrightarrow \mathbb{R}^3$ cuya imagen esté generada por los vectores $(2, 0, 1)$ y $(-1, 3, 1)$.

15. 2.7. Sea $\{v_1, v_2\}$ una base de $\mathbb{R}^2$. Se consideran las transformaciones lineales $T, G : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ tales que:

$$T(v_1) = v_1 + 2v_2, \qquad T(v_2) = T(v_1);$$
$$G(v_1) = -2v_1 + 2v_2, \qquad G(v_2) = v_1 - v_2.$$

Demostrar que $f \circ g = g \circ f$.

15.2.8. Considere las siguientes transformaciones lineales.

(1) $T : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$; $T(x, y) = (y, x)$.
(2) $T : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$; $T(x, y) = (x - 2y, -x + y)$.
(3) $T : \mathbb{R}^2 \longrightarrow \mathbb{R}^3$; $T(x, y) = (x + y, x - y, 2x + 3y)$.
(4) $T : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$; $T(x, y, z) = (-x + 2y + z, 2x - 4y - 2z, -3x + 6y + 3z)$.
(5) $T : \mathbb{R}^4 \longrightarrow \mathbb{R}^2$; $T(x, y, z, w) = (w - x, -y + 2z)$.

En cada caso, encuentre $M(T)$, $N(T)$, $Im(T)$, $\dim_{\mathbb{R}} N(T)$ y $\dim_{\mathbb{R}} Im(T)$.

15.2.9. Sean $T, G : \mathbb{R}^3 \longrightarrow \mathbb{R}^4$ transformaciones lineales definidas por

$$T(x, y, z) = (x, -y, z, x + y + z), \qquad G(x, y, z) = (-x, y, 2z, -x - y + z).$$

(1) Encuentre: $M(T)$, $M(G)$ y $M(T+G)$.
(2) Determinar $N(T)$ y $N(G)$.
¿Es cierto que $N(T)+N(G)=N(T+G)$?

15.2.10. Considérese las siguientes transformaciones lineales $T:\mathbb{R}^3\longrightarrow\mathbb{R}^2$ y $G:\mathbb{R}^2\longrightarrow\mathbb{R}^3$ definidas por

$$T(x,y,z)=(x-y+z,-2x+2y-2z),$$
$$G(x,y,z)=(2x+3y,-5x-4y,-6x-9y).$$

Encuentre: $M(G\circ T)$ y $M(T\circ G)$.

§§ Ejercicios sección 15.3.

15.3.1. Sean A_1, A_2, ..., A_n, matrices invertibles de $n\times n$. Demuestre que $A_1\cdot A_2\cdots A_n$ es una matriz invertible.

15.3.2. Demuestre que si $A\in M_{m\times n}(\mathbb{R})$ y $B\in M_{n\times n}(\mathbb{R})$ con B invertible. Demuestre que $rango(A\cdot B)=rango(A)$.

15.3.3. Demostrar que si $A,B\in M_{m\times n}$ y $\alpha\in\mathbb{R}$, entonces $(A+B)^t=A^t+B^t$ y $(\alpha\cdot A)^t=\alpha\cdot A^t$.

15.3.4. Demostrar que para cualquier matriz A en $M_{m\times n}(\mathbb{R})$, $rango(A)=0$ si y sólo si A es la matriz cero.

15.3.5. Sea $A\in M_{m\times n}(\mathbb{R})$. Demostrar que, para cualquier número real $c\in\mathbb{R}$; si $c\neq 0$, entonces $rango(c\cdot A)=rango(A)$.

15.3.6. Utilizando el método para escalonar matrices, encuentra el rango de las siguientes matrices

$$A=\begin{pmatrix}1&-1&2&0\\2&-1&-3&1\\0&1&-1&1\\1&0&-1&1\\1&2&1&3\end{pmatrix}\quad B=\begin{pmatrix}1&-1&-1&0\\2&-1&1&0\\3&-2&1&-1\\1&1&5&0\\2&1&7&0\end{pmatrix}$$

$$C=\begin{pmatrix}1&1&1&3\\1&1&-3&-1\\2&1&3&1\\1&2&-2&1\end{pmatrix}\quad D=\begin{pmatrix}1&1&1&-2&-2&5\\2&-1&0&-1&-2&0\\2&0&-1&-2&-1&0\\0&1&-1&-1&1&0\end{pmatrix},$$

$$E = \begin{pmatrix} 2 & 1 & -1 & 1 & 3 \\ 1 & 2 & 1 & -1 & 3 \\ 1 & 0 & -1 & 1 & 0 \\ 0 & 1 & 1 & -1 & 0 \\ 3 & 1 & -2 & 2 & 4 \\ 1 & 3 & 2 & -2 & 4 \end{pmatrix}, \quad F = \begin{pmatrix} 1 & -1 & 1 & 1 & 2 & -1 \\ -1 & 1 & 1 & 1 & -4 & 3 \\ -1 & -1 & 1 & 1 & -2 & 3 \\ 1 & -2 & 1 & 2 & 3 & -1 \\ 0 & -4 & 1 & 5 & 3 & 1 \end{pmatrix}$$

§§ Ejercicios sección 15.4.

15.4.1. Considere el sistema de ecuaciones lineales

$$\left\{ \begin{array}{ccccccc} a_{11}x_1 & + & \dots & + & a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + & \dots & + & a_{2n}x_n & = & b_2 \\ \vdots & & \vdots\vdots & & \vdots & & \vdots \\ a_{m1}x_1 & + & \dots & + & a_{mn}x_n & = & b_m \end{array} \right. .$$

Sea A la matriz de coeficientes y A' la matriz aumentada del sistema. Demuestre que

(1) Si $rango(A) = rango(A') = n$, entonces el sistema tiene una única solución.
(2) Si $rango(A) = rango(A') = r < n$, entonces el sistema tiene una infinidad de soluciones.

15.4.2. Sin resolver el sistema de ecuaciones lineales, determine si cada uno de los siguientes sistemas tiene

(*i*) una solución única,
(*ii*) un número infinito de soluciones o
(*iii*) ninguna solución.

$$1)\begin{cases} 2x_1 + x_2 - x_3 - 5x_4 = -6 \\ x_1 - x_2 + x_3 + 2x_4 = 0 \\ x_1 - 2x_2 + x_3 + 4x_4 = -1 \\ x_1 + x_2 + 2x_3 - x_4 = 5 \end{cases}$$

$$2)\begin{cases} x_1 + x_2 + x_3 + x_4 = 10 \\ 2x_1 + 3x_2 - x_4 = 4 \\ x_1 + x_2 - x_3 - x_4 = -4 \\ 2x_1 - x_2 + x_3 - x_4 = 2 \\ x_1 + 2x_2 - x_3 - 2x_4 = -6 \end{cases}$$

$$3)\begin{cases} 2x_1 + x_2 - x_3 + x_4 = 3 \\ -x_1 + x_3 - x_4 = 0 \\ 3x_1 + 2x_2 - x_3 + x_4 = 4 \\ x_1 + 2x_2 + x_3 - x_4 = 3 \\ 3x_1 + x_2 - 2x_3 + 2x_4 = 4 \\ x_1 + 3x_2 + 2x_3 - 2x_4 = 4 \end{cases}$$

$$4)\begin{cases} x_1 + x_2 + 3x_3 - 2x_4 - x_5 = 1 \\ 5x_1 - 2x_2 + 3x_3 + 7x_4 + 8x_5 = 3 \\ -3x_1 - x_2 + 2x_3 + 7x_4 + 5x_5 = 2 \\ 5x_1 + 3x_2 + x_3 - 2x_4 - x_5 = 3 \end{cases}$$

§§ Ejercicios sección 15.5.

15.5.1. Demuestre el corolario 15.5.19.

15.5.2. Sea $A = \begin{pmatrix} a & a \\ 4 & 2a \end{pmatrix} \in M_{2\times 2}(\mathbb{R})$. Encuentre todos los valores de a tales que $\det(A) = 0$.

15.5.3. Sean $a, b \in \mathbb{R}$; calcule: $\begin{vmatrix} \sin(a) & \cos(a) \\ \sin(b) & \cos(b) \end{vmatrix}$ y $\begin{vmatrix} \cos(a) & \sin(a) \\ \sin(b) & \cos(b) \end{vmatrix}$.

15.5.4. Demuestra que si $(a_1, b_1, c_1) = (a_1', b_1', c_1') + (a_1'', b_1'', c_1'') + (a_1''', b_1''', c_1''')$, entonces

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} = \begin{vmatrix} a_1' & b_1' & c_1' \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} + \begin{vmatrix} a_1'' & b_1'' & c_1'' \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} + \begin{vmatrix} a_1''' & b_1''' & c_1''' \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}$$

15.5.5. Sea $A = \left(a_{ij}\right) \in M_{n\times n}(\mathbb{R})$ una matriz triangular inferior. Demuestre que $\det(A) = a_{11} \cdot a_{22} \cdot \ldots \cdot a_{nn}$.

15.5.6. Sea $A \in M_{n\times n}(\mathbb{R})$ y $c \in \mathbb{R}$. Demostrar que $\det(c \cdot A) = c^n \cdot \det(A)$.

15.5.7. Demuestre que, en general, no se cumple que

$$\det(A + B) = \det(A) + \det(B).$$

15.5.8. Utilice las propiedades de los determinantes para encontrar el determinante de las siguientes matrices.

$$A = \begin{pmatrix} a & b & c \\ d & e & f \\ a & b & c \end{pmatrix}, \quad B = \begin{pmatrix} 1 & a & b+c \\ 1 & b & a+c \\ 1 & c & b+c \end{pmatrix},$$
$$C = \begin{pmatrix} a & d & e \\ 0 & b & f \\ 0 & 0 & c \end{pmatrix}, \quad D = \begin{pmatrix} a & 0 & b \\ c & 0 & d \\ e & 0 & f \end{pmatrix},$$
$$E = \begin{pmatrix} 0 & 0 & 3 \\ 0 & 2 & 1 \\ 1 & 4 & 3 \end{pmatrix}, \quad F = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

15.5.9. Mediante operaciones elementales (sobre renglones o columnas) reduzca el cálculo de los siguientes determinantes a un determinante de una matriz triangular superior y encuentre su valor.

1) $\begin{vmatrix} 1 & 5 & -6 \\ -1 & -4 & 4 \\ -2 & -7 & 9 \end{vmatrix}$

2) $\begin{vmatrix} 1 & 5 & -3 \\ 3 & -3 & 3 \\ 2 & 13 & -7 \end{vmatrix}$

3) $\begin{vmatrix} 1 & 3 & 0 & 2 \\ -2 & -5 & 7 & 4 \\ 3 & 5 & 2 & 1 \\ 1 & -1 & 2 & -3 \end{vmatrix}$

4) $\begin{vmatrix} 1 & 3 & 3 & -4 \\ 0 & 1 & 2 & -5 \\ 2 & 5 & 4 & -3 \\ -3 & -7 & -5 & 2 \end{vmatrix}$

5) $\begin{vmatrix} 1 & -1 & -3 & 0 \\ 0 & 1 & 5 & 4 \\ -1 & 2 & 8 & 5 \\ 3 & -1 & -2 & 3 \end{vmatrix}$

6) $\begin{vmatrix} 1 & 0 & 0 & 2 & -2 \\ 0 & 2 & -4 & -1 & -6 \\ -2 & -6 & 2 & 3 & 9 \\ 3 & 7 & -3 & 8 & -7 \\ 3 & 5 & 5 & 2 & 7 \end{vmatrix}$

15.5.10. Sean $a, b, c, d, e, f, g, h, i \in \mathbb{R}$. Si $\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = 5$, evalúe

1) $\begin{vmatrix} 3a & b & c \\ 3g & h & i \\ 3d & e & f \end{vmatrix}$ 2) $\begin{vmatrix} 3a & b & 2c \\ 9d & 3e & 6f \\ 3g & h & 2i \end{vmatrix}$ 3) $\begin{vmatrix} 2c & 2b & 2a \\ 3f & 3e & 3d \\ 5i & 5h & 5g \end{vmatrix}$

4) $\begin{vmatrix} a & b & c \\ d-a & e-b & f-c \\ 3g & 3h & 3i \end{vmatrix}$ 5) $\begin{vmatrix} c & b & -a \\ f & e & -d \\ i & h & -g \end{vmatrix}$ 6) $\begin{vmatrix} -1 & d & e & i \\ 0 & a & b & c \\ 0 & d & e & f \\ 0 & g & h & i \end{vmatrix}$

7) $\begin{vmatrix} a & b & c \\ 2d+3a & 2e+3b & 2f+3c \\ -i & -h & -g \end{vmatrix}$

15. 5.11. Calcule $\det \begin{pmatrix} 5 & -1 & 2 \\ 3 & 2 & 4 \\ -1 & 2 & -2 \end{pmatrix}$ usando la expansión por cofactores a través

(a) del renglón 1 (b) de la columna 2
(c) del renglón 3 (c) de la columna 1

15.5.12. Calcule los siguientes determinantes usando la expansión por cofactores a través de cualquier renglón o columna que parezca conveniente.

1) $\begin{vmatrix} 5 & 5 & 2 \\ -1 & 1 & 2 \\ 3 & 0 & 0 \end{vmatrix}$ 2) $\begin{vmatrix} 1 & 2 & 3 \\ -4 & 0 & 4 \\ -3 & -2 & 1 \end{vmatrix}$ 3) $\begin{vmatrix} 0 & a & 0 \\ b & c & d \\ 0 & e & 0 \end{vmatrix}$

4) $\begin{vmatrix} 1 & -1 & 0 & 3 \\ 2 & 5 & 2 & 6 \\ 0 & 1 & 0 & 0 \\ 1 & 4 & 2 & 1 \end{vmatrix}$ 5) $\begin{vmatrix} 3 & -2 & 0 & 1 \\ 1 & 3 & 0 & -1 \\ 0 & 2 & 2 & 4 \\ 3 & 1 & 0 & 0 \end{vmatrix}$

15.5.13. Considere el determinante

$$\det \begin{pmatrix} 1 & 0 & 4 & -1 \\ 3 & 0 & 2 & 1 \\ x & a & y & z \\ 3 & 0 & 2 & 8 \end{pmatrix}$$

(a) ¿Cuánto vale este determinate si $a = 0$?
(b) ¿Cuánto vale si $a \neq 0$?
(c) ¿Por qué el valor de este determinante no depende de x, y, z?

15.5.14. Sean $a \in \mathbb{R}$. Calcule $\begin{vmatrix} a-6 & 0 & 0 & -8 \\ 5 & a-4 & 0 & 12 \\ -1 & 3 & a-2 & -6 \\ 0 & -\frac{1}{2} & 1 & 1 \end{vmatrix}$.

15.5.15. Sea $A = \begin{pmatrix} 1 & a & 0 \\ a & 1 & 1 \\ -1 & a & -1 \end{pmatrix}$ en $M_{3\times3}(\mathbb{R})$. Encuentre todos los valores de a para los cuales la matriz A no es invertible.

15.5.16. Obtén el valor de $b \in \mathbb{R}$, para que $\begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & b & 1 \\ 1 & b & 1 & 1 \\ b & 1 & 1 & 1 \end{vmatrix} = -27$.

15.5.17. Probar que si $a, b \in \mathbb{Z}$, entonces el determinante $\begin{vmatrix} a & 2a & 3b \\ a & 2a & 0 \\ 2a & 0 & a \end{vmatrix}$ es un múltiplo de 16.

15.5.18. Encuentre $a, b, c \in \mathbb{N}$ para los cuales $\begin{vmatrix} a+b & c & c \\ a & b+c & a \\ b & b & a+c \end{vmatrix} = 4$.

15.5.19. Sean

$$A = \begin{pmatrix} 1 & -2 & 3 \\ -2 & 3 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 2 \\ 3 & -2 & 5 \\ 2 & 1 & 3 \end{pmatrix}.$$

Calcule $\det\left(A^2BA^{-1}\right)$ y $\det\left(B^tA^3\right)$.

15.5.20. Sea $\delta : M_{n\times n}(\mathbb{R}) \longrightarrow \mathbb{R}$ tal que

(1) $\delta(A \cdot B) = \delta(A) \cdot \delta(B)$ para $A, B \in M_{n\times n}(\mathbb{R})$.
(2) Si $A = \left(a_{ij}\right) \in M_{n\times n}(\mathbb{R})$ una matriz triangular superior, entonces

$$\det(A) = a_{11}a_{22} \cdot \ldots \cdot a_{nn}.$$

Demuestre que δ es un determinante.

Adjunta de una matriz

15.5.21. Usar la adjunta para encontrar la inversa, si existe, de cada una de las siguientes matrices.

1) $\begin{pmatrix} 0 & -2 & -1 \\ 3 & 0 & 0 \\ -1 & 1 & 1 \end{pmatrix}$ 2) $\begin{pmatrix} 1 & 1 & 3 \\ 2 & -2 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ 3) $\begin{pmatrix} 3 & 5 & 4 \\ 1 & 0 & 1 \\ 2 & 1 & 1 \end{pmatrix}$

4) $\begin{pmatrix} 3 & 6 & 7 \\ 0 & 2 & 1 \\ 2 & 3 & 4 \end{pmatrix}$ 5) $\begin{pmatrix} 3 & 0 & 0 \\ -1 & 1 & 0 \\ -2 & 3 & 2 \end{pmatrix}$ 6) $\begin{pmatrix} 1 & 2 & 4 \\ 0 & -3 & 1 \\ 0 & 0 & 3 \end{pmatrix}$

15.5.22. Sea $A \in M_{n\times n}(\mathbb{R})$ una matriz no invertible. Pruebe que $A \cdot A^a$ es la matriz cero.

15.5.23. Sea A una matriz cuadrada de orden $n \times n$. Si todas las entradas de la matriz A son números enteros y $\det(A) = 1$, explique por qué todas las entradas de A^{-1} son enteros.

15.5.24. Sea $A \in M_{n\times n}(\mathbb{R})$ una matriz triangular superior invertible. Pruebe que A^a es triangular superior y por lo tanto A^{-1} es triangular superior. Demostrar que resultados semejantes son ciertos si A es triangular inferior.

15.5.25. Sea $A \in M_{n\times n}(\mathbb{R})$. Demostrar $\left(A^t\right)^a = (A^a)^t$.

15.5.26.

(1) Demuestre que si el determinate de la matriz A de orden $n \times n$, con $n \geq 2$, es distinto de cero, entonces $\det(A^a) = (\det(A))^{n-1}$.
(2) Compruebe que si A es una matriz invertible, su matriz adjunta es también invertible. ¿Es válida la afirmación recíproca?

15.5.27. Sea $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2\times 2}(\mathbb{R})$. Demuestre que $(A^a)^a = A$.

15.5.28. Sea $A \in M_{n\times n}(\mathbb{R})$ con $n \geq 2$. Pruebe que si $\det(A) \neq 0$, entonces $(A^a)^a = (\det(A))^{n-2} A$.

15.5.29. Sea $A, B \in M_{n\times n}(\mathbb{R})$ matrices invertibles. Demuestre que $(A \cdot B)^a = B^a \cdot A^a$. (Esta igualdad también es válida para matrices no invertibles.)

Regla de Cramer

15.5.30. Aplique la regla de Cramer para resolver los siguientes sistemas de ecuaciones lineales.

1) $\begin{cases} x + 2y + 3z = 1 \\ y + 4z = 1 \\ z = 1 \end{cases}$ 2) $\begin{cases} x + y - z = 2 \\ x - y + z = 3 \\ -x + y + z = 4 \end{cases}$

3) $\begin{cases} 4x - 3y + 3z = 8 \\ x + 3y + z = 7 \\ 3x - y + 2z = 1 \end{cases}$

4) $\begin{cases} x - 3y - 2w = 0 \\ x - 3y + z + w = 0 \\ -3y + w = 0 \end{cases}$

5) $\begin{cases} 2x_1 + 3x_3 - 5x_4 = 12 \\ -2x_2 + x_3 + 3x_4 = 4 \\ 3x_1 - 5x_2 + 4x_3 = 5 \\ x_1 - 3x_2 - 4x_4 = -54 \end{cases}$

6) $\begin{cases} x_1 + x_2 + x_3 + x_4 + x_5 = 0 \\ x_2 + x_3 + x_4 + x_5 = 2 \\ x_3 + x_4 + x_5 = 3 \\ x_4 + x_5 = 3 \\ x_5 = 2 \end{cases}$

15.5.31. Considere el sistema de ecuaciones lineales

$$\begin{cases} x + ay + a^2z = a^2 \\ x + by + b^2z = b^2 \\ x + cy + c^2z = c^2 \end{cases},$$

donde a, b y c son constantes cualesquiera de $\mathbb{R}$.

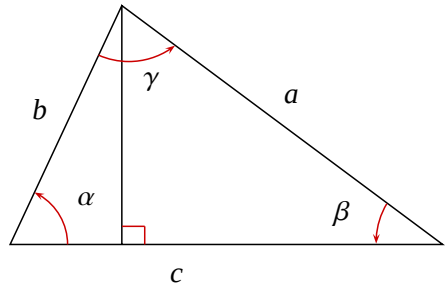
(1) Muestre que

$$\begin{vmatrix} 1 & a & a^2 \\ 1 & b & b^2 \\ 1 & c & c^2 \end{vmatrix} = (b-a)(c-a)(c-b).$$

(2) Pruebe que el sistema dado tiene solución única si y sólo si a, b y c son todas distintas.

(3) Para el caso en que el sistema tiene solución única, use la regla de Cramer para calcular dicha solución.

15.5.32. Considere el triángulo en la siguiente figura



(1) Demuestre, utilizando la trigonometría elemental, que

$$\begin{cases} b\cos(\alpha) + a\cos(\beta) = c \\ c\cos(\alpha) + a\cos(\gamma) = b \\ c\cos(\beta) + c\cos(\gamma) = a \end{cases}$$

(2) Si se piensa que el sistema del inciso (1) es un sistema lineal de tres ecuaciones con tres incógnitas, $\cos(\alpha)$, $\cos(\beta)$ y $\cos(\gamma)$, demuestre que el determinante de la matriz de coeficientes del sistema es diferente de cero.

(3) Utilice la regla de Cramer para despejar $\cos(\gamma)$.

(4) Utilice el inciso (3) para probar *la ley de cosenos*: $c^2 = a^2+b^2-2ab\cos(\gamma)$.

Bibliografía

[1] Cárdenas, H., Lluis, E., Raggi, F., Tomás, F., *Algebra Superior*, Segunda Edición, Trillas, México, 1999.

[2] Dummit, D. S., Foote, R. M., *Abstract Algebra*, Second Edition, John Wiley & Sons Inc., Nueva Jersey, 1999.

[3] Ebbinghaus, H-D., Hermes, H., Hirzebruch, F., Koecher, M., Mainzer, K., Neukirch, J., Prestel, A., Remmert, R., *Numbers*, Springer-Verlag, New York, 1991.

[4] Friedberg, S. H., Insel, A. J., Spence, L. E., *Linear Algebra*, Second Edition, Prentice-Hall, New Jersey, 2002.

[5] Hoffmann, K., Kunze, R.; *Linear Algebra*, Second Edition; Prentice-Hall, New Jersey, 1971.

[6] Gómez, C. H., *Introducción a la teoría intuitiva de conjuntos (Cardinales y ordinales)*, Segunda Edición, Las prensas de ciencias, México, 2012.

[7] Marsden, J. E., Hoffman, M. J., *Basic Complex Analysis*, Third Edition, W. H. Freeman, New York, 1999.

[8] Niven, I., Zuckerman, H. S., Montgomery, H, L., *An Introduction to the Theory of Numbers*, John Wiley & Sons, Inc., New York, 1991.

[9] Rudin, W., *Principles of Mathematical Analysis*, Third Edition, McGraw-Hill, Inc., New York, 1976.

[10] Stewart, I., Tall, D. *The Foundations of Mathematics*, Third Edition, Oxford university press, New York, 1977.

[11] Strichartz R. S., *The way of analysis*, revised edition, , Jones and Bartlett Publishers, Inc, U.S.A. 2000.

Índice de figuras

Índice analítico