ÁLGEBRA I

26 de mayo de 2021

Índice

Índice de figuras

1. LÓGICA Y CONJUNTOS

1.1. Proposiciones

Definición 1.1
Una proposición es una oración declarativa susceptible de ser considerada verdadera o falsa. La veracidad o falsedad de una proposición se denomina el valor de verdad de la proposición. Denotaremos el valor de verdad con V (verdadero) y F (falso).

Ejemplo 1.1

(a) Los triángulos tienen cuatro vértices.

F, pues los triángulos tienen tres vértices.

(b) $1 + 1 = 2$.

V, pues eso aprendimos en la escuela primaria.

(c) Horacio Quiroga escribió el libro "Cuentos de amor de locura y de muerte".

V, Horacio Quiroga escribió 18 relatos que fueron publicados en 1917.

(d) La edad del universo supera los 14000 millones de años.

Esta proposición tiene un valor de verdad, el problema es que no sabemos cuál es.

Frases imperativas, interrogativas y exclamativas no son proposiciones, puesto que no pueden ser consideradas verdaderas o falsas.

Ejemplo 1.2

(a) Oprima la tecla ENTER.

Frase imperativa.

(b) ¿Está lloviendo?

Frase interrogativa.

(c) ¡Viva la Patria!

Frase exclamativa.

Generalmente las proposiciones son denotadas con letras minúsculas, como por ejemplo: p, q, r, etc. Además diversas proposiciones pueden modificarse o combinarse para dar lugar a nuevas proposiciones.

Ejemplo 1.3
Consideremos las proposiciones

p : "los perros tienen 4 patas"
q : "el pizarrón es verde"

Podemos citar varias combinaciones que se muestran a continuación. El texto recuadrado con ■ es una palabra importante en la modificación y el texto recuadrado con ■ es un agregado para que la frase quede bien expresada en nuestro lenguaje.

(a) Los perros no tienen 4 patas.

(b) Los perros tienen 4 patas y el pizarrón es verde.

(c) Los perros tienen 4 patas o el pizarrón es verde.

(d) Si los perros tienen 4 patas , entonces el pizarrón es verde.

(e) Decir que los perros tienen 4 patas equivale a decir que el pizarrón es verde.

Algunas proposiciones del Ejemplo 1.3 nos resultan usuales (lingüísticamente hablando) y otras no.

La forma de combinar proposiciones se realiza a través de conectivos lógicos que explicaremos a continuación.

1.2. Conectivos lógicos

Un conectivo lógico es una operación para construir nuevas proposiciones a partir de proposiciones más simples.

1.2.1. Negación

La negación aparece en el lenguaje coloquial cuando se desea decir lo contrario de una sentencia declarativa. Consideremos la siguiente proposición:

$$p : \text{“Hoy es lunes”}$$

Si uno quisiera decir lo contrario diría: “Hoy no es lunes”. Analicemos las posibilidades:

- Supongamos que hoy es lunes. Luego la proposición p sería verdadera. Por otro lado la negación de la proposición p sería falsa, puesto que estaría diciendo que hoy no es lunes, es decir, diría que es domingo, martes, miércoles, jueves, viernes o sábado.
- Supongamos que hoy no es lunes. Luego proposición p sería falsa. Por otro lado la negación de la proposición p (“Hoy no es lunes”) sería entonces una afirmación verdadera.

De esta manera se define de manera natural el conectivo negación.

Definición 1.2
La negación es un conectivo lógico unitario y cambia el valor de verdad de la proposición original. La negación de p se denota mediante $\neg p$. Se puede confeccionar una tabla de verdad que muestre las diferentes posibilidades:

p	$\neg p$
V	F
F	V

Ejemplo 1.4

(a) p : “los perros tienen 4 patas”
$\neg p$: “los perros no tienen 4 patas”

(b) q : “todos los perros son marrones”
$\neg q$: “al menos un perro no es marrón”

(c) r : “al menos un gato es rojo”
$\neg r$: “ningún gato es rojo”

(d) s : "el pizarrón no es verde"
$\neg s$: "el pizarrón es verde"

Notemos que hay varias formas lingüísticas de expresar una negación. Por ejemplo si p: "todo hombre es honesto", entonces $\neg p$ puede expresarse de las siguientes maneras:

- No todo hombre es honesto.
- No es cierto que todo hombre es honesto.
- Existe al menos un hombre que no es honesto.
- Existe al menos un hombre deshonesto.

1.2.2. Conjunción

La conjunción aparece en el lenguaje coloquial cuando se quieren expresar dos afirmaciones de manera simultánea. Consideremos la siguiente proposición:

$$r : \text{"Juan tiene hambre y sed"}$$

La proposición r puede considerarse como una composición de dos proposiciones más simples, a saber:

$$\underbrace{\text{Juan tiene hambre}}_{p} \ \text{y} \ \underbrace{\text{Juan tiene sed}}_{q}$$

Pueden ocurrir cuatro situaciones:

- Juan tiene hambre y sed (p es V y q es V).
- Juan tiene hambre pero no tiene sed (p es V y q es F).
- Juan no tiene hambre pero sí tiene sed (p es F y q es V).
- Juan no tiene ni hambre ni sed (p es F y q es F).

Debido a esa idea de simultaneidad de la expresión, la manera natural de definir el valor de verdad de la proposición compuesta r sería que fuera verdadera solamente cuando ambas proposiciones simples (p y q) son verdaderas (primer caso), y falsa en los casos restantes (los tres últimos).

Definición 1.3
La conjunción es un operador lógico binario puesto que relaciona dos proposiciones. La conjunción de dos proposiciones p y q es una nueva proposición denotada por $p \wedge q$ que se lee "p y q". Diremos que $p \wedge q$ es verdadera sólo cuando ambas p y q sean verdaderas. Notar que las posibilidades de valores de verdad para $p \wedge q$ serán cuatro. De esta manera la tabla de verdad es:

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

Ejemplo 1.5
(a) $\underbrace{\underbrace{\text{Los perros tienen 4 patas}}_{V} \ \text{y} \ \underbrace{\text{Marte es un planeta.}}_{V}}_{V}$

(b) $\underbrace{\underbrace{1<2}_{V} \text{ y } \underbrace{3<1}_{F}}_{F}$.

(c) $\underbrace{\underbrace{10-1=8}_{F} \text{ y } \underbrace{4:2=2}_{V}}_{F}$.

(d) $\underbrace{\underbrace{4 \text{ es un número impar}}_{F} \text{ y } \underbrace{3 \text{ es divisible por } 2}_{F}}_{F}$.

De la escuela primaria y secundaria se aprendieron los símbolos "<" y ">" para establecer un orden entre los números. Introduciremos una nueva notación para combinar estos símbolos.

Definición 1.4
La expresión $a < b < c$ se define como la proposición compuesta $(a < b) \wedge (b < c)$. Análogamente se define $a > b > c$.

Ejemplo 1.6
(a) $1 < 2 < 3$ es V.

$\underbrace{\underbrace{1<2}_{V} \text{ y } \underbrace{2<3}_{V}}_{V}$.

(b) $2 < 3 < 1$ es F.

$\underbrace{\underbrace{2<3}_{V} \text{ y } \underbrace{3<1}_{F}}_{F}$.

(c) $2 < 1 < 4$ es F.

$\underbrace{\underbrace{2<1}_{F} \text{ y } \underbrace{1<4}_{V}}_{F}$.

1.2.3. Disyunción

La disyunción aparece en el lenguaje coloquial cuando se expresan dos afirmaciones dando a entender que ellas constituyen opciones (no excluyentes). Consideremos la siguiente proposición:

r : "A Pedro le gustan los fideos con tuco o con crema"

La forma en que está expresada la frase da a entender que a Pedro le gustan los fideos ya sea con tuco o con crema. Si ocurriese que a Pedro le gustan los fideos con tuco, tampoco le molestaría comerlos si se los sirvieran con crema. Análogamente, si ocurriese que a Pedro le gustan los fideos con crema, no le molestaría comerlos si el plato tuviera fideos con tuco.

La proposición r puede considerarse como una composición de dos proposiciones más simples, a saber:

$$\underbrace{\text{A Pedro le gustan los fideos con tuco}}_{p} \boxed{\text{o}} \underbrace{\text{a Pedro le gustan los fideos con crema}}_{q}$$

Pueden ocurrir cuatro situaciones:

- A Pedro le gustan los fideos con tuco y con crema (p es V y q es V).
- A Pedro le gustan los fideos con tuco pero no con crema (p es V y q es F).
- A Pedro no le gustan los fideos con tuco, pero sí le gustan con crema (p es F y q es V).
- A Pedro no le gustan los fideos con tuco ni con crema (p es F y q es F).

Debido a esa idea de opciones (no excluyentes) de la expresión, la manera natural de definir el valor de verdad de la proposición compuesta r sería que fuera verdadera cuando alguna de las proposiciones simples (p o q) son verdaderas (los primeros tres casos), y falsa en el último caso.

Definición 1.5
La disyunción (o disyunción inclusiva) es un operador lógico binario puesto que relaciona dos proposiciones. La disyunción de dos proposiciones p y q es una nueva proposición denotada por $p \vee q$ que se lee "p o q". Diremos que $p \vee q$ es falsa sólo cuando p y q sean falsas. Notar que las posibilidades de valores de verdad para $p \vee q$ serán cuatro. De esta manera la tabla de verdad es:

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

Ejemplo 1.7

(a) $\underbrace{\underbrace{\text{Los gatos son felinos}}_{V} \text{ o } \underbrace{2 \text{ es un número primo}}_{V}}_{V}$.

(b) $\underbrace{\underbrace{1 < 2}_{V} \text{ o } \underbrace{3 < 1}_{F}}_{V}$.

(c) $\underbrace{\underbrace{\text{Saturno no es un planeta}}_{F} \text{ o } \underbrace{4 : 2 = 2}_{V}}_{V}$.

(d) $\underbrace{\underbrace{1 \text{ es un número primo}}_{F} \text{ o } \underbrace{5 \text{ es un número par}}_{F}}_{F}$.

Extenderemos los símbolos de desigualdad utilizando la disyunción.

Definición 1.6
La expresión $a \leqslant b$ es definida como la proposición compuesta $(a < b) \vee (a = b)$. Análogamente se define $a \geqslant b$.

Ejemplo 1.8

(a) $1 \leqslant 2$ es V.

$\underbrace{\underbrace{1 < 2}_{V} \text{ o } \underbrace{1 = 2}_{F}}_{V}$.

(b) $2 \leqslant 2$ es V.

$$\underbrace{\underbrace{2 < 2}_{F} \text{ o } \underbrace{2 = 2}_{V}}_{V}.$$

(c) $2 \geqslant 5$ es F.

$$\underbrace{\underbrace{2 > 5}_{F} \text{ o } \underbrace{2 = 5}_{F}}_{F}.$$

1.2.4. Disyunción exclusiva

La disyunción exclusiva aparece en el lenguaje coloquial cuando se expresan dos afirmaciones con la idea de que ellas constituyan opciones, pero que éstas no ocurran de manera simultánea (es decir, excluyentes). Consideremos la siguiente proposición:

r : "A Pedro le gustan los fideos o bien con tuco o bien con crema"

La forma en que está expresada la frase dice que a Pedro le gustan los fideos con tuco, o con crema. Sin embargo, si ocurriese que a Pedro le gustan los fideos con tuco, no soportaría la idea de comerlos con crema. Análogamente, si ocurriese que a Pedro le gustan los fideos con crema, no le agradaría que le sirvieran un plato de fideos con tuco. Esto último es lo que da el sentido excluyente a la expresión.

La proposición r puede considerarse como una composición de dos proposiciones más simples, a saber:

$$\underbrace{\text{A Pedro le gustan los fideos con tuco}}_{p} \boxed{\text{o}} \underbrace{\text{a Pedro le gustan los fideos con crema}}_{q}$$

Como lingüísticamente casi no hay diferencias entre este tipo de expresiones y aquéllas relativas a la disyunción, se agregan partículas tales como "o bien ... o bien ...". Si no puede deducirse del contexto, debe aclararse explícitamente el sentido correcto de lo que se quiere decir.

Pueden ocurrir cuatro situaciones:

- A Pedro le gustan los fideos con tuco y con crema (p es V y q es V).
- A Pedro le gustan los fideos con tuco pero no con crema (p es V y q es F).
- A Pedro no le gustan los fideos con tuco, pero sí le gustan con crema (p es F y q es V).
- A Pedro no le gustan los fideos con tuco ni con crema (p es F y q es F).

Debido a esa idea de opciones excluyentes de la expresión, la manera natural de definir el valor de verdad de la proposición compuesta r sería que fuera verdadera cuando sólo alguna de las proposiciones simples (p o q) son verdaderas (segundo y tercer caso), y falsa en los casos restantes (primero y último caso).

Definición 1.7
La disyunción exclusiva es un operador lógico binario puesto que relaciona dos proposiciones. La disyunción exclusiva de dos proposiciones p y q es una nueva proposición denotada por $p \veebar q$ que se lee "p o q". Notemos que se lee igual que la disyunción inclusiva. Diremos que $p \veebar q$ es verdadera

sólo cuando p y q tengan valores de verdad distintos. Notar que las posibilidades de valores de verdad para $p \veebar q$ serán cuatro. De esta manera la tabla de verdad es:

p	q	$p \veebar q$
V	V	F
V	F	V
F	V	V
F	F	F

Ejemplo 1.9

(a) O $\underbrace{\underbrace{\text{existen mamíferos que viven en el mar}}_{V,\text{ pues las ballenas son mamíferos}} \text{ o } \underbrace{2 \text{ es un número primo}}_{V}}_{F}$.

(b) O bien $\underbrace{\underbrace{\text{existen mamíferos que vuelan}}_{V,\text{ pues los murciélagos son mamíferos}} \text{ o bien } \underbrace{3 < 1}_{F}}_{V}$.

(c) O $\underbrace{\underbrace{2 < 1}_{F} \text{ o } \underbrace{\text{el Río Paraná es un río de Argentina}}_{V}}_{V}$.

(d) O bien $\underbrace{\underbrace{\text{Corrientes no pertenece a Argentina}}_{F} \text{ o bien } \underbrace{4 = 1}_{F}}_{F}$.

Cuando no sea claro del contexto, entenderemos que la disyunción hace referencia a la disyunción inclusiva.

1.2.5. Condicional o implicación

El condicional aparece en el lenguaje coloquial cuando se expresan frases sujetas al cumplimiento de una condición. Consideremos la siguiente proposición:

r : "Si Clara hace la tarea, entonces podrá ir a jugar con sus amigas"

La proposición r puede considerarse como una composición de dos proposiciones más simples, a saber:

$$\text{Si } \underbrace{\text{Clara hace la tarea,}}_{p} \text{ entonces } \underbrace{\text{Clara podrá ir a jugar con sus amigas}}_{q}$$

La forma en que está expresada la frase se parece a una promesa. Si Clara hace la tarea y tiene permiso de jugar con sus amigas, entonces la promesa se ha cumplido. En cambio, si Clara hace la tarea y no le dan permiso de salir a jugar, la promesa se ha roto. Notar que la proposición r no dice nada en el caso que Clara no haga la tarea, y es allí donde deberemos tomar una decisión del valor de verdad que le asignaremos a r.

Veamos otro ejemplo. Supongamos que el Dr. John Watson le da al detective Sherlock Holmes la siguiente pista "el asesino ha dejado huellas en el césped". Luego Holmes enuncia la siguiente proposición condicional:

r : "Si el asesino dejó huellas en el césped, entonces eso significa que el asesino está ahora camino a Londres"

Vamos a analizar las cuatro situaciones que pueden aparecer:

- Si la pista que le dio Watson a Holmes es correcta, su mente brillante habrá realizado un razonamiento deductivo correcto y podrán atrapar al ladrón cuando llegue a Londres.
- Si la pista que le dio Watson a Holmes es correcta, y el asesino no va camino a Londres, entonces la capacidad deductiva de Holmes habrá fallado. Recordar que Holmes tenía problemas con las drogas.
- Si la pista de Watson es errónea (podría ocurrir que las huellas en el césped no sean las del asesino), Holmes podría arribar a la conclusión de que el asesino va camino a Londres aún utilizando argumentos deductivos correctos de su mente brillante.
- Si la pista de Watson es errónea y el ladrón no va camino hacia Londres, no podemos culpar a Holmes de haber deducido algo erróneo a partir de una pista falsa. En este caso, su poder deductivo aún seguiría intacto.

En base a los ejemplos anteriormente presentados, una buena definición del condicional sería la siguiente.

Definición 1.8
El condicional (o implicación) [1] *es un operador lógico binario puesto que relaciona dos proposiciones. La implicación de dos proposiciones p y q es una nueva proposición denotada por $p \Rightarrow q$ que se lee "p implica q" o "si p entonces q".*

La tabla de verdad de la implicación es:

p	q	$p \Rightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

La proposición p se denomina antecedente, y q se denomina consecuente.

Otras denominaciones para $p \Rightarrow q$ son:

- *p implica q.*
- *Si p, entonces q.*
- *q si p.*
- *p sólo si q.*
- *q se sigue de p.*
- *p es condición suficiente para q,*
- *q es condición necesaria para p,*

Ejemplo 1.10
(a) Si $\underbrace{1+1=2}_{V}$ entonces $\underbrace{\text{el Aconcagua tiene más de 6000 metros de altura.}}_{V}$

$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}_{V}$

[1] Si bien el condicional y la implicación son levemente distintos desde el punto de vista conceptual, en este curso los tomaremos como equivalentes

(b) Si $\underbrace{1 < 2}_{V}$ entonces $\underbrace{\text{los pinos no son árboles perennes}}_{F}$.
$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}_{F}$

(c) Si $\underbrace{\text{el ser humano no es un mamífero}}_{F}$ entonces $\underbrace{\text{hay rosas de color rojo}}_{V}$.
$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}_{V}$

(d) Si $\underbrace{2 \text{ es un número impar}}_{F}$ entonces $\underbrace{\text{hay más de una estrella en nuestro sistema solar}}_{F}$.
$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}_{V}$

Notar que si p es V y q es F, entonces $p \Rightarrow q$ es F, lo cual es deseable en toda ciencia deductiva. No puede un razonamiento matemático deducir una proposición falsa de una proposición verdadera. Sin embargo se puede deducir una proposición verdadera o falsa a partir de una proposición falsa. Por ejemplo:

- Si $1 = -1$ (F), elevando al cuadrado ambos miembros, obtenemos $1 = 1$ (V).
- Si $1 = -1$ (F), sumando 1 a cada miembro obtenemos que $2 = 0$ (F).

Sin embargo, jamás probaremos que $3 = 0$ a partir de $1 < 2$.

Definición 1.9
Si tenemos una implicación $p \Rightarrow q$, se suele denominar:

$$\begin{array}{rcll} q & \Rightarrow & p & \textit{recíproca,} \\ \neg p & \Rightarrow & \neg q & \textit{inversa o contraria,} \\ \neg q & \Rightarrow & \neg p & \textit{contrarrecíproca.} \end{array}$$

1.2.6. Bicondicional o doble implicación

El bicondicional aparece en el lenguaje coloquial cuando se quiere resaltar la equivalencia de dos afirmaciones. Consideremos la siguiente proposición:

$$r : \text{“Juan usa paraguas si y sólo si llueve”}$$

La frase “si y sólo si” es muy común en el ambiente de la matemática como veremos más adelante en este curso.

La proposición r puede considerarse como una composición de dos proposiciones más simples, a saber:

$$\underbrace{\text{Juan usa paraguas}}_{p} \boxed{\text{si y sólo si}} \underbrace{\text{llueve}}_{q}$$

La proposición r nos dice dos cosas:

- Si Juan usa paraguas entonces llueve $(p \Rightarrow q)$, y
- si llueve entonces Juan usa paraguas $(q \Rightarrow p)$.

Es decir, la frase puede ser considerada como una conjunción de dos implicaciones.

Definición 1.10
La doble implicación es un operador lógico binario puesto que relaciona dos proposiciones. La doble implicación entre dos proposiciones p y q es una nueva proposición denotada por $p \Leftrightarrow q$ que se lee "p si y sólo si q". La doble implicación está definida como la proposición compuesta

$$(p \Rightarrow q) \wedge (q \Rightarrow p)\,.$$

Por lo tanto, la tabla de verdad de la doble implicación es [2]*:*

p	q	$p \Leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

Notar que la doble implicación de dos proposiciones es verdadera sólo cuando ambas proposiciones tienen el mismo valor de verdad. Por ello la doble implicación también puede ser considerada como una equivalencia.

Ejemplo 1.11

(a) Que a $\underbrace{\text{los ratones les guste el queso}}_{V}$ equivale a que a $\underbrace{\text{los conejos les gusten las zanahorias}}_{V}$.
$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}_{V}$

(b) $\underbrace{1+1=2}_{V}$ si y sólo si $\underbrace{1=0}_{F}$.
$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad}_{F}$

(c) $\underbrace{\text{El triángulo tiene cuatro lados}}_{F}$ si y sólo si $\underbrace{\text{el pentágono tiene cinco lados}}_{V}$.
$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}_{F}$

(d) $\underbrace{\text{Los elefantes son carnívoros}}_{F}$ si y sólo si $\underbrace{\text{los leones son herbívoros}}_{F}$.
$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}_{V}$

1.2.7. Propiedades de los conectivos lógicos

Definición 1.11
Se dice que dos proposiciones son lógicamente equivalentes si tienen los mismos valores de verdad independientemente del valor de verdad de las proposiciones involucradas. Usamos el símbolo $\equiv$ para expresar que dos proposiciones son lógicamente equivalentes y $\not\equiv$ para expresar que no lo son.

Notemos que de acuerdo a la definición, es lo mismo utilizar el símbolo $\equiv$ que el conectivo lógico $\Leftrightarrow$.

[2] Construyamos la tabla de verdad de la doble implicación:

p	q	$p \Rightarrow q$	$q \Rightarrow p$	$(p \Rightarrow q) \wedge (q \Rightarrow p)$
V	V	V	V	V
V	F	F	V	F
F	V	V	F	F
F	F	V	V	V

Definición 1.12
Diremos que una proposición es una tautología (contradicción) si es siempre verdadera (falsa) independientemente del valor de verdad de las proposiciones que la componen. Llamaremos contingencia a una proposición que no es ni una tautología ni una contradicción.

A continuación veremos una lista de propiedades de los conectivos lógicos junto a su demostración mediante las tablas de verdad. Notar que es importante construir las tablas de verdad listando los valores de verdad en el mismo orden para realizar una comparación adecuada.

Proposición 1.1
Sean p, q y r proposiciones, $\boldsymbol{V}$ una tautología y $\boldsymbol{F}$ una contradicción. Entonces se satisfacen las siguientes propiedades de los conectivos lógicos:

(a) Conmutatividad de la conjunción:

$$p \wedge q \equiv q \wedge p.$$

(b) Conmutatividad de la disyunción:

$$p \vee q \equiv q \vee p.$$

(c) Asociatividad de la conjunción:

$$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r).$$

(d) Asociatividad de la disyunción:

$$(p \vee q) \vee r \equiv p \vee (q \vee r).$$

(e) Idempotencia de la conjunción:

$$p \wedge p \equiv p.$$

(f) Idempotencia de la disyunción:

$$p \vee p \equiv p.$$

(g) Doble negación:

$$\neg(\neg p) \equiv p.$$

(h) Distributiva de la conjunción respecto de la disyunción:

$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r).$$

(i) Distributiva de la disyunción respecto de la conjunción:

$$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r).$$

(j) Ley de De Morgan (negación de una conjunción):

$$\neg(p \wedge q) \equiv (\neg p) \vee (\neg q).$$

(k) Ley de De Morgan (negación de una disyunción):

$$\neg(p \vee q) \equiv (\neg p) \wedge (\neg q).$$

(l) Contrarrecíproca de la implicación:

$$p \Rightarrow q \equiv (\neg q) \Rightarrow (\neg p).$$

(m) Condicional como disyunción:

$$p \Rightarrow q \equiv (\neg p) \vee q.$$

(n) Negación del condicional:

$$\neg (p \Rightarrow q) \equiv p \wedge (\neg q).$$

(ñ) Modus ponens:

$$[p \wedge (p \Rightarrow q)] \Rightarrow q \equiv \boldsymbol{V}.$$

(o) Silogismo hipotético:

$$[(p \Rightarrow q) \wedge (q \Rightarrow r)] \Rightarrow (p \Rightarrow r) \equiv \boldsymbol{V}.$$

(p) Absorción:

$$p \wedge (p \vee q) \equiv p,$$
$$p \vee (p \wedge q) \equiv p.$$

(q) Principio de contradicción:

$$p \wedge (\neg p) \equiv \boldsymbol{F}.$$

(r) Principio del tercero excluido:

$$p \vee (\neg p) \equiv \boldsymbol{V}.$$

(s) Dominancia de la conjunción:

$$p \wedge \boldsymbol{F} \equiv \boldsymbol{F}.$$

(t) Dominancia de la disyunción

$$p \vee \boldsymbol{V} \equiv \boldsymbol{V}.$$

(u) Identidad de la conjunción:

$$p \wedge \boldsymbol{V} \equiv p,$$

(v) Identidad de la disyunción:

$$p \vee \boldsymbol{F} \equiv p.$$

Demostración.
(a) Probaremos que $p \wedge q \equiv q \wedge p$ construyendo la tabla de verdad.

p	q	$p \wedge q$	$q \wedge p$
V	V	V	V
V	F	F	F
F	V	F	F
F	F	F	F

(b) Probaremos que $p \vee q \equiv q \vee p$ construyendo la tabla de verdad.

p	q	$p \vee q$	$q \vee p$
V	V	V	V
V	F	V	V
F	V	V	V
F	F	F	F

(c) Probaremos que $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ construyendo la tabla de verdad.

p	q	r	$p \wedge q$	$q \wedge r$	$(p \wedge q) \wedge r$	$p \wedge (q \wedge r)$
V	V	V	V	V	V	V
V	V	F	V	F	F	F
V	F	V	F	F	F	F
V	F	F	F	F	F	F
F	V	V	F	V	F	F
F	V	F	F	F	F	F
F	F	V	F	F	F	F
F	F	F	F	F	F	F

(d) Probaremos que $(p \vee q) \vee r \equiv p \vee (q \vee r)$ construyendo la tabla de verdad.

p	q	r	$p \vee q$	$q \vee r$	$(p \vee q) \vee r$	$p \vee (q \vee r)$
V	V	V	V	V	V	V
V	V	F	V	V	V	V
V	F	V	V	V	V	V
V	F	F	V	F	V	V
F	V	V	V	V	V	V
F	V	F	V	V	V	V
F	F	V	F	V	V	V
F	F	F	F	F	F	F

(e) Probaremos que $p \wedge p \equiv p$ construyendo la tabla de verdad.

p	$p \wedge p$
V	V
F	F

(f) Probaremos que $p \vee p \equiv p$ construyendo la tabla de verdad.

p	$p \vee p$
V	V
F	F

(g) Probaremos que $\neg(\neg p) \equiv p$ construyendo la tabla de verdad.

p	$\neg p$	$\neg(\neg p)$
V	F	V
F	V	F

(h) Probaremos que $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ construyendo la tabla de verdad.

p	q	r	$q \vee r$	$p \wedge q$	$p \wedge r$	$p \wedge (q \vee r)$	$(p \wedge q) \vee (p \wedge r)$
V	V	V	V	V	V	V	V
V	V	F	V	V	F	V	V
V	F	V	V	F	V	V	V
V	F	F	F	F	F	F	F
F	V	V	V	F	F	F	F
F	V	F	V	F	F	F	F
F	F	V	V	F	F	F	F
F	F	F	F	F	F	F	F

(i) Probaremos que $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ construyendo la tabla de verdad.

p	q	r	$q \wedge r$	$p \vee q$	$p \vee r$	$p \vee (q \wedge r)$	$(p \vee q) \wedge (p \vee r)$
V	V	V	V	V	V	V	V
V	V	F	F	V	V	V	V
V	F	V	F	V	V	V	V
V	F	F	F	V	V	V	V
F	V	V	V	V	V	V	V
F	V	F	F	V	F	F	F
F	F	V	F	F	V	F	F
F	F	F	F	F	F	F	F

(j) Probaremos que $\neg (p \wedge q) \equiv (\neg p) \vee (\neg q)$ construyendo la tabla de verdad.

p	q	$p \wedge q$	$\neg p$	$\neg q$	$\neg (p \wedge q)$	$(\neg p) \vee (\neg q)$
V	V	V	F	F	F	F
V	F	F	F	V	V	V
F	V	F	V	F	V	V
F	F	F	V	V	V	V

(k) Probaremos que $\neg (p \vee q) \equiv (\neg p) \wedge (\neg q)$ construyendo la tabla de verdad.

p	q	$p \vee q$	$\neg p$	$\neg q$	$\neg (p \vee q)$	$(\neg p) \wedge (\neg q)$
V	V	V	F	F	F	F
V	F	V	F	V	F	F
F	V	V	V	F	F	F
F	F	F	V	V	V	V

(l) Probaremos que $p \Rightarrow q \equiv (\neg q) \Rightarrow (\neg p)$ construyendo la tabla de verdad.

p	q	$\neg p$	$\neg q$	$p \Rightarrow q$	$(\neg q) \Rightarrow (\neg p)$
V	V	F	F	V	V
V	F	F	V	F	F
F	V	V	F	V	V
F	F	V	V	V	V

(m) Probaremos que $p \Rightarrow q \equiv (\neg p) \vee q$ construyendo la tabla de verdad.

p	q	$\neg p$	$p \Rightarrow q$	$(\neg p) \vee q$
V	V	F	V	V
V	F	F	F	F
F	V	V	V	V
F	F	V	V	V

(n) Probaremos que $\neg (p \Rightarrow q) \equiv p \wedge (\neg q)$ construyendo la tabla de verdad.

p	q	$\neg q$	$p \Rightarrow q$	$\neg (p \Rightarrow q)$	$p \wedge (\neg q)$
V	V	F	V	F	F
V	F	V	F	V	V
F	V	F	V	F	F
F	F	V	V	F	F

(ñ) Probaremos que $[p \wedge (p \Rightarrow q)] \Rightarrow q \equiv \boldsymbol{V}$ construyendo la 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

(o) Probaremos que $[(p \Rightarrow q) \wedge (q \Rightarrow r)] \Rightarrow (p \Rightarrow r) \equiv \boldsymbol{V}$ construyendo la tabla de verdad.

p	q	r	$p \Rightarrow q$	$q \Rightarrow r$	$(p \Rightarrow q) \wedge (q \Rightarrow r)$	$p \Rightarrow r$	$[(p \Rightarrow q) \wedge (q \Rightarrow r)] \Rightarrow (p \Rightarrow r)$
V	V	V	V	V	V	V	V
V	V	F	V	F	F	F	V
V	F	V	F	V	F	V	V
V	F	F	F	V	F	F	V
F	V	V	V	V	V	V	V
F	V	F	V	F	F	V	V
F	F	V	V	V	V	V	V
F	F	F	V	V	V	V	V

(p) Probaremos que $p \wedge (p \vee q) \equiv p$ construyendo la tabla de verdad.

p	q	$p \vee q$	$p \wedge (p \vee q)$
V	V	V	V
V	F	V	V
F	V	V	F
F	F	F	F

Probaremos que $p \vee (p \wedge q) \equiv p$ construyendo la tabla de verdad.

p	q	$p \wedge q$	$p \vee (p \wedge q)$
V	V	V	V
V	F	F	V
F	V	F	F
F	F	F	F

(q) Probaremos que $p \wedge (\neg p) \equiv \boldsymbol{F}$ construyendo la tabla de verdad.

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

(r) Probaremos que $p \vee (\neg p) \equiv \boldsymbol{V}$ construyendo la tabla de verdad.

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

(s) Probaremos que $p \wedge \boldsymbol{F} \equiv \boldsymbol{F}$ construyendo la tabla de verdad.

p	$\boldsymbol{F}$	$p \wedge F$
V	F	F
F	F	F

(t) Probaremos que $p \vee \boldsymbol{V} \equiv \boldsymbol{V}$ construyendo la tabla de verdad.

p	$\boldsymbol{V}$	$p \vee \boldsymbol{V}$
V	V	V
F	V	V

(u) Probaremos que $p \wedge \boldsymbol{V} \equiv p$ construyendo la tabla de verdad.

p	$\boldsymbol{V}$	$p \wedge \boldsymbol{V}$
V	V	V
F	V	F

(v) Probaremos que $p \vee \boldsymbol{F} \equiv p$ construyendo la tabla de verdad.

p	$\boldsymbol{F}$	$p \vee F$
V	F	V
F	F	F

Esto concluye la demostración. ■

1.2.8. Reglas de precedencia

Utilizar múltiples conectivos lógicos para formar proposiciones compuestas puede causar confusiones si no se hace un correcto uso de paréntesis. Por ejemplo,

$$p \Rightarrow p \wedge q \Rightarrow r,$$

¿debe ser interpretada como $[p \Rightarrow (p \wedge q)] \Rightarrow r$, como $(p \Rightarrow p) \wedge (q \Rightarrow r)$ o de alguna otra manera?

Para evitar el uso excesivo de paréntesis se ha establecido cierto orden de precedencia. Este orden de precedencia de mayor a menor es: $\neg$, $\wedge$, $\vee$, $\Rightarrow$ y $\Leftrightarrow$. Si bien la prioridad de $\wedge$ es mayor que la de $\vee$, suele no hacerse distinción entre ellos y se usan los paréntesis para evitar confusiones.

Ejemplo 1.12
Veamos en los siguientes ejemplos el uso de las reglas de precedencia para evitar escribir paréntesis:

Proposición sin paréntesis	Proposición con paréntesis
$\neg p \wedge q$	$(\neg p) \wedge q$
$p \vee \neg q$	$p \vee (\neg q)$
$p \wedge q \vee r$	$(p \wedge q) \vee r$
$p \vee q \wedge r$	$p \vee (q \wedge r)$
$p \Rightarrow q \Leftrightarrow r$	$(p \Rightarrow q) \Leftrightarrow r$
$p \vee q \Rightarrow r$	$(p \vee q) \Rightarrow r$

1.3. Razonamiento deductivo y tipos de demostraciones

En un enunciado de la forma $p \Rightarrow q$, la proposición p representa la hipótesis y la proposición q representa la tesis o lo que se quiere demostrar. Hay varias maneras de demostrar esto:

- Directa: Asumiendo verdadera la hipótesis p, realizamos una sucesión de pasos lógicos válidos, representados por las siguientes implicaciones (que resultan verdaderas):

  $$p \Rightarrow p_1, \quad p_1 \Rightarrow p_2, \ldots, \quad p_{n-1} \Rightarrow p_n, \quad p_n \Rightarrow q$$

  Como p es verdadera y $p \Rightarrow p_1$ es verdadera, entonces la propiedad de modus ponens (ver Proposición 1.1-(ñ)) nos asegura que p_1 es verdadera. Análogamente se sigue que p_2 es verdadera y así sucesivamente hasta concluir que q es verdadera.

- Indirecta: Utilizando la contrarrecíproca de la implicación (ver Proposición 1.1-(l)), demostrar que $p \Rightarrow q$ es verdadera es equivalente a mostrar que $\neg q \Rightarrow \neg p$ es verdadera. Esto significa asumir que la tesis es falsa (o que $\neg q$ es verdadera), y a través de pasos lógicos válidos llegar a que p es falsa (o que $\neg p$ es verdadera).
- Por el absurdo: Si se desea probar que una proposición p es verdadera, suponemos que es falsa, y a través de pasos lógicos válidos deberíamos deducir la falsedad de algo que sabemos que es verdadero. Esta contradicción provino de suponer la falsedad de p, por lo cual se concluye que p es verdadera.

Ejemplos de este tipo de demostraciones se usarán durante toda la carrera.

Ejemplo 1.13

(a) Demostración directa: "Si n es par, entonces n^2 es par".

Demostración.

Este enunciado puede expresarse como una implicación $p \Rightarrow q$, donde

$$\begin{aligned} p &: \text{“}n \text{ es par”} \\ q &: \text{“}n^2 \text{ es par”} \end{aligned}$$

Asumiendo verdadera la hipótesis, podemos escribir:

$$n = 2 \cdot k,$$

donde k es un número entero. Ahora realizando algunos cálculos:

$$n^2 = (2 \cdot k)^2 = 4 \cdot k^2 = 2 \cdot \left(2 \cdot k^2\right).$$

por lo que n^2 es un múltiplo de 2, es decir, n^2 es par. ■

(b) Demostración indirecta: "Si n^2 es par entonces n es par".

Demostración.

Este enunciado puede expresarse como una implicación $p \Rightarrow q$, donde

$$\begin{aligned} p &: \text{“}n^2 \text{ es par”} \\ q &: \text{“}n \text{ es par”} \end{aligned}$$

Lo que vamos a probar es $\neg q \Rightarrow \neg p$. Vamos a asumir que q es falsa, es decir, supondremos que n no es par. Esto significa asumir que n es impar, o sea, $n = 2 \cdot k + 1$ para algún entero k. Ahora podemos ver qué le sucede a n^2:

$$n^2 = (2 \cdot k + 1)^2 = 4 \cdot k^2 + 4 \cdot k + 1 = 2 \cdot \left(2 \cdot k^2 + 2 \cdot k\right) + 1.$$

Como el número $2 \cdot (2 \cdot k^2 + 2 \cdot k)$ es un entero par, entonces podemos deducir que n^2 es un número impar. Esto significa que n^2 no es par, o sea, p es falsa. ■

(c) Demostración por el absurdo: "El número $\sqrt{2}$ es un número irracional".

Demostración.

Vamos a suponer que el número $\sqrt{2}$ no es irracional, o sea, asumiremos que $\sqrt{2}$ es un número racional. Esto significa que $\sqrt{2}$ es un cociente de dos enteros, es decir:

$$\sqrt{2} = \frac{m}{n},$$

donde m y n son números enteros y $n \neq 0$. Podemos asumir que m y n son naturales que no poseen factores en común. De la expresión anterior, se obtiene que

$$2 = \frac{m^2}{n^2},$$

es decir,

$$2 \cdot n^2 = m^2.$$

Esto significa que m^2 es un número par. Anteriormente habíamos demostrado que m resulta un número par. Esto significa que

$$m = 2 \cdot k,$$

para algún entero k. Ahora bien, realizando los siguientes cálculos tenemos que:

$$2 \cdot n^2 = (2 \cdot k)^2 = 4 \cdot k^2.$$

Simplificando obtenemos que:

$$n^2 = 2 \cdot k^2.$$

O sea, n^2 es un número par. Por lo demostrado anteriormente tenemos que n también es un número par. Resumiendo, n y m son pares. Sin embargo habíamos dicho al comienzo que m y n no tenían factores en común. Esto es una contradicción que provino de suponer que $\sqrt{2}$ es un número racional. ■

1.4. Noción de conjuntos y elementos

Definición 1.13
Un conjunto es una colección de objetos que podrían ser de cualquier naturaleza. Se usarán letras mayúsculas para denotar los conjuntos.

Ejemplo 1.14

(a) A : conjunto de los peces de color naranja.

(b) B : conjunto de los alumnos de primer año de la FACENA.

(c) C : conjunto de los perros nacidos en la ciudad de Corrientes.

(d) D : conjunto de los personas vivas que poseen nacionalidad argentina.

Definición 1.14
Existen conjuntos numéricos especiales, a saber:

- $\mathbb{N}$*: conjunto de los números naturales.*
- $\mathbb{Z}$*: conjunto de los números enteros.*
- $\mathbb{Q}$*: conjunto de los números racionales.*
- $\mathbb{R}$*: conjunto de los números reales.*

- $\mathbb{C}$*: conjunto de los números complejos.*

Más adelante definiremos con precisión estos conjuntos, aunque seguramente ya se ha visto algo en la escuela secundaria.

Definición 1.15
Los objetos que forman el conjunto son llamados elementos. Se usarán letras minúsculas para denotar a los elementos.

Definición 1.16
Dado un objeto cualquiera a y un conjunto A, puede decirse si el objeto a está o no en el conjunto A. Si el elemento a está en el conjunto A, diremos que pertenece a A, y se denota como:

$$a \in A.$$

En caso de no estar, diremos que a no pertenece a A, y se denota como:

$$a \notin A.$$

Observación 1.1
Notar que $a \in A$ es una proposición lógica. Además se satisface que

$$a \notin A \equiv \neg\,(a \in A)\,.$$

Definición 1.17
Definir un conjunto es describir de manera precisa cuáles son los elementos de dicho conjunto.

Una forma de definir un conjunto es por extensión, es decir, listando los elementos uno por uno (en caso que sea posible) separándolos por comas, sin repetirlos, sin importar el orden, y encerrándolos entre llaves.

Otra manera de definir un conjunto es por comprensión, es decir, enunciando las propiedades que satisfacen sus elementos:

$$A = \{x \in \mathcal{U} : x \text{ cumple la propiedad } P\}\,.$$

Se lee: el conjunto formado por los elementos x que pertenecen a $\mathcal{U}$ tales que satisfacen la propiedad P. La pertenencia al conjunto $\mathcal{U}$ puede omitirse en caso que el contexto lo aclare.

A veces resulta conveniente usar puntos suspensivos para denotar elementos que se sobreentiende están en el conjunto. Así, por ejemplo, el conjunto $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ puede escribirse como $A = \{0, 1, 2, \ldots, 9\}$. La forma en donde se ubican los puntos suspensivos debe ser tal de no causar confusión en el lector. Es aún mas común usar esto para conjuntos infinitos, por ejemplo el conjunto de los números naturales $\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$, ya que de otro modo sería imposible listar todos sus elementos.

Ejemplo 1.15
(a) Veamos algunos ejemplos de conjuntos definidos por extensión:

- $A = \{1, 2, 3\}$. Los elementos son 1, 2 y 3.
- $B = \{\text{Damián}, \text{Leandro}, \text{Facundo}, \text{Pedro}, \text{Simón}\}$. Los elementos son Damián, Leandro, Facundo, Pedro y Simón.
- $C = \{\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow\}$. Los elementos son $\neg$, $\wedge$, $\vee$, $\Rightarrow$ y $\Leftrightarrow$.
- $D = \{\copyright, ✠, \alpha, \bigstar, ♫\}$. Los elementos son $\copyright$, ✠, α, $\bigstar$ y ♫.
- $E = \{a, b, \{c, d\}\}$. Los elementos son a, b y $\{c, d\}$.
- $F = \{2, 4, 6, 8, \ldots\}$. Los elementos son los naturales pares.

- $\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$.

(b) Veamos algunos ejemplos de conjuntos definidos por comprensión:

- $A = \{x \in \mathbb{N} : x + 1 > 2\}$. Los elementos son $2, 3, 4, \ldots$.
- $B = \left\{2^k : k \in \mathbb{N} \text{ y } 1 \leqslant k \leqslant 5\right\}$. Los elementos son 2^1, 2^2, 2^3, 2^4 y 2^5.
- $C = \{2 \cdot x + 1 : x \in \mathbb{N} \text{ y } 2 \leqslant x < 7\}$. Los elementos son 5, 7, 9, 11 y 13.
- $D = \{x \in \mathbb{R} : x^2 + 1 = 0\}$. Más adelante se verá que este conjunto no tiene elementos.

(c) Existen algunos conjuntos (llamados intervalos) que serán de utilidad:

- $(a, b) = \{x \in \mathbb{R} : a < x < b\}$.
- $[a, b] = \{x \in \mathbb{R} : a \leqslant x \leqslant b\}$.
- $(a, b] = \{x \in \mathbb{R} : a < x \leqslant b\}$.
- $[a, b) = \{x \in \mathbb{R} : a \leqslant x < b\}$.

Definición 1.18
Definimos el conjunto vacío como el conjunto que no posee elementos, y se denota por $\varnothing$.

Una forma errónea de escribir el conjunto vacío es $\{\varnothing\}$, ya que dicho símbolo representa un conjunto de un solo elemento, a saber el conjunto vacío.

1.5. Subconjuntos

Definición 1.19
Diremos que un conjunto A es un subconjunto del conjunto B si cada elemento de A es un elemento de B. Se denota por $A \subset B$ y se dice que A está incluido en B (análogamente denotaremos por $A \not\subset B$ si A no está incluido en B). En símbolos sería

$$A \subset B \Leftrightarrow \textit{para cada } x \textit{ se cumple: } x \in A \Rightarrow x \in B.^3$$

Ejemplo 1.16
Consideremos los siguientes conjuntos:

$$A = \{1, 2, a\}, \quad B = \{1, b, 2, a, c, \bigstar\}.$$

Notemos que

- tomamos $1 \in A$, y nos damos cuenta que $1 \in B$,
- tomamos $2 \in A$, y nos damos cuenta que $2 \in B$,
- tomamos $a \in A$, y nos damos cuenta que $a \in B$.

Hemos visto entonces que cada elemento de A es también un elemento de B, por lo que $A \subset B$.

[3] Más adelante veremos que la definición puede escribirse de la siguiente manera:

$$A \subset B \Leftrightarrow \forall x, x \in A \Rightarrow x \in B.$$

Definición 1.20
Diremos que dos conjuntos A y B son iguales si tienen los mismos elementos. Es decir,

$$A = B \Leftrightarrow A \subset B \wedge B \subset A,$$

es decir,

$$A = B \Leftrightarrow \text{para cada } x \text{ se cumple: } x \in A \Leftrightarrow x \in B.$$

Diremos que dos conjuntos A y B son:

- *Distintos: si $A \neq B$.*
- *Disjuntos: si A y B no tienen elementos en común.*
- *Si $A \subset B$, pero son distintos, diremos que A es un subconjunto propio de B, y se denota por $A \subsetneq B$.*

Ejemplo 1.17

(a) Consideremos los conjuntos:

$$A = \{1, 3\}, \quad B = \left\{n : n^2 - 4 \cdot n = -3\right\}.$$

Veamos que $A \subset B$. Notemos que $1 \in B$ pues $1^2 - 4 \cdot 1 = -3$, o sea que 1 satisface la propiedad para estar en B. Además notemos que $3 \in B$ pues $3^2 - 4 \cdot 3 = -3$, o sea que 3 satisface la propiedad para estar en B.

Veamos que $B \subset A$. Tomemos un elemento arbitrario n de B. Luego:

$$\begin{aligned}
n \in B &\Rightarrow n^2 - 4 \cdot n = -3 \text{ por definición del conjunto } B \\
&\Rightarrow n^2 - 4 \cdot n + 3 = 0 \text{ pasando de miembro} \\
&\Rightarrow n = \frac{-(-4) \pm \sqrt{(-4)^2 - 4 \cdot 1 \cdot 3}}{2 \cdot 1} \\
&\Rightarrow n = \frac{4 \pm \sqrt{16 - 12}}{2} \\
&\Rightarrow n = \frac{4 \pm \sqrt{4}}{2} \\
&\Rightarrow n = \frac{4 \pm 2}{2} \\
&\Rightarrow n = 1 \text{ o } n = 3 \\
&\Rightarrow n \in A.
\end{aligned}$$

Acabamos de probar que $A \subset B$ y $B \subset A$, lo que muestra que $A = B$.

(b) Consideremos los conjuntos:

$$A = \{1, 3\}, \quad B = \{1\}.$$

Como A y B no poseen los mismos elementos, entonces $A \neq B$.

(c) Consideremos los conjuntos:

$$A = \{1, 3\}, \quad B = \{2, 5, 6\}.$$

Como A y B no poseen elementos en común, entonces A y B son disjuntos.

(d) Notar que el Ejemplo 1.16 muestra que A es un subconjunto propio de B (pues $c \in B$ pero $c \notin A$), es decir, $A \subsetneq B$.

1.6. Conjunto universal y diagramas de Venn

El conjunto universal, usualmente denotado $\mathcal{U}$, es el conjunto más grande en una discusión, y todos los demás conjuntos considerados serán subconjuntos de éste. Muchas veces este universo está tácitamente dado, o se sobreentiende del contexto en el que se está trabajando. Otras veces es necesario indicarlo.

Por ejemplo, si estamos describiendo un conjunto numérico, podríamos decir que un conjunto está formado por números enteros que cumplen cierta propiedad. Tal conjunto o "universo" se denomina conjunto universal, y se simboliza por $\mathcal{U}$.

Por ejemplo, si

$$A = \{x \in \mathbb{R} : x > 2\},$$

el conjunto universal podría ser $\mathbb{R}$.

Usualmente, los conjuntos pueden ser representados gráficamente utilizando diagramas de Venn. El conjunto universal se representa con un cuadrilátero, los conjuntos dentro del universal se representan con una línea cerrada, y los elementos son colocados dentro señalándolos con puntos (ver Figura 1.1).

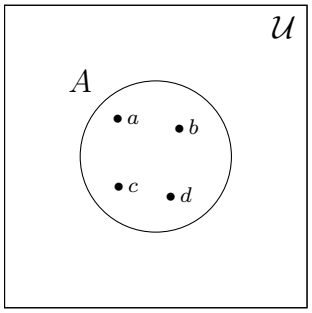


Figura 1.1: Diagrama de Venn del conjunto $A = \{a, b, c, d\}$ con el conjunto universal.

1.7. Operaciones entre conjuntos

1.7.1. Unión de conjuntos

Definición 1.21
Dados A y B dos conjuntos, el conjunto $A \cup B$ (se lee "A unión B") es un nuevo conjunto cuyos elementos pertenecen a A o a B. En símbolos:

$$A \cup B = \{x \in \mathcal{U} : x \in A \vee x \in B\}.$$

Notar que la unión de conjuntos está relacionada al conectivo lógico $\vee$.

En un diagrama de Venn se puede representar la unión de dos conjuntos sombreando el área que cubren ambos conjuntos (ver Figura 1.2).

Ejemplo 1.18

(a) Sean $A = \{a, b, 7\}$ y $B = \{1, 5, 7\}$. Entonces $A \cup B = \{a, b, 1, 5, 7\}$.

(b) Sean $A = \{1, 2, 3\}$ y $B = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Entonces $A \cup B = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

(c) Sean $A = \{x \in \mathbb{Z} : x \text{ es par}\}$ y $B = \{x \in \mathbb{Z} : x \text{ es impar}\}$. Entonces $A \cup B = \mathbb{Z}$.

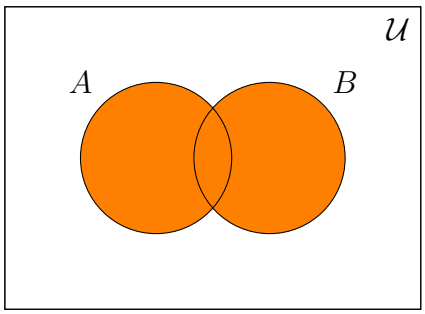


Figura 1.2: Unión de los conjuntos A y B.

1.7.2. Intersección de conjuntos

Definición 1.22
Dados A y B dos conjuntos, el conjunto $A \cap B$ (se lee "A intersección B") es un nuevo conjunto cuyos elementos pertenecen a A y a B. En símbolos:

$$A \cap B = \{x \in \mathcal{U} : x \in A \wedge x \in B\}.$$

Notar que la intersección de conjuntos está relacionada al conectivo lógico $\wedge$.

En un diagrama de Venn se puede representar la intersección de dos conjuntos sombreando el área común a ambos conjuntos (ver Figura 1.3).

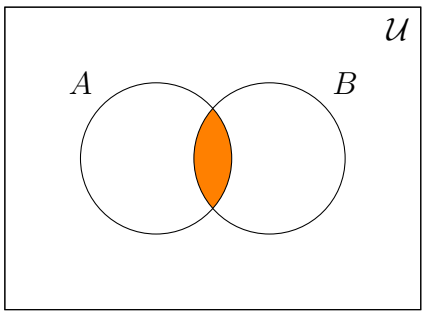


Figura 1.3: Intersección de los conjuntos A y B.

Ejemplo 1.19

(a) Sean $A = \{x \in \mathbb{N} : 1 \leqslant x \leqslant 10\}$ y $B = \{x \in \mathbb{N} : x \text{ es par}\}$. Entonces

$$A \cap B = \{2, 4, 6, 8, 10\}.$$

(b) Sean $A = \{a, b, 1, \bigstar\}$ y $B = \{b, \bigstar, 1, \eighthnote\eighthnote\}$. Entonces

$$A \cap B = \{b, 1, \bigstar\}.$$

(c) Sean $A = \{x \in \mathbb{N} : x \text{ es par}\}$ y $B = \{x \in \mathbb{N} : x \text{ es impar}\}$. Entonces

$$A \cap B = \varnothing.$$

Cuando A y B son disjuntos, la definición de intersección nos dice que $A \cap B = \varnothing$.

1.7.3. Complemento de un conjunto

Definición 1.23
Dado un conjunto A incluido en un conjunto universal $\mathcal{U}$, el conjunto A^c (se lee "complemento de A respecto de $\mathcal{U}$") es el conjunto cuyos elementos pertenecen a $\mathcal{U}$ pero que no están en A. En símbolos:

$$A^c = \{x \in \mathcal{U} : x \notin A\}.$$

Notar que el complemento de un conjunto está relacionado al conectivo lógico $\neg$.

En un diagrama de Venn se puede representar el complemento de un conjunto sombreando todo lo que no está en el conjunto (ver Figura 1.4).

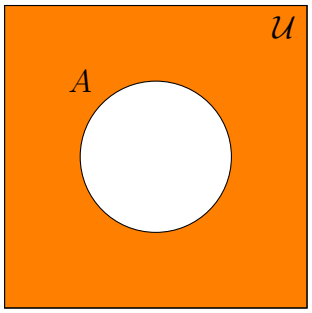


Figura 1.4: Complemento de A.

Ejemplo 1.20
(a) Sean $\mathcal{U} = \mathbb{N}$ y $A = \{x \in \mathbb{N} : x > 5\}$. Entonces

$$A^c = \{1, 2, 3, 4, 5\}.$$

(b) Sean $\mathcal{U} = \mathbb{N}$ y $A = \{x \in \mathbb{N} : x \text{ es par}\}$. Entonces

$$A^c = \{x \in \mathbb{N} : x \text{ es impar}\}.$$

1.7.4. Diferencia de conjuntos

Definición 1.24
Dados A y B dos conjuntos, el conjunto $A - B$ (se lee "diferencia entre A y B") es un nuevo conjunto cuyos elementos pertenecen a A pero no pertenecen a B. En símbolos:

$$A - B = \{x \in \mathcal{U} : x \in A \wedge x \notin B\}.$$

Notar que de la definición se desprende que:

$$A - B = A \cap B^c.$$

En un diagrama de Venn se puede representar la diferencia entre dos conjuntos sombreando el área que pertenece exclusivamente a uno de ellos (ver Figura 1.5).

Ejemplo 1.21
(a) Sean $A = \{1, 2, 3, x, w\}$ y $B = \{1, 9, a, b\}$. Entonces

$$A - B = \{2, 3, x, w\}.$$

(b) Sean $A = \mathbb{R}$ y $B = \{x \in \mathbb{R} : x < 0\}$. Entonces

$$A - B = \{x \in \mathbb{R} : x \geqslant 0\}.$$

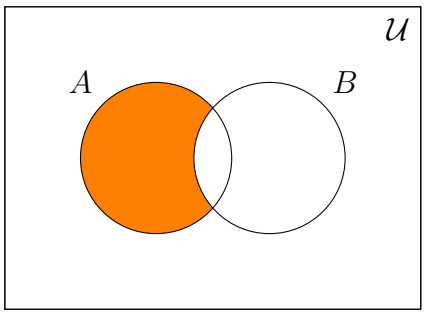


Figura 1.5: Diferencia entre los conjuntos A y B.

Notar que la diferencia entre conjuntos no tiene nada que ver con la operación aritmética de restar. Recordar que el concepto de conjuntos no sólo involucra conjuntos numéricos, sino elementos que pueden ser de otra naturaleza.

El complemento de un conjunto A que está incluido en un conjunto universal $\mathcal{U}$ es un caso particular de diferencia entre conjuntos, pues:

$$A^c = \mathcal{U} - A.$$

1.7.5. Diferencia simétrica de conjuntos

Definición 1.25
Dados A y B dos conjuntos, el conjunto $A\triangle B$ (se lee "diferencia simétrica entre A y B") es un nuevo conjunto definido por:

$$A\triangle B = \{x \in \mathcal{U} : x \in A \veebar x \in B\} = (A - B) \cup (B - A)\,.$$

Notar que la diferencia simétrica entre dos conjuntos está relacionada al conectivo lógico $\veebar$.

En un diagrama de Venn se puede representar la diferencia simétrica entre dos conjuntos sombreando el área que se muestra en la Figura 1.6.

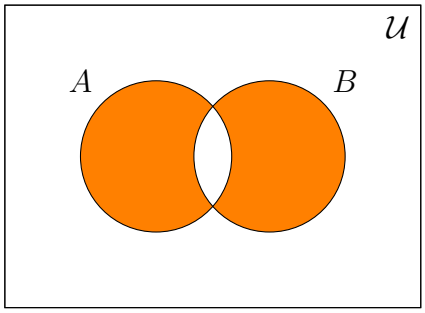


Figura 1.6: Diferencia simétrica entre los conjuntos A y B.

Ejemplo 1.22

(a) Sean $A = \{a, b, c, 1, 2, 3\}$ y $B = \{a, x, w, 1, 4, 5\}$. Entonces

$$A\triangle B = \{b, c, 2, 3, x, w, 4, 5\}\,.$$

(b) Sean $A = \{2, 4, 6, 8, 10\}$ y $B = \{1, 2, 6, 8, 9\}$. Entonces

$$A\triangle B = \{1, 4, 9, 10\}\,.$$

1.7.6. Propiedades de las operaciones entre conjuntos

A continuación se enunciarán y demostrarán las propiedades de las operaciones entre conjuntos. El objetivo es que el alumno aprenda a realizar sus primeras demostraciones y a usar correctamente los pasos lógicos.

Proposición 1.2
Sean A, B, C subconjuntos de un conjunto universal $\mathcal{U}$. Entonces se satisfacen las siguientes propiedades:

(a) Conmutativa de la intersección:

$$A \cap B = B \cap A.$$

(b) Conmutativa de la unión:

$$A \cup B = B \cup A.$$

(c) Asociativa de la intersección:

$$(A \cap B) \cap C = A \cap (B \cap C).$$

(d) Asociativa de la unión:

$$(A \cup B) \cup C = A \cup (B \cup C).$$

(e) Idempotencia de la intersección:

$$A \cap A = A.$$

(f) Idempotencia de la unión:

$$A \cup A = A.$$

(g) Doble complemento:

$$(A^c)^c = A.$$

(h) Propiedad distributiva de la intersección respecto de la unión:

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

(i) Propiedad distributiva de la unión respecto de la intersección:

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

(j) Ley de De Morgan (complemento de la intersección):

$$(A \cap B)^c = A^c \cup B^c.$$

(k) Ley de De Morgan (complemento de la unión):

$$(A \cup B)^c = A^c \cap B^c.$$

(l) Relación entre complemento e inclusión:

$$A \subset B \Rightarrow B^c \subset A^c.$$

(m) Absorción:

$$\begin{aligned} A \cap (A \cup B) &= A, \\ A \cup (A \cap B) &= A. \end{aligned}$$

(n) Ley de complemento (para la intersección):

$$A \cap A^c = \varnothing.$$

(ñ) Ley de complemento (para la unión):

$$A \cup A^c = \mathcal{U}.$$

(o) Dominancia de la intersección:

$$A \cap \varnothing = \varnothing.$$

(p) Dominancia de la unión:

$$A \cup \mathcal{U} = \mathcal{U}.$$

(q) Identidad de la intersección:

$$A \cap \mathcal{U} = A.$$

(r) Identidad de la unión:

$$A \cup \varnothing = A.$$

(s) Complemento del conjunto vacío:

$$\varnothing^c = \mathcal{U}.$$

(t) Complemento del conjunto universal:

$$\mathcal{U}^c = \varnothing.$$

(u) El conjunto vacío es subconjunto de todo conjunto:

$$\varnothing \subset A.$$

Demostración.
(a) Probaremos que $A \cap B = B \cap A$.

$$\begin{aligned} x \in A \cap B &\Leftrightarrow x \in A \wedge x \in B \text{ por Definición 1.22 (intersección de conjuntos)} \\ &\Leftrightarrow x \in B \wedge x \in A \text{ por Proposición 1.1-(a) (conmutativa de la conjunción)} \\ &\Leftrightarrow x \in B \cap A \text{ por Definición 1.22 (intersección de conjuntos)} \end{aligned}$$

(b) Probaremos que $A \cup B = B \cup A$.

$$\begin{aligned} x \in A \cup B &\Leftrightarrow x \in A \vee x \in B \text{ por Definición 1.21 (unión de conjuntos)} \\ &\Leftrightarrow x \in B \vee x \in A \text{ por Proposición 1.1-(b) (conmutativa de la disyunción)} \\ &\Leftrightarrow x \in B \cup A \text{ por Definición 1.21 (unión de conjuntos)} \end{aligned}$$

(c) Probaremos que $(A \cap B) \cap C = A \cap (B \cap C)$.

$$\begin{aligned} x \in (A \cap B) \cap C &\Leftrightarrow x \in A \cap B \wedge x \in C \text{ por Definición 1.22 (intersección de conjuntos)} \\ &\Leftrightarrow (x \in A \wedge x \in B) \wedge x \in C \text{ por Definición 1.22 (intersección de conjuntos)} \\ &\Leftrightarrow x \in A \wedge (x \in B \wedge x \in C) \text{ por Proposición 1.1-(c)} \\ &\Leftrightarrow x \in A \wedge x \in B \cap C \text{ por Definición 1.22 (intersección de conjuntos)} \\ &\Leftrightarrow x \in A \cap (B \cap C) \text{ por Definición 1.22 (intersección de conjuntos)} \end{aligned}$$

(d) Probaremos que $(A \cup B) \cup C = A \cup (B \cup C)$.

$$\begin{aligned}
x \in (A \cup B) \cup C &\Leftrightarrow x \in A \cup B \vee x \in C \text{ por Definición 1.21 (unión de conjuntos)} \\
&\Leftrightarrow (x \in A \vee x \in B) \vee x \in C \text{ por Definición 1.21 (unión de conjuntos)} \\
&\Leftrightarrow x \in A \vee (x \in B \vee x \in C) \text{ por Proposición 1.1-(d)} \\
&\Leftrightarrow x \in A \vee x \in B \cup C \text{ por Definición 1.21 (unión de conjuntos)} \\
&\Leftrightarrow x \in A \cup (B \cup C) \text{ por Definición 1.21 (unión de conjuntos)}
\end{aligned}$$

(e) Probaremos que $A \cap A = A$.

$$\begin{aligned}
x \in A \cap A &\Leftrightarrow x \in A \wedge x \in A \text{ por Definición 1.22 (intersección de conjuntos)} \\
&\Leftrightarrow x \in A \text{ por Proposición 1.1-(e)}
\end{aligned}$$

(f) Probaremos que $A \cup A = A$.

$$\begin{aligned}
x \in A \cup A &\Leftrightarrow x \in A \vee x \in A \text{ por Definición 1.21 (unión de conjuntos)} \\
&\Leftrightarrow x \in A \text{ por Proposición 1.1-(f) (idempotencia de la disyunción)}
\end{aligned}$$

(g) Probaremos que $(A^c)^c = A$.

$$\begin{aligned}
x \in (A^c)^c &\Leftrightarrow x \notin A^c \text{ por Definición 1.23 (complemento de un conjunto)} \\
&\Leftrightarrow \neg (x \in A^c) \text{ por Observación 1.1} \\
&\Leftrightarrow \neg (x \notin A) \text{ por Definición 1.23 (complemento de un conjunto)} \\
&\Leftrightarrow \neg (\neg (x \in A)) \text{ por Observación 1.1} \\
&\Leftrightarrow x \in A \text{ por Proposición 1.1-(g) (doble negación)}
\end{aligned}$$

(h) Probaremos que $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

$$\begin{aligned}
x \in A \cap (B \cup C) &\Leftrightarrow x \in A \wedge x \in B \cup C \text{ por Definición 1.22 (intersección de conjuntos)} \\
&\Leftrightarrow x \in A \wedge (x \in B \vee x \in C) \text{ por Definición 1.21 (unión de conjuntos)} \\
&\Leftrightarrow (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \text{ por Proposición 1.1-(h) (distributiva)} \\
&\Leftrightarrow x \in A \cap B \vee x \in A \cap C \text{ por Definición 1.22 (intersección de conjuntos)} \\
&\Leftrightarrow x \in (A \cap B) \cup (A \cap C) \text{ por Definición 1.21 (unión de conjuntos)}
\end{aligned}$$

(i) Probaremos que $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

$$\begin{aligned}
x \in A \cup (B \cap C) &\Leftrightarrow x \in A \vee x \in B \cap C \text{ por Definición 1.21 (unión de conjuntos)} \\
&\Leftrightarrow x \in A \vee (x \in B \wedge x \in C) \text{ por Definición 1.22 (intersección de conjuntos)} \\
&\Leftrightarrow (x \in A \vee x \in B) \wedge (x \in A \vee x \in C) \text{ por Proposición 1.1-(i) (distributiva)} \\
&\Leftrightarrow x \in A \cup B \wedge x \in A \cup C \text{ por Definición 1.21 (unión de conjuntos)} \\
&\Leftrightarrow x \in (A \cup B) \cap (A \cup C) \text{ por Definición 1.22 (intersección de conjuntos)}
\end{aligned}$$

(j) Probaremos que $(A \cap B)^c = A^c \cup B^c$.

$$\begin{aligned}
x \in (A \cap B)^c &\Leftrightarrow x \notin A \cap B \text{ por Definición 1.23 (complemento de un conjunto)} \\
&\Leftrightarrow \neg\,(x \in A \cap B) \text{ por Observación 1.1} \\
&\Leftrightarrow \neg\,(x \in A \wedge x \in B) \text{ por Definición 1.22 (intersección de conjuntos)} \\
&\Leftrightarrow \neg\,(x \in A) \vee \neg\,(x \in B) \text{ por Proposición 1.1-(j) (ley de De Morgan)} \\
&\Leftrightarrow x \notin A \vee x \notin B \text{ por Observación 1.1} \\
&\Leftrightarrow x \in A^c \vee x \in B^c \text{ por Definición 1.23 (complemento de un conjunto)} \\
&\Leftrightarrow x \in A^c \cup B^c \text{ por Definición 1.21 (unión de conjuntos)}
\end{aligned}$$

(k) Probaremos que $(A \cup B)^c = A^c \cap B^c$.

$$\begin{aligned}
x \in (A \cup B)^c &\Leftrightarrow x \notin A \cup B \text{ por Definición 1.23 (complemento de un conjunto)} \\
&\Leftrightarrow \neg\,(x \in A \cup B) \text{ por Observación 1.1} \\
&\Leftrightarrow \neg\,(x \in A \vee x \in B) \text{ por Definición 1.21 (unión de conjuntos)} \\
&\Leftrightarrow \neg\,(x \in A) \wedge \neg\,(x \in B) \text{ por Proposición 1.1-(k) (ley de De Morgan)} \\
&\Leftrightarrow x \notin A \wedge x \notin B \text{ por Observación 1.1} \\
&\Leftrightarrow x \in A^c \wedge x \in B^c \text{ por Definición 1.23 (complemento de un conjunto)} \\
&\Leftrightarrow x \in A^c \cap B^c \text{ por Definición 1.22 (intersección de conjuntos)}
\end{aligned}$$

(l) Probaremos que $A \subset B \Rightarrow B^c \subset A^c$.

$$\begin{aligned}
x \in B^c &\Rightarrow x \notin B \text{ por Definición 1.23 (complemento de un conjunto)} \\
&\Rightarrow \neg\,(x \in B) \text{ por Observación 1.1} \\
&\Rightarrow \neg\,(x \in A) \text{ por Proposición 1.1-(l) pues } x \in A \Rightarrow x \in B \text{ es } V \\
&\Rightarrow x \notin A \text{ por Observación 1.1} \\
&\Rightarrow x \in A^c \text{ por Definición 1.23 (complemento de un conjunto)}
\end{aligned}$$

(m) Probaremos que $A \cap (A \cup B) = A$.

$$\begin{aligned}
x \in A \cap (A \cup B) &\Leftrightarrow x \in A \wedge x \in A \cup B \text{ por Definición 1.22 (intersección de conjuntos)} \\
&\Leftrightarrow x \in A \wedge (x \in A \vee x \in B) \text{ por Definición 1.21 (unión de conjuntos)} \\
&\Leftrightarrow x \in A \text{ por Proposición 1.1-(p) (absorción)}
\end{aligned}$$

Ahora probaremos que $A \cup (A \cap B) = A$.

$$\begin{aligned}
x \in A \cup (A \cap B) &\Leftrightarrow x \in A \vee x \in A \cap B \text{ por Definición 1.21 (unión de conjuntos)} \\
&\Leftrightarrow x \in A \vee (x \in A \wedge x \in B) \text{ por Definición 1.22 (intersección de conjuntos)} \\
&\Leftrightarrow x \in A \text{ por Proposición 1.1-(p) (absorción)}
\end{aligned}$$

(n) Probaremos que $A \cap A^c = \varnothing$.
Supongamos que $A \cap A^c \neq \varnothing$. Esto significa que existe $x \in A \cap A^c$. Ahora:

$$\begin{aligned}
x \in A \cap A^c &\Leftrightarrow x \in A \wedge x \in A^c \text{ por Definición 1.22 (intersección de conjuntos)} \\
&\Leftrightarrow x \in A \wedge x \notin A \text{ por Definición 1.23 (complemento de un conjunto)}
\end{aligned}$$

$$\Leftrightarrow \quad x \in A \wedge \neg\,(x \in A) \text{ por Observación 1.1}$$
$$\Leftrightarrow \quad \boldsymbol{F} \text{ por Proposición 1.1-(q) (principio de contradicción)}$$

Esto conduce a una contradicción, que provino de suponer que $A \cap A^c \neq \varnothing$.

(ñ) Probaremos que $A \cup A^c = \mathcal{U}$.

Por hipótesis y Definición 1.23, tanto A como A^c son subconjuntos de $\mathcal{U}$. Por Definición 1.21 se tiene que $A \cup A^c \subset \mathcal{U}$.

Por otro lado, si $x \in \mathcal{U}$ hay únicamente dos posibilidades: $x \in A$ o $x \notin A$, es decir $x \in A$ o $x \in A^c$, es decir, $x \in A \cup A^c$. Esto significa que $\mathcal{U} \subset A \cup A^c$.

(o) Probaremos que $A \cap \varnothing = \varnothing$.

$$\begin{aligned} x \in A \cap \varnothing \quad &\Leftrightarrow \quad x \in A \wedge x \in \varnothing \text{ por Definición 1.22 (intersección de conjuntos)} \\ &\Leftrightarrow \quad x \in A \wedge \boldsymbol{F} \text{ pues la proposición } x \in \varnothing \text{ es una contradicción} \\ &\Leftrightarrow \quad \boldsymbol{F} \text{ por Proposición 1.1-(s) (dominancia de la conjunción)} \\ &\Leftrightarrow \quad x \in \varnothing \text{ pues la proposición } x \in \varnothing \text{ es una contradicción} \end{aligned}$$

(p) Probaremos que $A \cup \mathcal{U} = \mathcal{U}$.

$$\begin{aligned} x \in A \cup \mathcal{U} \quad &\Leftrightarrow \quad x \in A \vee x \in \mathcal{U} \text{ por Definición 1.21 (unión de conjuntos)} \\ &\Leftrightarrow \quad x \in A \vee \boldsymbol{V} \text{ pues la proposición } x \in \mathcal{U} \text{ es una tautología} \\ &\Leftrightarrow \quad \boldsymbol{V} \text{ por Proposición 1.1-(t) (dominancia de la disyunción)} \\ &\Leftrightarrow \quad x \in \mathcal{U} \text{ pues la proposición } x \in \mathcal{U} \text{ es una tautología} \end{aligned}$$

(q) Probaremos que $A \cap \mathcal{U} = A$.

$$\begin{aligned} x \in A \cap \mathcal{U} \quad &\Leftrightarrow \quad x \in A \wedge x \in \mathcal{U} \text{ por Definición 1.22 (intersección de conjuntos)} \\ &\Leftrightarrow \quad x \in A \wedge \boldsymbol{V} \text{ pues la proposición } x \in \mathcal{U} \text{ es una tautología} \\ &\Leftrightarrow \quad x \in A \text{ por Proposición 1.1-(u) (pues la proposición } x \in \mathcal{U} \text{ es una tautología)} \end{aligned}$$

(r) Probaremos que $A \cup \varnothing = A$.

$$\begin{aligned} x \in A \cup \varnothing \quad &\Leftrightarrow \quad x \in A \vee x \in \varnothing \text{ por Definición 1.21 (unión de conjuntos)} \\ &\Leftrightarrow \quad x \in A \vee \boldsymbol{F} \text{ pues la proposición } x \in \varnothing \text{ es una contradicción} \\ &\Leftrightarrow \quad x \in A \text{ por Proposición 1.1-(v) (pues la proposición } x \in \varnothing \text{ es una contradicción)} \end{aligned}$$

(s) Probaremos que $\varnothing^c = \mathcal{U}$.

$$\begin{aligned} x \in \varnothing^c \quad &\Leftrightarrow \quad x \notin \varnothing \text{ por Definición 1.23 (complemento de un conjunto)} \\ &\Leftrightarrow \quad \boldsymbol{V} \text{ por Definición 1.18 (conjunto de vacío)} \\ &\Leftrightarrow \quad x \in \mathcal{U} \text{ pues la proposición } x \in \mathcal{U} \text{ es una tautología} \end{aligned}$$

(t) Probaremos que $\mathcal{U}^c = \varnothing$.

$$\mathcal{U}^c \quad = \quad (\varnothing^c)^c \text{ por (s) (complemento del conjunto vacío)}$$

$$= \quad \varnothing \text{ por (g) (doble complemento)}$$

(u) Probaremos que $\varnothing \subset A$.
Por hipótesis sabemos que $A \subset \mathcal{U}$. Ahora

$$\begin{aligned} A \subset \mathcal{U} \quad &\Rightarrow \quad A^c \subset \mathcal{U} \text{ por Definición 1.23 (complemento de un conjunto)} \\ &\Rightarrow \quad \mathcal{U}^c \subset (A^c)^c \text{ por (l)} \\ &\Rightarrow \quad \varnothing \subset (A^c)^c \text{ por (t)} \\ &\Rightarrow \quad \varnothing \subset A \text{ por (g) (doble complemento)} \end{aligned}$$

■

1.7.7. Unión e intersección arbitraria de conjuntos

Definición 1.26
Si $\{A_i : i \in \mathcal{I}\}$ es una familia arbitraria de conjuntos indexados por el conjunto de índices $\mathcal{I}$, se suele escribir la unión de esta familia de la siguiente manera:

$$\bigcup_{i \in \mathcal{I}} A_i,$$

y la intersección como:

$$\bigcap_{i \in \mathcal{I}} A_i.$$

En ambos estamos usando la propiedad asociativa de la unión y de la intersección (ver Proposición 1.2-(d) y 1.2-(c)) para evitar los paréntesis.

Ejemplo 1.23
A manera de ejemplo, si $\mathcal{I} = \{1, \ldots, 10\}$, se suele escribir:

$$A_1 \cup \ldots \cup A_{10} = \bigcup_{i=1}^{10} A_i,$$

$$A_1 \cap \ldots \cap A_{10} = \bigcap_{i=1}^{10} A_i.$$

1.7.8. Producto cartesiano

Definición 1.27
Dos elementos dados en cierto orden forman un par ordenado. Tales elementos se representan entre paréntesis y separados por una coma. En general, si a y b son dos objetos, se define el par ordenado (a, b). De acuerdo a la definición: $(a, b) \neq (b, a)$ cuando $a \neq b$.

Ejemplo 1.24

(a) Un punto geográfico está determinado por las coordenadas latitud y longitud, por lo que se puede representar cualquier posición geográfica como un par ordenado (latitud, longitud). Por ejemplo, la localización de la FACENA es:

$$(-27.467203690669503, -58.78345102071762)\,.$$

(b) Una fecha del año está dada por el día y el mes, por lo que se puede representar como un par ordenado (día, mes).

Definición 1.28
Dados dos conjuntos A y B, el producto cartesiano entre A y B, denotado por $A \times B$, es el conjunto de todos los pares ordenados tales que el primer miembro del par ordenado es un elemento de A y el segundo miembro es un elemento de B. En el caso particular $A \times A$ el producto cartesiano se suele escribir como A^2. En símbolos:

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

Ejemplo 1.25
Consideremos que $A = \{a, b, c\}$ y $B = \{1, 2\}$. Entonces:

$$\begin{aligned} A \times B &= \{(a,1), (a,2), (b,1), (b,2), (c,1), (c,2)\}, \\ B \times A &= \{(1,a), (1,b), (1,c), (2,a), (2,b), (2,c)\}, \\ A^2 &= \{(a,a), (a,b), (a,c), (b,a), (b,b), (b,c), (c,a), (c,b), (c,c)\}, \\ B^2 &= \{(1,1), (1,2), (2,1), (2,2)\}. \end{aligned}$$

Definición 1.29
Dados $A_1, \ldots, A_n$ conjuntos, se define el producto cartesiano $\prod_{i=1}^{n} A_i$ como

$$\prod_{i=1}^{n} A_i = \{(a_1, \ldots, a_n) : a_i \in A_i, 1 \leqslant i \leqslant n\}.$$

Ejemplo 1.26
Consideremos que $A_1 = \{\alpha, \beta\}$, $A_2 = \{✠, \bigstar\}$ y $A_3 = \{0, a\}$. Entonces:

$$\begin{aligned} \prod_{i=1}^{3} A_i &= A_1 \times A_2 \times A_3 \\ &= \{(\alpha, ✠, 0), (\alpha, ✠, a), (\alpha, \bigstar, 0), (\alpha, \bigstar, a), (\beta, ✠, 0), (\beta, ✠, a), (\beta, \bigstar, 0), (\beta, \bigstar, a)\}. \end{aligned}$$

1.8. Funciones proposicionales

Definición 1.30
Una función proposicional es una proposición cuyo valor de verdad depende de una variable. A las funciones proposicionales se las representa con letras mayúsculas y entre paréntesis se coloca la variable. La variable podría también pertenecer a algún conjunto universal.

Veamos algunos ejemplos de funciones proposicionales.

Ejemplo 1.27
(a) $P(x)$: x es un animal.

(b) $P(x)$: x es argentino nativo o nacionalizado, donde x es una persona que vive en Argentina.

(c) $P(x)$: x está resfriado.

(d) $P(x)$: x es un número par, donde $x \in \mathbb{Z}$.

Cuando la variable se reemplaza por un objeto (se suele decir instanciación de la variable), la función proposicional asume un valor de verdad determinado. Algunas posibilidades de instanciación de la función proposicional de uno de los ejemplos anteriores pueden ser:

$$\begin{aligned} P(\text{perro}) &: \text{El perro es un animal.} \\ P(\text{flor}) &: \text{La flor es un animal.} \\ P(\text{elefante}) &: \text{El elefante es un animal.} \end{aligned}$$

1.9. Cuantificadores

Los cuantificadores nos permiten construir otras proposiciones a partir de funciones proposicionales, ya sea generalizando o particularizando.

Definición 1.31
El cuantificador existencial particulariza una función proposicional. Se representa simbólicamente como

$$\exists x \in A : P(x), \tag{1}$$

y se lee "existe x en A tal que cumple $P(x)$". Cuando uno dice "existe" está queriendo decir "existe al menos un ...", por lo que el significado exacto del cuantificador existencial es "existe al menos un x en A que satisface $P(x)$". Cuando el conjunto A es claro del contexto, podemos omitirlo en la expresión, quedando $\exists x : P(x)$.

En caso de querer expresar otra cosa, se aclarará explícitamente, por ejemplo, es usual escribir:

$$\exists! x \in A : P(x),$$

para expresar que existe un único x en A que satisface $P(x)$. Notar que hay una diferencia entre decir: "existe un perro negro" y "existe un único perro negro".

Ejemplo 1.28

(a) Si consideramos la función proposicional

$$P(x) : x \text{ es mayor que } 0,$$

donde $x \in \mathbb{R}$, el cuantificador existencial sería

$$\exists x \in \mathbb{R} : x \text{ es mayor que } 0.$$

(b) Si consideramos la función proposicional

$$P(x) : x \text{ es un número par},$$

donde $x \in \mathbb{Z}$, el cuantificador existencial sería

$$\exists x \in \mathbb{Z} : x \text{ es un número par}.$$

En este caso, como la paridad tiene sentido solamente en $\mathbb{Z}$, el conjunto donde se cuantifica puede omitirse, quedando

$$\exists x : x \text{ es un número par},$$

Definición 1.32
El cuantificador universal generaliza una función proposicional. Se representa simbólicamente como

$$\forall x \in A, P(x), \tag{2}$$

y se lee "para cada x en A se cumple $P(x)$". Cuando uno dice "para cada" está queriendo decir "para todo ...". Cuando el conjunto A es claro del contexto, podemos omitirlo en la expresión, quedando $\forall x, P(x)$.

Ejemplo 1.29

(a) Si consideramos la función proposicional

$$P(x) : x \text{ es menor que } 0,$$

donde $x \in \mathbb{R}$, el cuantificador universal sería

$$\forall x \in \mathbb{R}, x \text{ es menor que } 0.$$

(b) Si consideramos la función proposicional

$$P(x) : x \text{ es un número impar},$$

donde $x \in \mathbb{Z}$, el cuantificador universal sería

$$\forall x \in \mathbb{Z}, x \text{ es un número impar}.$$

En este caso, como la paridad tiene sentido solamente en $\mathbb{Z}$, el conjunto donde se cuantifica puede omitirse, quedando

$$\forall x, x \text{ es un número impar},$$

(c) De acuerdo a la Definición 1.19, la definición de $A \subset B$ quedaría expresada de la siguiente manera:

$$\forall x, x \in A \Rightarrow x \in B.$$

Definición 1.33

(a) Diremos que la proposición $\exists x \in A : P(x)$ es verdadera si y sólo si $P(a)$ es verdadera para algún $a \in A$. Luego, para ver que la proposición $\exists x \in A : P(x)$ es verdadera, basta encontrar un $a \in A$ que satisfaga la propiedad requerida. En caso de querer demostrar que la proposición es falsa, habrá que ver que $P(x)$ es falsa para cada $x \in A$.

(b) Diremos que la proposición $\forall x \in A, P(x)$ es verdadera si y sólo si $P(a)$ es verdadera para cada $a \in A$. Luego, para ver que la proposición $\forall x \in A, P(x)$ es verdadera, debemos chequear que $P(a)$ es verdadera para todas las instancias posibles. En caso de querer demostrar que la proposición es falsa, habrá que hallar algún $a \in A$ que haga que $P(a)$ sea falsa (esto se llama hallar un contraejemplo).

De acuerdo a la Definición 1.33, para verificar la veracidad o falsedad de una proposición cuantificada, podemos chequear la Tabla 1.9

PROPOSICIÓN	VERDADERA	FALSA
$\exists x \in A : P(x)$	hallar **un** $x \in A$ que **cumpla** $P(x)$ (requiere ejemplo)	mostrar que **cada** $x \in A$ **no cumple** $P(x)$ (requiere demostración)
$\forall x \in A, P(x)$	mostrar que **cada** $x \in A$ **cumple** $P(x)$ (requiere demostración)	hallar **un** $x \in A$ que **no cumpla** $P(x)$ (requiere contraejemplo)

Tabla 1: Cómo demostrar la veracidad o falsedad de una proposición cuantificada.

Ejemplo 1.30
Consideremos las siguientes proposiciones cuantificadas

(a) $\exists x \in \mathbb{N} : x > 1$.

V, pues se cumple que $2 > 1$ es V.

(b) $\exists x \in \mathbb{N} : x < 0$.

F, pues no hay ningún $x \in \mathbb{N}$ que sea negativo.

(c) $\forall x \in \mathbb{N}, x > 0$.

V, pues cada uno de los números naturales (1, 2, 3, ...) es positivo.

(d) $\forall x \in \mathbb{R}, x < 0$.

F, pues el 1 no es un número negativo (éste es el contraejemplo). Notar que la proposición es falsa aún cuando la propiedad $x < 0$ se satisfaga para muchos elementos de $\mathbb{R}$.

Definición 1.34

(a) Negar que existe un x en A que cumpla la propiedad $P(x)$ equivale a decir que ningún $x \in A$ satisface $P(x)$, es decir que todos los elementos x de A no cumplen con la propiedad $P(x)$. Por lo tanto:

$$\neg\left(\exists x \in A : P(x)\right) \equiv \forall x \in A, \neg P(x). \tag{3}$$

(b) Negar que para cada x en A se cumple la propiedad $P(x)$ equivale a decir que al menos un $x \in A$ no cumple con la propiedad $P(x)$. Por lo tanto:

$$\neg\left(\forall x \in A, P(x)\right) \equiv \exists x \in A : \neg P(x). \tag{4}$$

Ejemplo 1.31

(a) p : "todos los planetas están deshabitados"
$\neg p$: "existe un planeta que está habitado"

(b) p : "existe un perro de color negro"
$\neg p$: "todos los perros son de un color diferente al negro"

(c) p : $\forall x \in \mathbb{R}, x^2 + 1 < x$
$\neg p$: $\exists x \in \mathbb{R} : x^2 + 1 \geqslant x$

(d) p : $\exists x \in \mathbb{R} : x^2 + x^3 = 1$
$\neg p$: $\forall x \in \mathbb{R}, x^2 + x^3 \neq 1$

(e) Si $A = \varnothing$ entonces $\exists x \in A : P(x)$ es falsa, pues no hay elementos en el conjunto A.

(f) Si $A = \varnothing$ entonces $\forall x \in A, P(x)$ es verdadera.

Notar que debido a la Definición 1.34-(b), la negación de la proposición en cuestión es:

$$\neg\left(\forall x \in A, P(x)\right) \equiv \exists x \in A, \neg P(x)$$

Pero esta última proposición es falsa pues no hay ningún elemento $x \in A$ que cumpla $\neg P(x)$ ya que $A = \varnothing$. Por lo tanto la proposición del enunciado es verdadera.

Hemos visto a través de diferentes ejemplos que se usa la letra x para representar números u objetos. Esta elección es totalmente arbitraria, por lo que se puede reemplazar la variable por otras letras, siempre y cuando se haga de manera consistente. Esto se suele denominar renombre de variables.

Ejemplo 1.32

(a) $\forall x \in \mathbb{R}, x^2 + 1 > 0 \equiv \forall w \in \mathbb{R}, w^2 + 1 > 0$.

(b) $\exists x \in \mathbb{R}, x + 1 = 0 \equiv \exists z \in \mathbb{R}, z + 1 = 0$.

1.10. Partes de un conjunto

Definición 1.35
Dado un conjunto A, se llama conjunto de partes de A, denotado por $\mathcal{P}(A)$, al conjunto formado por todos los subconjuntos de A. En símbolos:

$$\mathcal{P}(A) = \{B : B \subset A\}.$$

Notar que los elementos de $\mathcal{P}(A)$ no son elementos de A, sino que son subconjuntos de A.

Ejemplo 1.33

(a) Si $A = \varnothing$, entonces

$$\mathcal{P}(A) = \Big\{\varnothing\Big\}.$$

(b) Si $A = \{\star\}$, entonces

$$\mathcal{P}(A) = \Big\{\varnothing, \{\star\}\Big\}.$$

(c) Si $A = \{\alpha, \beta\}$, entonces

$$\mathcal{P}(A) = \Big\{\varnothing, \{\alpha\}, \{\beta\}, \{\alpha, \beta\}\Big\}.$$

(d) Si $A = \{1, 2, 3\}$, entonces

$$\mathcal{P}(A) = \Big\{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\Big\}.$$

(e) Si $A = \{a, b, c, d\}$, entonces

$$\begin{aligned}\mathcal{P}(A) = \Big\{&\varnothing, \{a\}, \{b\}, \{c\}, \{d\}, \{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}, \{a, b, c\},\\ &\{a, b, d\}, \{a, c, d\}, \{b, c, d\}, \{a, b, c, d\}\Big\}.\end{aligned}$$

Aunque todavía no estamos en condiciones de demostrarlo, se puede ver que si el conjunto A tiene n elementos, entonces el conjunto de partes de A tiene 2^n elementos.

Proposición 1.3
Sean A y B conjuntos. Entonces se satisfacen las siguientes propiedades:

(a) $A \subset B \Rightarrow \mathcal{P}(A) \subset \mathcal{P}(B)$.

(b) $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.

(c) $\mathcal{P}(A) \cup \mathcal{P}(B) \subset \mathcal{P}(A \cup B)$.

Demostración.
(a) Probaremos que $A \subset B \Rightarrow \mathcal{P}(A) \subset \mathcal{P}(B)$.

$$\begin{aligned}X \in \mathcal{P}(A) &\Rightarrow X \subset A \text{ por Definición 1.35 (partes de un conjunto)}\\ &\Rightarrow X \subset B \text{ pues } A \subset B\\ &\Rightarrow X \in \mathcal{P}(B) \text{ por Definición 1.35 (partes de un conjunto)}\end{aligned}$$

(b) Probaremos que $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.

$$X \in \mathcal{P}(A \cap B) \Leftrightarrow X \subset A \cap B \text{ por Definición 1.35 (partes de un conjunto)}$$

$$\begin{aligned}
&\Leftrightarrow\ X \subset A \text{ y } X \subset B \text{ por Definición 1.22 (intersección de conjuntos)}\\
&\Leftrightarrow\ X \in \mathcal{P}(A) \text{ y } X \in \mathcal{P}(B) \text{ por Definición 1.35 (partes de un conjunto)}\\
&\Leftrightarrow\ X \in \mathcal{P}(A) \cap \mathcal{P}(B) \text{ por Definición 1.22 (intersección de conjuntos)}
\end{aligned}$$

(c) Probaremos que $\mathcal{P}(A) \cup \mathcal{P}(B) \subset \mathcal{P}(A \cup B)$.

$$\begin{aligned}
X \in \mathcal{P}(A) \cup \mathcal{P}(B) &\Rightarrow X \in \mathcal{P}(A) \text{ o } X \in \mathcal{P}(B) \text{ por Definición 1.21 (unión de conjuntos)}\\
&\Rightarrow X \subset A \text{ o } X \subset B \text{ por Definición 1.35 (partes de un conjunto)}\\
&\Rightarrow X \subset A \cup B \text{ por Definición 1.21 (unión de conjuntos)}\\
&\Rightarrow X \in \mathcal{P}(A \cup B) \text{ por Definición 1.35 (partes de un conjunto)}
\end{aligned}$$

■

1.11. Partición de un conjunto

Definición 1.36
Dado un conjunto A, diremos que la familia $\{A_i : i \in \mathcal{I}\}$ es una partición de A si:

$$\begin{aligned}
A &= \bigcup_{i\in\mathcal{I}} A_i,\\
A_i &\neq \varnothing, \quad \forall i \in \mathcal{I},\\
A_i \cap A_j &= \varnothing, \quad \forall i, j \in \mathcal{I} \text{ tal que } i \neq j.
\end{aligned}$$

Ejemplo 1.34
Consideremos el siguiente conjunto:

$$A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}.$$

Si definimos:

$$\begin{aligned}
A_1 &= \{1, 3, 5\},\\
A_2 &= \{2, 4, 6\},\\
A_3 &= \{7, 9\},\\
A_4 &= \{8, 10\}.
\end{aligned}$$

la familia $\{A_1, A_2, A_3, A_4\}$ define una partición de A pues:

$$\begin{aligned}
A &= A_1 \cup A_2 \cup A_3 \cup A_4,\\
A_1 &\neq \varnothing,\\
A_2 &\neq \varnothing,\\
A_3 &\neq \varnothing,\\
A_4 &\neq \varnothing,\\
A_1 \cap A_2 &= \varnothing,\\
A_1 \cap A_3 &= \varnothing,\\
A_1 \cap A_4 &= \varnothing,\\
A_2 \cap A_3 &= \varnothing,\\
A_2 \cap A_4 &= \varnothing,\\
A_3 \cap A_4 &= \varnothing.
\end{aligned}$$

2. RELACIONES

2.1. Concepto de relación

Definición 2.1
Dados dos conjuntos A y B, una relación $\mathcal{R}$ entre A y B es un subconjunto del producto cartesiano $A \times B$.

Si un par ordenado (a, b) está en $\mathcal{R}$, se suele decir que los elementos a y b están relacionados, y se denota por $a\mathcal{R}b$ o $a \sim b$.

Como todos los conjuntos, una relación puede ser definida ya sea por extensión o por comprensión.

Ejemplo 2.1

(a) Si $A = \{1, 2, 3\}$ y $B = \{a, b\}$, podríamos considerar las siguientes relaciones:

$$\begin{aligned} \mathcal{R} &= \{(1, a), (2, b), (3, b)\}, \quad \text{notar que } \mathcal{R} \subsetneq A \times B, \\ \mathcal{S} &= \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}, \quad \text{notar que } \mathcal{S} \text{ coincide con } A \times B, \\ \mathcal{T} &= \varnothing. \end{aligned}$$

(b) Sea $A = \{x : x \text{ es un ciudadano de Corrientes}\}$ y $\mathcal{R} \subset A \times A$ definida por

$$\mathcal{R} = \{(x, y) : x \text{ es padre de } y\}.$$

Es claro que no todo par de ciudadanos estará relacionado. Por ejemplo, hay personas que no tienen hijos, por lo que no estarán relacionados con nadie. Además habrá personas que estarán relacionadas con más de una persona (por ejemplo, una persona que sea el papá de dos hijos o más).

(c) Sea A un conjunto y $P = \mathcal{P}(A)$ el conjunto de partes de A. Sea $\mathcal{R} \subset P \times P$ definida por

$$\mathcal{R} = \{(B, C) : B \subset C\}.$$

En este caso el conjunto vacío está relacionado con todos los elementos de P (recordar Proposición 1.2-(u)). Por otra parte, todos los elementos de P estarán relacionados a A. Sin embargo habrá conjuntos que no estén relacionados [4]

(d) Sean $A = \{x : x \text{ es un ciudadano de Corrientes}\}$, $B = \{x : x \text{ es una carrera de la UNNE}\}$, y $\mathcal{R} \subset A \times B$ definida por

$$\mathcal{R} = \{(x, y) : x \text{ estudia la carrera } y\}.$$

Notar que los estudiantes de la UNNE están relacionados a alguna carrera. Sin embargo, hay personas que ya se recibieron, o no pudieron estudiar ninguna carrera universitaria de la UNNE, o estudian en otra universidad, con lo cual ellos no estarán relacionados a ninguna carrera de la UNNE.

2.2. Representación gráfica de relaciones

Consideremos una relación $\mathcal{R} \subset A \times B$. Se puede representar la relación utilizando diagramas de Venn:

- graficando los conjuntos A y B con diagramas de Venn,

[4] Considerar el siguiente ejemplo: $B = \{1, 2, 3\}$, $C = \{1, 2, 4\}$. Es claro que $B \not\subset C$ y $C \not\subset B$.

- uniendo con una flecha los elementos que están relacionados.

Ejemplo 2.2
Si $A = \{a, b, c\}$ y $B = \{\alpha, \beta\}$, consideremos la siguiente relación:

$$\mathcal{R} = \{(a, \beta), (c, \alpha), (c, \beta)\}.$$

Luego la representación gráfica mediante diagramas de Venn puede verse en la Figura 2.1.

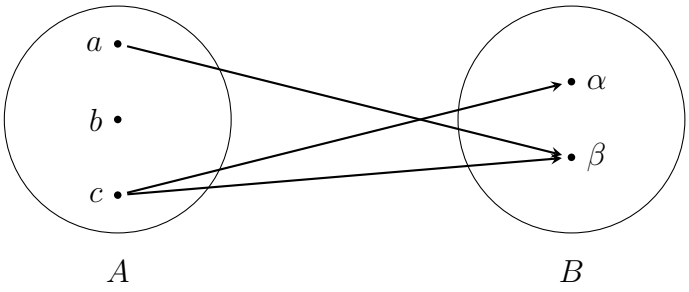


Figura 2.1: Representación de relaciones mediante diagramas de Venn.

Otra manera de graficar una relación es mediante una representación cartesiana:

- dibujando dos rectas perpendiculares,
- ubicando esquemáticamente los elementos del conjunto A en el eje horizontal, y los elementos de B en el eje vertical,
- marcando un punto en aquellos elementos pertenecientes a la relación.

Ejemplo 2.3
Si $A = \{a, b, c, d\}$, $B = \{1, 2, 3\}$, consideremos la siguiente relación:

$$\mathcal{R} = \{(a, 1), (a, 3), (b, 1), (b, 2), (c, 3)\}.$$

Luego la representación cartesiana puede verse en la Figura 2.2.

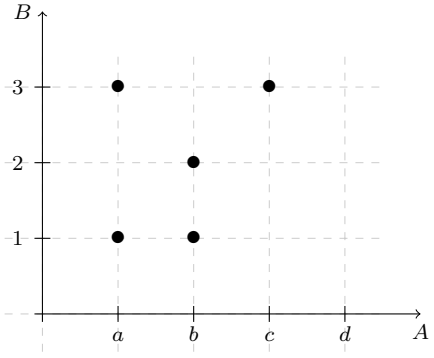


Figura 2.2: Representación cartesiana de relaciones.

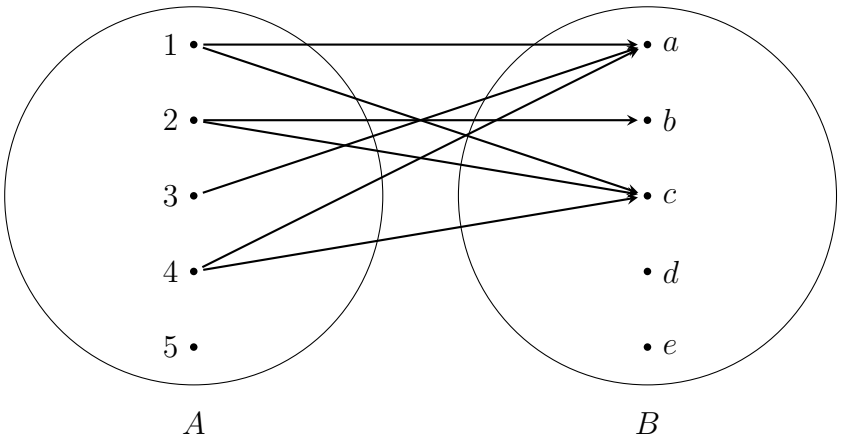


Figura 2.3: Ejemplo para motivar la definición de dominio, imagen e inversa de una relación.

2.3. Dominio, imagen y relación inversa

Consideremos el siguiente ejemplo. Sean $A = \{1, 2, 3, 4, 5\}$, $B = \{a, b, c, d, e\}$ y

$$\mathcal{R} = \{(1, a), (1, c), (2, b), (2, c), (3, a), (4, a), (4, c)\}.$$

Una representación mediante diagramas de Venn puede verse en la Figura 2.3.

Llamaremos dominio de la relación al conjunto formado por las primeras componentes de los pares ordenados definidos por la relación (o equivalentemente aquellos elementos de donde salen las flechas). En el ejemplo, el dominio está formado por los elementos: 1, 2, 3, 4.

Llamaremos imagen de la relación al conjunto formado por las segundas componentes de los pares ordenados definidos por la relación (o equivalentemente aquellos elementos donde llegan las flechas). En el ejemplo, la imagen está formada por los elementos: a, b, c.

La relación inversa se define como un subconjunto de $B \times A$ cuyos elementos son pares ordenados "invertidos". En el ejemplo, la relación inversa está compuesta por los pares: $(a, 1)$, $(c, 1)$, $(b, 2)$, $(c, 2)$, $(a, 3)$, $(a, 4)$, $(c, 4)$.

A continuación vamos a formalizar estos conceptos.

Definición 2.2
Sean A y B dos conjuntos y $\mathcal{R}$ una relación entre A y B.

(a) El dominio de la relación $\mathcal{R}$, denotado por $\mathrm{Dom}(\mathcal{R})$*, es el subconjunto de elementos de A que están relacionados con algún elemento de B, es decir,*

$$\mathrm{Dom}(\mathcal{R}) = \{a \in A : \exists b \in B \text{ tal que } (a, b) \in \mathcal{R}\}.$$

(b) La imagen de la relación $\mathcal{R}$, denotado por $\mathrm{Im}(\mathcal{R})$*, es el subconjunto de elementos de B tales que algún elemento de A está relacionado a ellos, es decir,*

$$\mathrm{Im}(\mathcal{R}) = \{b \in B : \exists a \in A \text{ tal que } (a, b) \in \mathcal{R}\}.$$

(c) La relación inversa de $\mathcal{R}$, denotada por $\mathcal{R}^{-1}$, es una nueva relación entre B y A (o sea, un subconjunto de $B \times A$) definida por:

$$\mathcal{R}^{-1} = \{(b, a) : (a, b) \in \mathcal{R}\}.$$

De este modo, para el ejemplo anterior quedaría:

$$\begin{aligned} \mathrm{Dom}(\mathcal{R}) &= \{1, 2, 3, 4\}, \\ \mathrm{Im}(\mathcal{R}) &= \{a, b, c\}, \\ \mathcal{R}^{-1} &= \{(a, 1), (c, 1), (b, 2), (c, 2), (a, 3), (a, 4), (c, 4)\}. \end{aligned}$$

2.4. Composición de relaciones

Antes de dar la definición de composición de relaciones veamos un ejemplo. Consideremos

$$A = \{-1, 0, 2\}, \quad B = \{1, 3\}, \quad C = \{a, b, c\},$$

y las relaciones $\mathcal{R} \subset A \times B$ y $\mathcal{S} \subset B \times C$ definidas por:

$$\begin{aligned} \mathcal{R} &= \{(-1, 1), (2, 1)\}, \\ \mathcal{S} &= \{(1, a), (3, b)\}. \end{aligned}$$

Se pueden representar ambas relaciones de manera simultánea como muestra la Figura 2.4.

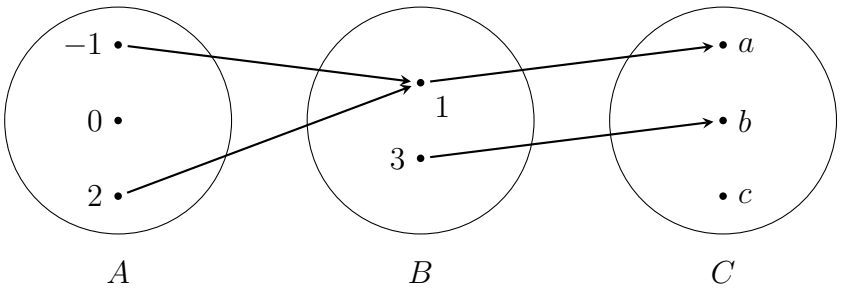


Figura 2.4: Ejemplo de composición de relaciones.

Se podría definir una relación entre los conjuntos A y C siguiendo "el camino de las flechas". En este sentido, el elemento -1 queda relacionado al elemento a pues hay una flecha que sale de -1, pasa por algún elemento de B (el 1) y sigue su camino hasta a. Análogamente el elemento $2 \in A$ está relacionado a $a \in C$.

A continuación vamos a formalizar este concepto.

Definición 2.3
Sean A, B y C conjuntos. Si tenemos dos relaciones $\mathcal{R} \subset A \times B$ y $\mathcal{S} \subset B \times C$, se puede definir una nueva relación entre A y C llamada la composición entre $\mathcal{R}$ y $\mathcal{S}$ denotada por $\mathcal{S} \circ \mathcal{R}$ (se lee "$\mathcal{S}$ o $\mathcal{R}$"):

$$\mathcal{S} \circ \mathcal{R} = \{(a, c) : \exists b \in B \text{ tal que } (a, b) \in \mathcal{R} \text{ y } (b, c) \in \mathcal{S}\}.$$

De este modo, para el ejemplo anterior quedaría:

$$\mathcal{S} \circ \mathcal{R} = \{(-1, a), (2, a)\}.$$

Proposición 2.1
Supongamos que se tienen conjuntos A, B, C y D, y relaciones $\mathcal{R} \subset A \times B$, $\mathcal{S} \subset B \times C$ y $\mathcal{T} \subset C \times D$. Se puede ver que se satisfacen las siguientes propìedades:

(a) Asociatividad de la composición:

$$(\mathcal{T} \circ \mathcal{S}) \circ \mathcal{R} = \mathcal{T} \circ (\mathcal{S} \circ \mathcal{R}).$$

(b) Inversa de la composición:

$$(\mathcal{S} \circ \mathcal{R})^{-1} = \mathcal{R}^{-1} \circ \mathcal{S}^{-1}.$$

Demostración.
(a) Probaremos que se cumple la asociatividad de la composición. En realidad debemos probar una igualdad de conjuntos:

$$(a, d) \in (\mathcal{T} \circ \mathcal{S}) \circ \mathcal{R} \iff \exists b \in B : (a, b) \in \mathcal{R} \wedge (b, d) \in \mathcal{T} \circ \mathcal{S}$$

$$
\begin{aligned}
& \text{por Definición 2.3 (composición de relaciones)} \\
\Leftrightarrow\ & \exists b \in B, \exists c \in C : (a,b) \in \mathcal{R} \wedge [(b,c) \in \mathcal{S} \wedge (c,d) \in \mathcal{T}] \\
& \text{por Definición 2.3 (composición de relaciones)} \\
\Leftrightarrow\ & \exists b \in B, \exists c \in C : [(a,b) \in \mathcal{R} \wedge (b,c) \in \mathcal{S}] \wedge (c,d) \in \mathcal{T} \\
& \text{por Proposición 1.1-(c) (asociatividad de conjunción)} \\
\Leftrightarrow\ & \exists c \in C : (a,c) \in \mathcal{S} \circ \mathcal{R} \wedge (c,d) \in \mathcal{T} \\
& \text{por Definición 2.3 (composición de relaciones)} \\
\Leftrightarrow\ & (a,d) \in \mathcal{T} \circ (\mathcal{S} \circ \mathcal{R}) \\
& \text{por Definición 2.3 (composición de relaciones)}
\end{aligned}
$$

(b) Veremos ahora una fórmula para la relación inversa de una composición. Al igual que antes hay que chequear una igualdad de conjuntos:

$$
\begin{aligned}
(c,a) \in (\mathcal{S} \circ \mathcal{R})^{-1} \ \Leftrightarrow\ & (a,c) \in \mathcal{S} \circ \mathcal{R} \text{ por Definición 2.2-(c) (relación inversa)} \\
\Leftrightarrow\ & \exists b \in B : (a,b) \in \mathcal{R} \wedge (b,c) \in \mathcal{S} \text{ por Definición 2.3 (composición de relaciones)} \\
\Leftrightarrow\ & \exists b \in B : (b,a) \in \mathcal{R}^{-1} \wedge (c,b) \in \mathcal{S}^{-1} \text{ por Definición 2.2-(c) (relación inversa)} \\
\Leftrightarrow\ & \exists b \in B : (c,b) \in \mathcal{S}^{-1} \wedge (b,a) \in \mathcal{R}^{-1} \\
& \text{por Proposición 1.1-(a) (conmutativa de la conjunción)} \\
\Leftrightarrow\ & (c,a) \in \mathcal{R}^{-1} \circ \mathcal{S}^{-1} \text{ por Definición 2.3 (composición de relaciones)}
\end{aligned}
$$

Esto concluye la demostración. ■

2.5. Clasificación de las relaciones en un conjunto

Definición 2.4

Supongamos que tenemos una relación $\mathcal{R} \subset A \times A$ (es decir, es una relación entre elementos de un mismo conjunto). Diremos que $\mathcal{R}$ es:

(a) Reflexiva:

$$\forall a \in A, \quad (a,a) \in \mathcal{R}.$$

(b) Arreflexiva:

$$\forall a \in A, \quad (a,a) \notin \mathcal{R}.$$

(c) Simétrica:

$$\forall a,b \in A, \quad (a,b) \in \mathcal{R} \Rightarrow (b,a) \in \mathcal{R}.$$

(d) Asimétrica:

$$\forall a,b \in A, \quad (a,b) \in \mathcal{R} \Rightarrow (b,a) \notin \mathcal{R}.$$

(e) Antisimétrica:

$$\forall a,b \in A, \quad a \neq b \wedge (a,b) \in \mathcal{R} \Rightarrow (b,a) \notin \mathcal{R}.$$

Las siguientes proposiciones son equivalentes a la definición de antisimetría [5]*:*

$$(e^*) \quad \forall a,b \in A, \quad a \neq b \Rightarrow (a,b) \notin \mathcal{R} \vee (b,a) \notin \mathcal{R},$$

[5] Considerando $p : a = b$, $q : (a,b) \in \mathcal{R}$ y $r : (b,a) \in \mathcal{R}$ notemos que

$$\neg p \wedge q \Rightarrow \neg r \equiv \neg p \Rightarrow \neg q \vee \neg r \equiv q \wedge r \Rightarrow p$$

simplemente confeccionando las tablas de verdad

$$(e^{**}) \quad \forall a, b \in A, \qquad (a, b) \in \mathcal{R} \wedge (b, a) \in \mathcal{R} \Rightarrow a = b.$$

(f) Transitiva:

$$\forall a, b, c \in A, \quad (a, b) \in \mathcal{R} \wedge (b, c) \in \mathcal{R} \Rightarrow (a, c) \in \mathcal{R}.$$

A continuación veremos una serie de ejemplos y haremos algunos comentarios para comprender la definición.

Ejemplo 2.4
A continuación consideremos el conjunto $A = \{1, 2, 3, 4\}$ y una relación $\mathcal{R} \subset A \times A$.

(a) Si $\mathcal{R} = \{(1, 2), (4, 4), (2, 2), (2, 1), (1, 1), (3, 3)\}$ entonces $\mathcal{R}$ es reflexiva, pues

$$\begin{aligned} (1,1) &\in \mathcal{R}, \\ (2,2) &\in \mathcal{R}, \\ (3,3) &\in \mathcal{R}, \\ (4,4) &\in \mathcal{R}, \end{aligned}$$

es decir, $(a, a) \in \mathcal{R}$ para cada $a \in A$.

(b) Si $\mathcal{R} = \{(1, 2), (2, 2), (2, 1), (1, 1), (3, 3)\}$ entonces $\mathcal{R}$ no es reflexiva, pues $(4, 4) \notin \mathcal{R}$. Es decir,

$$\exists a \in A : (a, a) \notin A,$$

que es la negación de la definición de reflexividad.

(c) Si $\mathcal{R} = \{(1, 2), (2, 1), (1, 3), (3, 4)\}$ entonces $\mathcal{R}$ es arreflexiva, pues

$$\begin{aligned} (1,1) &\notin \mathcal{R}, \\ (2,2) &\notin \mathcal{R}, \\ (3,3) &\notin \mathcal{R}, \\ (4,4) &\notin \mathcal{R}, \end{aligned}$$

es decir, $(a, a) \notin \mathcal{R}$ para cada $a \in A$.

(d) Si $\mathcal{R} = \{(1, 2), (2, 2), (2, 1), (3, 4)\}$ entonces $\mathcal{R}$ no es arreflexiva, pues $(2, 2) \in \mathcal{R}$. Es decir,

$$\exists a \in A : (a, a) \in A,$$

que es la negación de la definición de arreflexividad.

(e) La definición de una relación simétrica nos dice que si hay un par (a, b) en la relación, entonces el par (b, a) también está.
Si $\mathcal{R} = \{(1, 2), (2, 1), (1, 3), (1, 1), (3, 1)\}$ entonces $\mathcal{R}$ es simétrica, pues

$$\begin{aligned} &(1,2) \in \mathcal{R} \Rightarrow (2,1) \in \mathcal{R} \text{ es } V, && \text{pues } (1,2), (2,1) \in \mathcal{R} \\ &(2,1) \in \mathcal{R} \Rightarrow (1,2) \in \mathcal{R} \text{ es } V, && \text{pues } (1,2), (2,1) \in \mathcal{R} \\ &(1,3) \in \mathcal{R} \Rightarrow (3,1) \in \mathcal{R} \text{ es } V, && \text{pues } (1,3), (3,1) \in \mathcal{R} \\ &(1,1) \in \mathcal{R} \Rightarrow (1,1) \in \mathcal{R} \text{ es } V, && \text{pues } (1,1) \in \mathcal{R} \\ &(3,1) \in \mathcal{R} \Rightarrow (1,3) \in \mathcal{R} \text{ es } V, && \text{pues } (3,1), (1,3) \in \mathcal{R} \end{aligned}$$

es decir,

$$\forall a, b \in A, (a, b) \in \mathcal{R} \Rightarrow (b, a) \in \mathcal{R}.$$

(f) Si $\mathcal{R} = \{(1,2),(1,3),(1,1),(3,1)\}$ entonces $\mathcal{R}$ no es simétrica, pues $(1,2) \in \mathcal{R}$ pero $(2,1) \notin \mathcal{R}$. Es decir,

$$\exists a, b \in A : (a,b) \in \mathcal{R} \text{ y } (b,a) \notin \mathcal{R},$$

que es la negación de la definición de simetría (ver Proposición 1.1-(n)).

(g) La definición de una relación asimétrica nos dice que si hay un par (a,b) en la relación, entonces el par (b,a) no debe estar. Notar que la definición de una relación asimétrica no es la negación de la definición de una relación simétrica. Además se desprende de la definición que una relación asimétrica no tiene como elementos a pares de la forma (a,a), por lo cual una relación asimétrica es en particular arreflexiva.

Si $\mathcal{R} = \{(1,2),(1,3),(3,2),(2,4)\}$ entonces $\mathcal{R}$ es asimétrica, pues

$$\begin{aligned}
&(1,2) \in \mathcal{R} \Rightarrow (2,1) \notin \mathcal{R} \text{ es } V, && \text{pues } (1,2) \in \mathcal{R} \text{ y } (2,1) \notin \mathcal{R} \\
&(1,3) \in \mathcal{R} \Rightarrow (3,1) \notin \mathcal{R} \text{ es } V, && \text{pues } (1,3) \in \mathcal{R} \text{ y } (3,1) \notin \mathcal{R} \\
&(3,2) \in \mathcal{R} \Rightarrow (2,3) \notin \mathcal{R} \text{ es } V, && \text{pues } (3,2) \in \mathcal{R} \text{ y } (2,3) \notin \mathcal{R} \\
&(2,4) \in \mathcal{R} \Rightarrow (4,2) \notin \mathcal{R} \text{ es } V, && \text{pues } (2,4) \in \mathcal{R} \text{ y } (4,2) \notin \mathcal{R}
\end{aligned}$$

es decir,

$$\forall a, b \in A, (a,b) \in \mathcal{R} \Rightarrow (b,a) \notin \mathcal{R}.$$

(h) Si $\mathcal{R} = \{(1,2),(2,1),(1,1),(3,1)\}$ entonces $\mathcal{R}$ no es asimétrica, pues $(1,2) \in \mathcal{R}$ y $(2,1) \in \mathcal{R}$. Es decir,

$$\exists a, b \in A : (a,b) \in \mathcal{R} \text{ y } (b,a) \in \mathcal{R},$$

que es la negación de la definición de asimetría (ver Proposición 1.1-(n)).

Otra razón por la que $\mathcal{R}$ no es asimétrica es que $(1,1) \in \mathcal{R}$ ya que la proposición $(1,1) \in \mathcal{R} \Rightarrow (1,1) \notin \mathcal{R}$ es F.

(i) La definición de una relación antisimétrica nos dice que si hay un par (a,b) en la relación con $a \neq b$, entonces el par (b,a) no debe estar. Se desprende de la definición que una relación antisimétrica podría tener como elementos a pares de la forma (a,a).

Si $\mathcal{R} = \{(1,2),(1,3),(1,1),(2,4)\}$ entonces $\mathcal{R}$ es antisimétrica, pues

$$\begin{aligned}
&1 \neq 2 \wedge (1,2) \in \mathcal{R} \Rightarrow (2,1) \notin \mathcal{R} \text{ es } V, && \text{pues } (1,2) \in \mathcal{R} \text{ pero } (2,1) \notin \mathcal{R} \\
&1 \neq 3 \wedge (1,3) \in \mathcal{R} \Rightarrow (3,1) \notin \mathcal{R} \text{ es } V, && \text{pues } (1,3) \in \mathcal{R} \text{ pero } (3,1) \notin \mathcal{R} \\
&2 \neq 4 \wedge (2,4) \in \mathcal{R} \Rightarrow (4,2) \notin \mathcal{R} \text{ es } V, && \text{pues } (2,4) \in \mathcal{R} \text{ pero } (4,2) \notin \mathcal{R}
\end{aligned}$$

es decir,

$$\forall a, b \in A, a \neq b \wedge (a,b) \in \mathcal{R} \Rightarrow (b,a) \notin \mathcal{R}.$$

(j) Si $\mathcal{R} = \{(1,2),(2,1),(1,1),(3,1)\}$ entonces $\mathcal{R}$ no es antisimétrica, pues $1 \neq 2$, $(1,2) \in \mathcal{R}$ y $(2,1) \in \mathcal{R}$. Es decir,

$$\exists a, b \in A : a \neq b, (a,b) \in \mathcal{R} \text{ y } (b,a) \in \mathcal{R},$$

que es la negación de la definición de antisimetría (ver Proposición 1.1-(n)).

(k) Si $\mathcal{R} = \{(1,2),(2,3),(1,1),(1,3)\}$ entonces $\mathcal{R}$ es transitiva, pues

$$\begin{aligned}
&(1,2) \in \mathcal{R} \wedge (2,3) \in \mathcal{R} \Rightarrow (1,3) \in \mathcal{R} \text{ es } V, && \text{pues } (1,2) \in \mathcal{R}, (2,3) \in \mathcal{R} \text{ y } (1,3) \in \mathcal{R} \\
&(1,1) \in \mathcal{R} \wedge (1,2) \in \mathcal{R} \Rightarrow (1,2) \in \mathcal{R} \text{ es } V, && \text{pues } (1,1) \in \mathcal{R} \text{ y } (1,2) \in \mathcal{R} \\
&(1,1) \in \mathcal{R} \wedge (1,1) \in \mathcal{R} \Rightarrow (1,1) \in \mathcal{R} \text{ es } V, && \text{pues } (1,1) \in \mathcal{R}
\end{aligned}$$

$$(1,1) \in \mathcal{R} \wedge (1,3) \in \mathcal{R} \Rightarrow (1,3) \in \mathcal{R} \text{ es } V, \qquad \text{pues } (1,1) \in \mathcal{R} \text{ y } (1,3) \in \mathcal{R}$$

es decir,

$$\forall a, b, c \in A, (a,b) \in \mathcal{R} \wedge (b,c) \in \mathcal{R} \Rightarrow (a,c) \in \mathcal{R}.$$

(l) Si $\mathcal{R} = \{(1,2), (2,1), (3,1)\}$ entonces $\mathcal{R}$ no es transitiva, pues $(1,2) \in \mathcal{R}$, $(2,1) \in \mathcal{R}$ y $(1,1) \notin \mathcal{R}$. Es decir,

$$\exists a, b, c \in A : (a,b) \in \mathcal{R}, (b,c) \in \mathcal{R} \text{ y } (a,c) \notin \mathcal{R},$$

que es la negación de la definición de transitividad (ver Proposición 1.1-(n)).

2.6. Relaciones de equivalencia

Definición 2.5
Sea A un conjunto y $\mathcal{R} \subset A \times A$ una relación. Diremos que $\mathcal{R}$ es una relación de equivalencia si es reflexiva, simétrica y transitiva.

A continuación veremos un ejemplo que sugerirá un resultado muy importante sobre relaciones de equivalencia.

Ejemplo 2.5
Consideremos $A = \{1,2,3,4,5\}$ y

$$\mathcal{R} = \{(1,1), (1,2), (2,1), (2,2), (3,3), (4,4), (4,5), (5,4), (5,5)\}.$$

Se puede ver que $\mathcal{R}$ es reflexiva, pues se observa que

$$\begin{array}{ll} (1,1) \in \mathcal{R}, & (2,2) \in \mathcal{R}, \\ (3,3) \in \mathcal{R}, & (4,4) \in \mathcal{R}, \\ (5,5) \in \mathcal{R}, & \end{array}$$

es decir, $\forall a \in A, (a,a) \in \mathcal{R}$.

Además se puede comprobar que $\mathcal{R}$ es simétrica, pues

$$\begin{array}{ll}
(1,1) \in \mathcal{R} \Rightarrow (1,1) \in \mathcal{R} \text{ es } V, & \text{pues } (1,1) \in \mathcal{R} \\
(1,2) \in \mathcal{R} \Rightarrow (2,1) \in \mathcal{R} \text{ es } V, & \text{pues } (1,2), (2,1) \in \mathcal{R} \\
(2,1) \in \mathcal{R} \Rightarrow (1,2) \in \mathcal{R} \text{ es } V, & \text{pues } (2,1), (1,2) \in \mathcal{R} \\
(2,2) \in \mathcal{R} \Rightarrow (2,2) \in \mathcal{R} \text{ es } V, & \text{pues } (2,2) \in \mathcal{R} \\
(3,3) \in \mathcal{R} \Rightarrow (3,3) \in \mathcal{R} \text{ es } V, & \text{pues } (3,3) \in \mathcal{R} \\
(4,4) \in \mathcal{R} \Rightarrow (4,4) \in \mathcal{R} \text{ es } V, & \text{pues } (4,4) \in \mathcal{R} \\
(4,5) \in \mathcal{R} \Rightarrow (5,4) \in \mathcal{R} \text{ es } V, & \text{pues } (4,5), (5,4) \in \mathcal{R} \\
(5,4) \in \mathcal{R} \Rightarrow (4,5) \in \mathcal{R} \text{ es } V, & \text{pues } (5,4), (4,5) \in \mathcal{R} \\
(5,5) \in \mathcal{R} \Rightarrow (5,5) \in \mathcal{R} \text{ es } V, & \text{pues } (5,5) \in \mathcal{R}
\end{array}$$

es decir,

$$\forall a, b \in A, (a,b) \in \mathcal{R} \Rightarrow (b,a) \in \mathcal{R}.$$

Finalmente, podemos ver que $\mathcal{R}$ es transitiva, pues

$$\begin{array}{ll}
(1,1) \in \mathcal{R} \wedge (1,1) \in \mathcal{R} \Rightarrow (1,1) \in \mathcal{R} \text{ es } V, & \text{pues } (1,1) \in \mathcal{R} \\
(1,1) \in \mathcal{R} \wedge (1,2) \in \mathcal{R} \Rightarrow (1,2) \in \mathcal{R} \text{ es } V, & \text{pues } (1,1) \in \mathcal{R} \text{ y } (1,2) \in \mathcal{R} \\
(1,2) \in \mathcal{R} \wedge (2,1) \in \mathcal{R} \Rightarrow (1,1) \in \mathcal{R} \text{ es } V, & \text{pues } (1,2) \in \mathcal{R}, (2,1) \in \mathcal{R} \text{ y } (1,1) \in \mathcal{R}
\end{array}$$

$(1,2) \in \mathcal{R} \wedge (2,2) \in \mathcal{R} \Rightarrow (1,2) \in \mathcal{R}$ es V, pues $(1,2) \in \mathcal{R}$ y $(2,2) \in \mathcal{R}$

$(2,1) \in \mathcal{R} \wedge (1,1) \in \mathcal{R} \Rightarrow (2,1) \in \mathcal{R}$ es V, pues $(2,1) \in \mathcal{R}$ y $(1,1) \in \mathcal{R}$

$(2,1) \in \mathcal{R} \wedge (1,2) \in \mathcal{R} \Rightarrow (2,2) \in \mathcal{R}$ es V, pues $(2,1) \in \mathcal{R}$, $(1,2) \in \mathcal{R}$ y $(2,2) \in \mathcal{R}$

$(2,2) \in \mathcal{R} \wedge (2,2) \in \mathcal{R} \Rightarrow (2,2) \in \mathcal{R}$ es V, pues $(2,2) \in \mathcal{R}$

$(2,2) \in \mathcal{R} \wedge (2,1) \in \mathcal{R} \Rightarrow (2,1) \in \mathcal{R}$ es V, pues $(2,2) \in \mathcal{R}$ y $(2,1) \in \mathcal{R}$

$(3,3) \in \mathcal{R} \wedge (3,3) \in \mathcal{R} \Rightarrow (3,3) \in \mathcal{R}$ es V, pues $(3,3) \in \mathcal{R}$

$(4,4) \in \mathcal{R} \wedge (4,4) \in \mathcal{R} \Rightarrow (4,4) \in \mathcal{R}$ es V, pues $(4,4) \in \mathcal{R}$

$(4,4) \in \mathcal{R} \wedge (4,5) \in \mathcal{R} \Rightarrow (4,5) \in \mathcal{R}$ es V, pues $(4,4) \in \mathcal{R}$ y $(4,5) \in \mathcal{R}$

$(4,5) \in \mathcal{R} \wedge (5,4) \in \mathcal{R} \Rightarrow (4,4) \in \mathcal{R}$ es V, pues $(4,5) \in \mathcal{R}$, $(5,4) \in \mathcal{R}$ y $(4,4) \in \mathcal{R}$

$(4,5) \in \mathcal{R} \wedge (5,5) \in \mathcal{R} \Rightarrow (4,5) \in \mathcal{R}$ es V, pues $(4,5) \in \mathcal{R}$ y $(5,5) \in \mathcal{R}$

$(5,4) \in \mathcal{R} \wedge (4,4) \in \mathcal{R} \Rightarrow (5,4) \in \mathcal{R}$ es V, pues $(5,4) \in \mathcal{R}$ y $(4,4) \in \mathcal{R}$

$(5,4) \in \mathcal{R} \wedge (4,5) \in \mathcal{R} \Rightarrow (5,5) \in \mathcal{R}$ es V, pues $(5,4) \in \mathcal{R}$, $(4,5) \in \mathcal{R}$ y $(5,5) \in \mathcal{R}$

$(5,5) \in \mathcal{R} \wedge (5,5) \in \mathcal{R} \Rightarrow (5,5) \in \mathcal{R}$ es V, pues $(5,5) \in \mathcal{R}$

$(5,5) \in \mathcal{R} \wedge (5,4) \in \mathcal{R} \Rightarrow (5,4) \in \mathcal{R}$ es V, pues $(5,5) \in \mathcal{R}$ y $(5,4) \in \mathcal{R}$

es decir,

$$\forall a, b, c \in A, (a,b) \in \mathcal{R} \wedge (b,c) \in \mathcal{R} \Rightarrow (a,c) \in \mathcal{R}.$$

Como $\mathcal{R}$ es una relación reflexiva, simétrica y transitiva se tiene que $\mathcal{R}$ es una relación de equivalencia. Para aclarar la situación, haremos un diagrama de Venn y dibujaremos la relación mediante flechas sobre los mismos elementos.

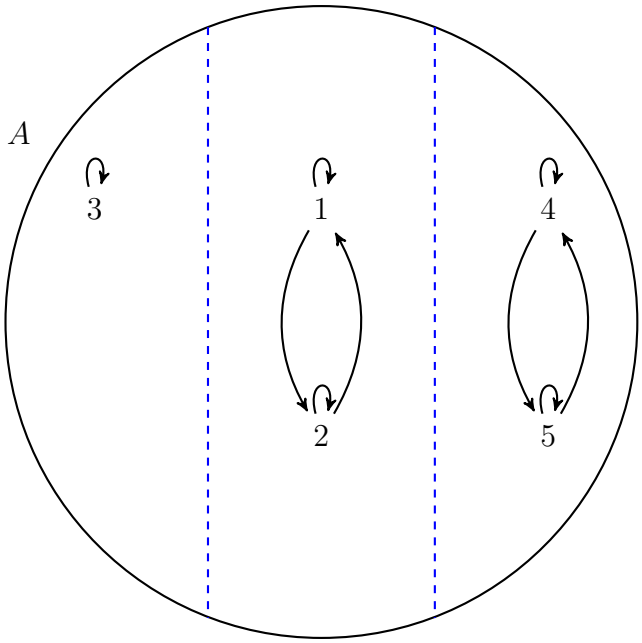


Figura 2.5: Representación de una relación de equivalencia mediante un diagrama de Venn.

Se observa de la Figura 2.5 que el conjunto A queda particionado en partes cuyos elementos están relacionados entre sí.

Definición 2.6
Sea A un conjunto y $\mathcal{R} \subset A \times A$ una relación de equivalencia sobre A. Si $a \in A$, llamamos clase de equivalencia de a al conjunto:

$$P(a) = \{b \in A : (a,b) \in \mathcal{R}\}.$$

El elemento se llama un representante de la clase $P(a)$.

Proposición 2.2
Sea A un conjunto y $\mathcal{R} \subset A \times A$ una relación de equivalencia sobre A. Entonces $\mathcal{R}$ induce una partición de A en clases de equivalencia.

Demostración.
La proposición resultará de demostrar varias afirmaciones.

(a) Si $a \in A$ entonces $a \in P(a)$, es decir $P(a) \neq \varnothing$.

Debido a que $\mathcal{R}$ es reflexiva se tiene que $(a, a) \in \mathcal{R}$. Esto nos dice que $a \in P(a)$, por lo que $P(a) \neq \varnothing$.

(b) Si $a, b \in A$ se tiene que $P(a) = P(b)$ o $P(a) \cap P(b) = \varnothing$.

Si ocurriese que $P(a) \cap P(b) = \varnothing$ listo.

Supongamos entonces que $P(a) \cap P(b) \neq \varnothing$. Esto significa que existe un elemento $c \in A$ tal que:

$$c \in P(a) \text{ y } c \in P(b),$$

es decir,

$$\begin{aligned} (a, c) &\in \mathcal{R} \qquad \text{por lo tanto } (c, a) \in \mathcal{R} \text{ por simetría de } \mathcal{R} \\ (b, c) &\in \mathcal{R} \qquad \text{por lo tanto } (c, b) \in \mathcal{R} \text{ por simetría de } \mathcal{R} \end{aligned}$$

Veamos que $P(a) \subset P(b)$. Si $x \in P(a)$ entonces $(a, x) \in \mathcal{R}$. Del hecho que $(b, c), (c, a), (a, x) \in \mathcal{R}$ se tiene que $(b, x) \in \mathcal{R}$ por la transitividad de $\mathcal{R}$, lo cual nos dice que $x \in P(b)$.

Veamos que $P(b) \subset P(a)$. Si $x \in P(b)$ entonces $(b, x) \in \mathcal{R}$. Del hecho que $(a, c), (c, b), (b, x) \in \mathcal{R}$ se tiene que $(a, x) \in \mathcal{R}$ por la transitividad de $\mathcal{R}$, lo cual nos dice que $x \in P(a)$.

Esto significa que $P(a) = P(b)$.

(c) Si $a, b \in A$ se tiene que $(a, b) \in \mathcal{R} \Leftrightarrow P(a) = P(b)$.

Supongamos que $(a, b) \in \mathcal{R}$. Luego, $b \in P(a)$, pero además por (a) sabemos que $b \in P(b)$. Por lo tanto $P(a) \cap P(b) \neq \varnothing$. Por (b) se deduce que $P(a) = P(b)$.

Supongamos que $P(a) = P(b)$. Por (a) se tiene que $b \in P(b)$, lo que significa que $b \in P(a)$, lo que implica que $(a, b) \in \mathcal{R}$.

(d) Si $\{A_i : i \in \mathcal{I}\}$ es el conjunto de las distintas clases de equivalencia de A, entonces

$$A = \bigcup_{i \in \mathcal{I}} A_i,$$

y es una unión disjunta.

Veamos la inclusión $\subset$. Si $x \in A$, entonces $x \in P(x)$ por (a). Luego $P(x)$ es alguna de las distintas clases de equivalencia, digamos A_k. Esto implica que $x \in \bigcup_{i \in \mathcal{I}} A_i$.

Veamos la inclusión $\supset$. Si $x \in \bigcup_{i \in \mathcal{I}} A_i$, entonces existe un $k \in \mathcal{I}$ tal que $x \in A_k$. Por Definición 2.6, se tiene que $A_k \subset A$, por lo que $x \in A$. ■

La recíproca de la Proposición 2.2 es verdadera.

Proposición 2.3
Sea A un conjunto y una partición $\{B_j : j \in \mathcal{J}\}$ de A. Entonces esta partición define una relación de equivalencia $\mathcal{S}$ en A definida por:

$$(a, b) \in \mathcal{S} \Leftrightarrow \exists j \in \mathcal{J} : a, b \in B_j.$$

Demostración.

Veamos que $\mathcal{S}$ es reflexiva. Si $a \in A$, por Definición 1.36 (partición de un conjunto) tenemos que:

$$a \in \bigcup_{j \in \mathcal{J}} B_j.$$

Luego existe $k \in \mathcal{J}$ tal que $a \in B_k$, lo que significa que $(a, a) \in \mathcal{S}$.

Veamos que $\mathcal{S}$ es simétrica. Sean $a, b \in A$ tal que $(a, b) \in \mathcal{S}$. Esto significa que existe $k \in \mathcal{J}$ tal que $a, b \in B_k$. Pero esto es lo mismo que decir que existe $k \in \mathcal{J}$ tal que $b, a \in B_k$, lo que significa que $(b, a) \in \mathcal{S}$.

Veamos que $\mathcal{S}$ es transitiva. Sean $a, b, c \in A$ tal que $(a, b) \in \mathcal{S}$ y $(b, c) \in \mathcal{S}$. Luego,

$$\begin{aligned} (a, b) \in \mathcal{S} &\Leftrightarrow \exists k \in \mathcal{J} : a, b \in B_k, \\ (b, c) \in \mathcal{S} &\Leftrightarrow \exists l \in \mathcal{J} : b, c \in B_l. \end{aligned}$$

Pero entonces $b \in B_k \cap B_l$, lo que significa que $B_k \cap B_l \neq \varnothing$. Luego $k = l$ por Definición 1.36. Por lo tanto, $a, b, c \in B_k$. En particular, $a, c \in B_k$, es decir, $(a, c) \in \mathcal{S}$. ■

Es usual representar a las relaciones de equivalencia con el símbolo $\sim$.

2.7. Relaciones de orden

Definición 2.7

Sea A un conjunto y $\mathcal{R}$ una relación sobre A. Diremos que $\mathcal{R}$ es una relación de

(a) orden amplio si es reflexiva, antisimétrica y transitiva.

(b) orden estricto si es arreflexiva, asimétrica y transitiva.

Las relaciones de orden suelen ser denotadas por $\prec$.

Ejemplo 2.6

Sea $A = \{1, 2, 3, 4\}$.

(a) Si $\mathcal{R} = \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,3), (2,4), (3,3), (3,4), (4,4)\}$ entonces $\mathcal{R}$ es una relación de orden amplio.

Notemos que $\mathcal{R}$ es reflexiva, pues

$$\begin{aligned} &(1,1) \in \mathcal{R}, \quad (2,2) \in \mathcal{R}, \\ &(3,3) \in \mathcal{R}, \quad (4,4) \in \mathcal{R}. \end{aligned}$$

Notemos que $\mathcal{R}$ es antisimétrica, pues

$$\begin{aligned} &1 \neq 2 \wedge (1,2) \in \mathcal{R} \Rightarrow (2,1) \notin \mathcal{R} \text{ es } V, && \text{pues } (1,2) \in \mathcal{R} \text{ pero } (2,1) \notin \mathcal{R} \\ &1 \neq 3 \wedge (1,3) \in \mathcal{R} \Rightarrow (3,1) \notin \mathcal{R} \text{ es } V, && \text{pues } (1,3) \in \mathcal{R} \text{ pero } (3,1) \notin \mathcal{R} \\ &1 \neq 4 \wedge (1,4) \in \mathcal{R} \Rightarrow (4,1) \notin \mathcal{R} \text{ es } V, && \text{pues } (1,4) \in \mathcal{R} \text{ pero } (4,1) \notin \mathcal{R} \\ &2 \neq 3 \wedge (2,3) \in \mathcal{R} \Rightarrow (3,2) \notin \mathcal{R} \text{ es } V, && \text{pues } (2,3) \in \mathcal{R} \text{ pero } (3,2) \notin \mathcal{R} \\ &2 \neq 4 \wedge (2,4) \in \mathcal{R} \Rightarrow (4,2) \notin \mathcal{R} \text{ es } V, && \text{pues } (2,4) \in \mathcal{R} \text{ pero } (4,2) \notin \mathcal{R} \\ &3 \neq 4 \wedge (3,4) \in \mathcal{R} \Rightarrow (4,3) \notin \mathcal{R} \text{ es } V, && \text{pues } (3,4) \in \mathcal{R} \text{ pero } (4,3) \notin \mathcal{R} \end{aligned}$$

Notemos que $\mathcal{R}$ es transitiva, pues

$$(1,1) \in \mathcal{R} \wedge (1,1) \in \mathcal{R} \Rightarrow (1,1) \in \mathcal{R} \text{ es } V, \qquad \text{pues } (1,1) \in \mathcal{R}$$

$$
\begin{aligned}
&(1,1)\in\mathcal{R}\wedge(1,2)\in\mathcal{R}\Rightarrow(1,2)\in\mathcal{R}\text{ es }V, && \text{pues } (1,1)\in\mathcal{R} \text{ y } (1,2)\in\mathcal{R}\\
&(1,1)\in\mathcal{R}\wedge(1,3)\in\mathcal{R}\Rightarrow(1,3)\in\mathcal{R}\text{ es }V, && \text{pues } (1,1)\in\mathcal{R} \text{ y } (1,3)\in\mathcal{R}\\
&(1,1)\in\mathcal{R}\wedge(1,4)\in\mathcal{R}\Rightarrow(1,4)\in\mathcal{R}\text{ es }V, && \text{pues } (1,1)\in\mathcal{R} \text{ y } (1,4)\in\mathcal{R}\\
&(1,2)\in\mathcal{R}\wedge(2,2)\in\mathcal{R}\Rightarrow(1,2)\in\mathcal{R}\text{ es }V, && \text{pues } (1,2)\in\mathcal{R} \text{ y } (2,2)\in\mathcal{R}\\
&(1,2)\in\mathcal{R}\wedge(2,3)\in\mathcal{R}\Rightarrow(1,3)\in\mathcal{R}\text{ es }V, && \text{pues } (1,2)\in\mathcal{R},\ (2,3)\in\mathcal{R} \text{ y } (1,3)\in\mathcal{R}\\
&(1,2)\in\mathcal{R}\wedge(2,4)\in\mathcal{R}\Rightarrow(1,4)\in\mathcal{R}\text{ es }V, && \text{pues } (1,2)\in\mathcal{R},\ (2,4)\in\mathcal{R} \text{ y } (1,4)\in\mathcal{R}\\
&(1,3)\in\mathcal{R}\wedge(3,3)\in\mathcal{R}\Rightarrow(1,3)\in\mathcal{R}\text{ es }V, && \text{pues } (1,3)\in\mathcal{R} \text{ y } (3,3)\in\mathcal{R}\\
&(1,3)\in\mathcal{R}\wedge(3,4)\in\mathcal{R}\Rightarrow(1,4)\in\mathcal{R}\text{ es }V, && \text{pues } (1,3)\in\mathcal{R},\ (3,4)\in\mathcal{R} \text{ y } (1,4)\in\mathcal{R}\\
&(1,4)\in\mathcal{R}\wedge(4,4)\in\mathcal{R}\Rightarrow(1,4)\in\mathcal{R}\text{ es }V, && \text{pues } (1,4)\in\mathcal{R} \text{ y } (4,4)\in\mathcal{R}\\
&(2,2)\in\mathcal{R}\wedge(2,2)\in\mathcal{R}\Rightarrow(2,2)\in\mathcal{R}\text{ es }V, && \text{pues } (2,2)\in\mathcal{R}\\
&(2,2)\in\mathcal{R}\wedge(2,3)\in\mathcal{R}\Rightarrow(2,3)\in\mathcal{R}\text{ es }V, && \text{pues } (2,2)\in\mathcal{R} \text{ y } (2,3)\in\mathcal{R}\\
&(2,2)\in\mathcal{R}\wedge(2,4)\in\mathcal{R}\Rightarrow(2,4)\in\mathcal{R}\text{ es }V, && \text{pues } (2,2)\in\mathcal{R} \text{ y } (2,4)\in\mathcal{R}\\
&(2,3)\in\mathcal{R}\wedge(3,3)\in\mathcal{R}\Rightarrow(2,3)\in\mathcal{R}\text{ es }V, && \text{pues } (2,3)\in\mathcal{R} \text{ y } (3,3)\in\mathcal{R}\\
&(2,3)\in\mathcal{R}\wedge(3,4)\in\mathcal{R}\Rightarrow(2,4)\in\mathcal{R}\text{ es }V, && \text{pues } (2,3)\in\mathcal{R},\ (3,4)\in\mathcal{R} \text{ y } (2,4)\in\mathcal{R}\\
&(2,4)\in\mathcal{R}\wedge(4,4)\in\mathcal{R}\Rightarrow(2,4)\in\mathcal{R}\text{ es }V, && \text{pues } (2,4)\in\mathcal{R} \text{ y } (4,4)\in\mathcal{R}\\
&(3,3)\in\mathcal{R}\wedge(3,3)\in\mathcal{R}\Rightarrow(3,3)\in\mathcal{R}\text{ es }V, && \text{pues } (3,3)\in\mathcal{R}\\
&(3,3)\in\mathcal{R}\wedge(3,4)\in\mathcal{R}\Rightarrow(3,4)\in\mathcal{R}\text{ es }V, && \text{pues } (3,3)\in\mathcal{R} \text{ y } (3,4)\in\mathcal{R}\\
&(3,4)\in\mathcal{R}\wedge(4,4)\in\mathcal{R}\Rightarrow(3,4)\in\mathcal{R}\text{ es }V, && \text{pues } (3,4)\in\mathcal{R} \text{ y } (4,4)\in\mathcal{R}\\
&(4,4)\in\mathcal{R}\wedge(4,4)\in\mathcal{R}\Rightarrow(4,4)\in\mathcal{R}\text{ es }V, && \text{pues } (4,4)\in\mathcal{R}
\end{aligned}
$$

(b) Si $\mathcal{R}=\{(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)\}$ entonces $\mathcal{R}$ es una relación de orden estricto.

Notemos que $\mathcal{R}$ es arreflexiva, pues

$$
\begin{aligned}
&(1,1)\notin\mathcal{R}, \quad (2,2)\notin\mathcal{R},\\
&(3,3)\notin\mathcal{R}, \quad (4,4)\notin\mathcal{R}.
\end{aligned}
$$

Notemos que $\mathcal{R}$ es asimétrica, pues

$$
\begin{aligned}
&(1,2)\in\mathcal{R}\Rightarrow(2,1)\notin\mathcal{R}\text{ es }V, && \text{pues } (1,2)\in\mathcal{R} \text{ y } (2,1)\notin\mathcal{R}\\
&(1,3)\in\mathcal{R}\Rightarrow(3,1)\notin\mathcal{R}\text{ es }V, && \text{pues } (1,3)\in\mathcal{R} \text{ y } (3,1)\notin\mathcal{R}\\
&(1,4)\in\mathcal{R}\Rightarrow(4,1)\notin\mathcal{R}\text{ es }V, && \text{pues } (1,4)\in\mathcal{R} \text{ y } (4,1)\notin\mathcal{R}\\
&(2,3)\in\mathcal{R}\Rightarrow(3,2)\notin\mathcal{R}\text{ es }V, && \text{pues } (2,3)\in\mathcal{R} \text{ y } (3,2)\notin\mathcal{R}\\
&(2,4)\in\mathcal{R}\Rightarrow(4,2)\notin\mathcal{R}\text{ es }V, && \text{pues } (2,4)\in\mathcal{R} \text{ y } (4,2)\notin\mathcal{R}\\
&(3,4)\in\mathcal{R}\Rightarrow(4,3)\notin\mathcal{R}\text{ es }V, && \text{pues } (3,4)\in\mathcal{R} \text{ y } (4,3)\notin\mathcal{R}
\end{aligned}
$$

Notemos que $\mathcal{R}$ es transitiva, pues

$$
\begin{aligned}
&(1,2)\in\mathcal{R}\wedge(2,3)\in\mathcal{R}\Rightarrow(1,3)\in\mathcal{R}\text{ es }V, && \text{pues } (1,2)\in\mathcal{R},\ (2,3)\in\mathcal{R} \text{ y } (1,3)\in\mathcal{R}\\
&(1,2)\in\mathcal{R}\wedge(2,4)\in\mathcal{R}\Rightarrow(1,4)\in\mathcal{R}\text{ es }V, && \text{pues } (1,2)\in\mathcal{R},\ (2,4)\in\mathcal{R} \text{ y } (1,4)\in\mathcal{R}\\
&(1,3)\in\mathcal{R}\wedge(3,4)\in\mathcal{R}\Rightarrow(1,4)\in\mathcal{R}\text{ es }V, && \text{pues } (1,3)\in\mathcal{R},\ (3,4)\in\mathcal{R} \text{ y } (1,4)\in\mathcal{R}\\
&(2,3)\in\mathcal{R}\wedge(3,4)\in\mathcal{R}\Rightarrow(2,4)\in\mathcal{R}\text{ es }V, && \text{pues } (2,3)\in\mathcal{R},\ (3,4)\in\mathcal{R} \text{ y } (2,4)\in\mathcal{R}
\end{aligned}
$$

Definición 2.8

Sea A un conjunto y $\prec$ una relación de orden (amplio o estricto) sobre A. Diremos que $\prec$ es un orden total si todos los elementos de A se relacionan entre sí. Es decir,

$$\forall x,y\in A,\quad x\prec y\vee y\prec x.$$

Ejemplo 2.7

(a) Notemos que la relación definida en el Ejemplo 2.6-(a) es un orden total.

(b) Notemos que la relación definida en el Ejemplo 2.6-(b) no es un orden total.

En general, de la Definición 2.8 se observa que una relación de orden estricto no es un orden total, pues es arreflexiva.

3. FUNCIONES

3.1. Concepto de función

Definición 3.1
Una función f de un conjunto A en un conjunto B es una relación entre A y B (es decir, $f \subset A \times B$) que satisface:

(a) Existencia: $\forall a \in A, \exists b \in B$ tal que $(a,b) \in f$.

(b) Unicidad: Si $(a,b), (a,c) \in f$ entonces $b = c$.

Dicho con otras palabras, todo elemento de A tiene un único correspondiente en B.

Si el par $(a,b) \in f$ se suele decir que b es el correspondiente de a (pues es el único) y se simboliza por $f(a)$.

Las funciones suelen denotarse con letras minúsculas: f, g, h, etc. Una función de A en B suele denotarse de la siguiente manera:

$$f : A \to B.$$

Ejemplo 3.1
Consideremos $A = \{a, b, c, d\}$ y $B = \{1, 2, 3\}$.

(a) Sea

$$f = \{(a,1), (b,2), (c,2), (d,1)\}.$$

En este caso f está definida por extensión. Notar que cada elemento de A está relacionado a un único elemento de B, lo cual puede verse gráficamente en un diagrama de Venn observando que de cada elemento de A sale una sola flecha (ver Figura 3.1). Esto nos dice que f es una función, y además se tiene que:

$$f(a) = 1, \quad f(b) = 2, \quad f(c) = 2, \quad f(d) = 1.$$

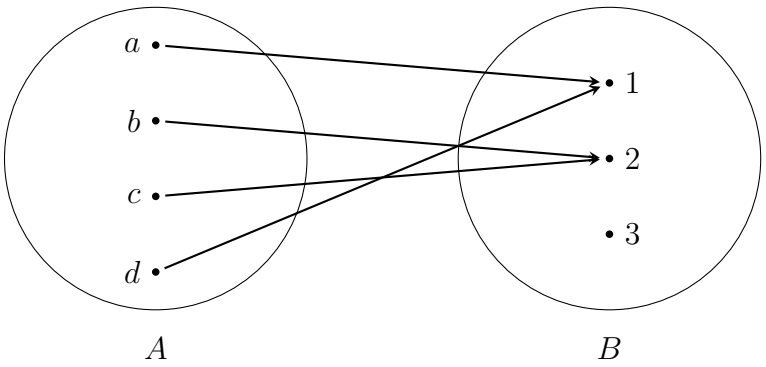


Figura 3.1: Diagrama de Venn de una función.

(b) Sea

$$f = \{(a,1), (b,2), (c,2)\}.$$

Notar que no todo elemento de A está relacionado a un elemento de B, lo cual puede verse gráficamente en un diagrama de Venn observando que del elemento d no sale ninguna flecha (ver Figura 3.2). Esto nos dice que f no es una función, pues no satisface la Definición 3.1-(a) (condición de existencia).

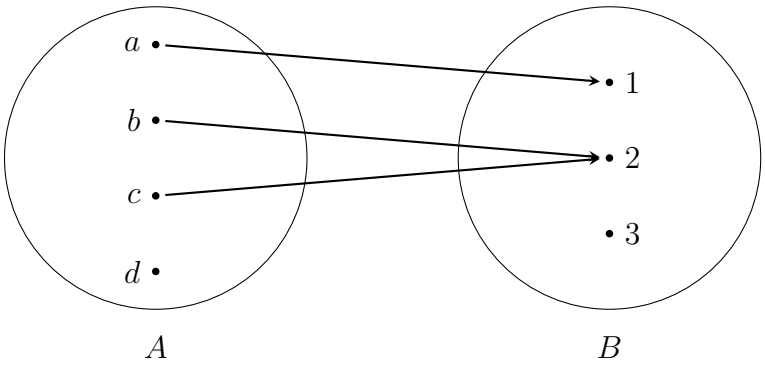


Figura 3.2: Diagrama de Venn de una relación que no es función (falla la condición de existencia).

(c) Sea

$$f = \{(a,1),(b,2),(c,2),(a,3),(d,3)\}.$$

Notar que no todo elemento de A está relacionado a un único elemento de B, lo cual puede verse gráficamente en un diagrama de Venn observando que del elemento a salen dos flechas (ver Figura 3.3). Esto nos dice que f no es una función, pues no satisface la Definición 3.1-(b) (condición de unicidad).

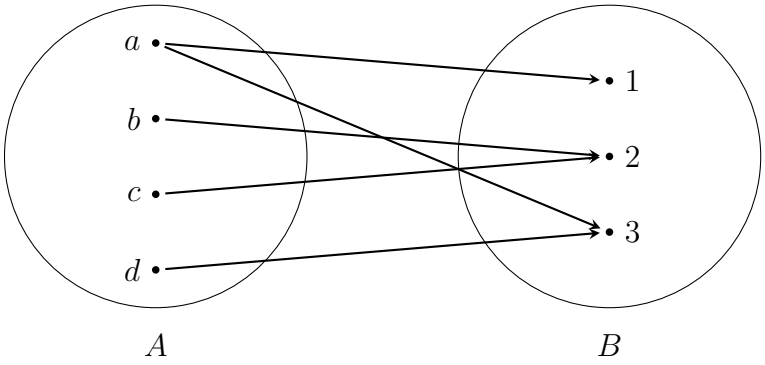


Figura 3.3: Diagrama de Venn de una relación que no es función (falla la condición de unicidad).

Recordemos que una relación entre dos conjuntos A y B era un subconjunto del producto cartesiano $A \times B$. En particular, una función f puede definirse por extensión (como en el Ejemplo 3.1(a)), o bien por comprensión, enunciando una característica o propiedad de los elementos de f.

Ejemplo 3.2

(a) Sea $A = \{x : x \text{ es una estación del año}\}$ y $B = \{x : x \text{ es un mes del año}\}$ y

$$f = \{(a,b) : a \text{ comienza el mes } b\}.$$

Notar que cada estación del año comienza en algún mes, por lo que la relación f satisface la condición de existencia. Asimismo, una estación del año no comienza en meses distintos, por lo que también satisface la condición de unicidad. Estas observaciones nos hacen concluir que f es una función. El diagrama de Venn correspondiente se puede ver en la Figura 3.4.

(b) Sea $A = \{x : x \text{ fue un ser humano nacido en el siglo X}\}$, $B = \{x : x \text{ es o fue un ser humano}\}$ y $f \subset A \times B$ definida por:

$$f = \{(a,b) : b \text{ fue el padre biológico de } a\}.$$

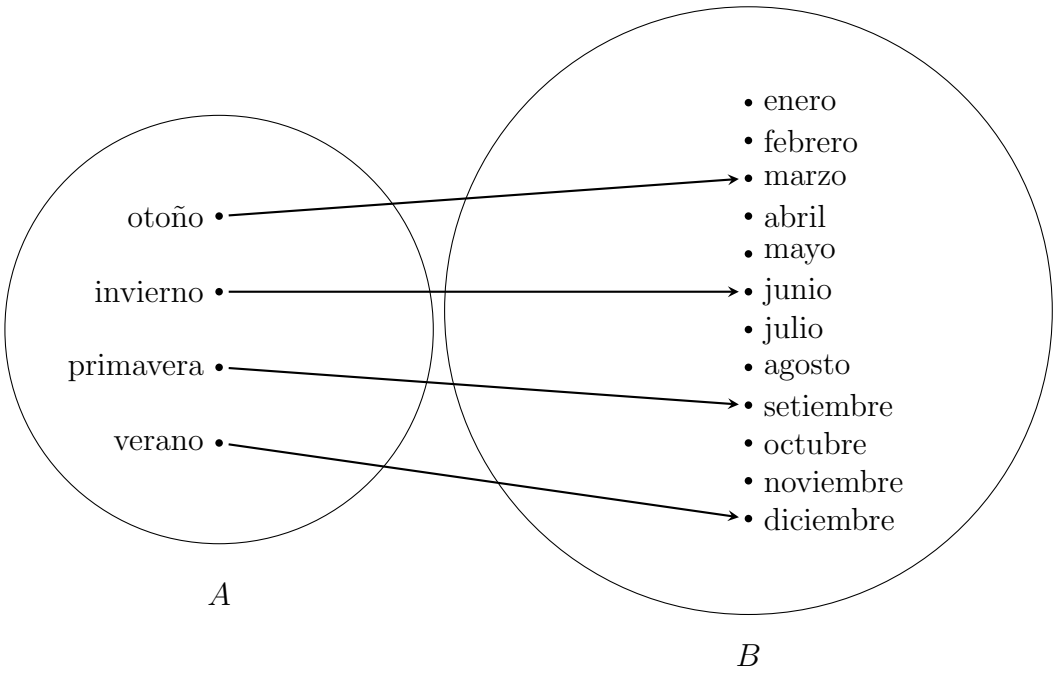


Figura 3.4: Diagrama de Venn de una función.

Cada elemento de A tuvo un padre, por lo que la relación f satisface la condición de existencia. Asimismo, cada persona tuvo un único padre biológico, por lo que también satisface la condición de unicidad. Estas observaciones nos hacen concluir que f es una función.

Cuando definimos una función $f : A \to B$ por comprensión expresamos una característica de los pares ordenados. En realidad, estamos definiendo una regla de asignación entre los elementos de A y B. Por ello a veces las funciones vienen dadas enunciando solamente la regla de asignación y aclarando cuáles son los conjuntos A y B.

Ejemplo 3.3

(a) Consideremos $f : \mathbb{N} \to \mathbb{N}$ que a cada número natural le asigna su siguiente. La fórmula que define a f se puede escribir:

$$f(x) = x + 1.$$

De este modo: $f = \{(x, x+1) : x \in \mathbb{N}\}$.

(b) Consideremos $g : \mathbb{R} \to \mathbb{R}$ que a cada número real le asigna el doble de su cubo. La fórmula que define a g se puede escribir:

$$g(x) = 2 \cdot x^3.$$

De este modo: $g = \{(x, 2 \cdot x^3) : x \in \mathbb{R}\}$.

Diremos que dos funciones $f : A \to B$ y $g : A \to B$ son iguales si lo son como relaciones. En particular, se tiene que:

$$f = g \Leftrightarrow f(x) = g(x), \quad \forall x \in A.$$

3.2. Dominio e imagen de una función

Recordemos de la Definición 3.1 que una función es una relación (pero con algunos ingredientes adicionales). Por lo tanto están definidos los conceptos de dominio e imagen de una función.

Para el caso del dominio de una función $f : A \to B$:

$$\text{Dom}(f) = \{a \in A : \exists b \in B \text{ tal que } (a, b) \in f\} \text{ por Definición 2.2-(a) (dominio de una relación)}$$

$= A$ por Definición 3.1-(a) (definición de función)

Por lo tanto, para el caso de funciones, el dominio coincide con A. En los casos en que la función está definida por una fórmula y no se aclara quién es el conjunto A (o sea, el dominio), se suele sobreenteder que el dominio está dado por el subconjunto más grande del universal en el que la fórmula se puede aplicar.

Ejemplo 3.4

(a) Si f es la función que a cada número real le asigna su inverso:

$$f(x) = \frac{1}{x}, \quad x \in \mathbb{R},$$

entonces $f(x)$ puede calcularse siempre que x sea distinto de 0. Luego

$$\mathrm{Dom}(f) = \mathbb{R} - \{0\}.$$

(b) Si g es la función que a cada número entero le asigna su opuesto:

$$g(x) = -x, \quad x \in \mathbb{Z},$$

entonces $g(x)$ puede calcularse para cualquier número entero. Luego

$$\mathrm{Dom}(g) = \mathbb{Z}.$$

Para el caso de la imagen de una función $f : A \to B$:

$$\begin{aligned} \mathrm{Im}(f) &= \{b \in B : \exists a \in A \text{ tal que } (a,b) \in f\} \text{ por Definición 2.2-(b) (imagen de una relación)} \\ &= \{f(a) : a \in A\} \text{ por Definición 3.1-(a) y 3.1-(b) (definición de función)} \end{aligned}$$

Ejemplo 3.5

(a) Sea $f : \mathbb{R} \to \mathbb{R}$ la función definida por:

$$f(x) = x + 1,$$

Vamos a determinar el conjunto $\mathrm{Im}(f) = \{x + 1 : x \in \mathbb{R}\}$. Aparentemente, este conjunto se parece mucho a $\mathbb{R}$. Claramente $\mathrm{Im}(f) \subset \mathbb{R}$. Para chequear la otra inclusión tomemos $y \in \mathbb{R}$ y tratemos de descubrir si existe un $x \in \mathbb{R}$ tal que $y = f(x)$. Para ello planteamos la ecuación $y = x + 1$ e intentamos despejar x:

$$y = x + 1 \Rightarrow x = y - 1.$$

Como fue posible hallar el x, entonces se satisface que $\mathbb{R} \subset \mathrm{Im}(f)$, con lo cual tenemos que $\mathrm{Im}(f) = \mathbb{R}$.

(b) Sea $f : \mathbb{R} \to \mathbb{R}$ la función definida por:

$$f(x) = x^2,$$

Vamos a determinar el conjunto $\mathrm{Im}(f) = \{x^2 : x \in \mathbb{R}\}$. Se puede observar que este conjunto está formado únicamente por números no negativos. Claramente $\mathrm{Im}(f) \subset [0, \infty)$. Para chequear la otra inclusión tomemos $y \in [0, \infty)$ y tratemos de descubrir si existe algún $x \in \mathbb{R}$ tal que $y = f(x)$. Por lo tanto planteamos la ecuación $y = x^2$ e intentamos despejar x. No es necesario que la ecuación $y = x^2$ tenga una única solución, de hecho posee dos soluciones.

$$y = x^2 \Rightarrow x = \sqrt{y} \text{ o } x = -\sqrt{y}.$$

Notar que el cálculo de la raíz cuadrada es posible puesto que $y \geqslant 0$. Como fue posible hallar un x (por ejemplo $x = \sqrt{y}$), entonces se satisface que $[0, \infty) \subset \mathrm{Im}(f)$, con lo cual tenemos que $\mathrm{Im}(f) = [0, \infty)$.

3.3. Representación gráfica de funciones

Como las funciones son relaciones, también puede hacerse una representación cartesiana de ellas. Cuando el dominio de la función es un conjunto infinito, se suelen dibujar algunos elementos de la función y se "completa" el gráfico de manera esquemática. Cuando se aprendan herramientas de Análisis Matemático, se podrán realizar estos dibujos de manera más precisa.

Ejemplo 3.6

(a) Supongamos que f es una función de $\mathbb{R}$ en $\mathbb{R}$ de manera que $f(x) = 2$ para todo $x \in \mathbb{R}$. Funciones de este tipo se denominan funciones constantes. El gráfico de f se puede ver en la Figura 3.5.

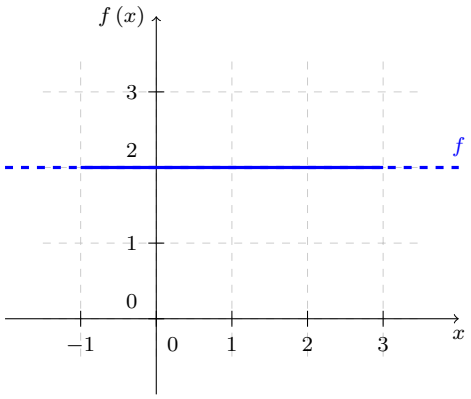


Figura 3.5: Gráfico de una función constante.

(b) Consideremos que f es una función de A en A de manera que $f(x) = x$ para todo $x \in A$. Esta función se suele denominar función identidad y se denota por i_A. En la Figura 3.6 se puede ver el gráfico de f cuando $A = \mathbb{R}$.

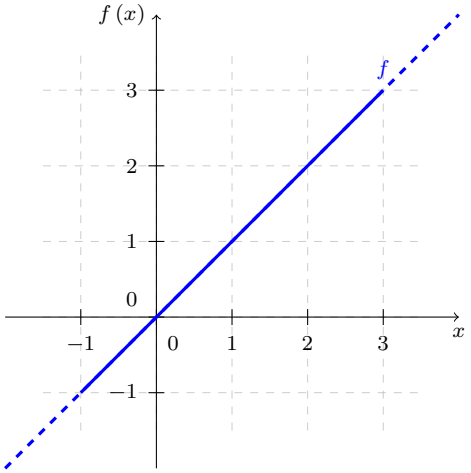


Figura 3.6: Gráfico de la función identidad.

(c) Sea $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = x^3 - x$. Esta función es una caso particular de una función cúbica. Luego el gráfico de f puede verse en la Figura 3.7.

Si en un gráfico de una relación hay dos elementos que comparten la primera componente, entonces tal gráfico no corresponde al gráfico de una función. En efecto, supongamos que (a, b) y (a, c) están en una relación $\mathcal{R}$ y que $b \neq c$. Como se está violando la Definición 3.1-(b) se tiene que $\mathcal{R}$ no es una función.

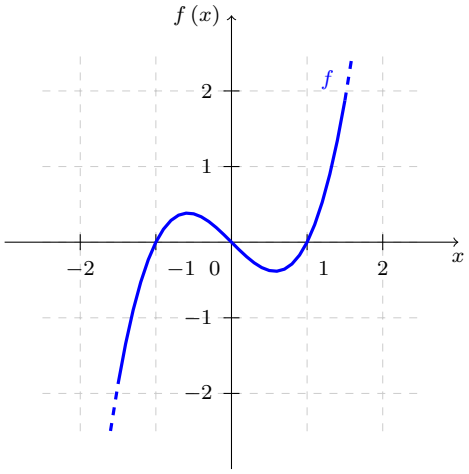


Figura 3.7: Gráfico de una función cúbica.

Ejemplo 3.7
Consideremos la relación $\mathcal{R} \subset \mathbb{R} \times \mathbb{R}$ definida por

$$\mathcal{R} = \{(1, x) : x \in \mathbb{R}\}.$$

En este caso, $(1,1), (1,2) \in \mathcal{R}$ con $1 \neq 2$. Esto nos dice que $\mathcal{R}$ no puede ser función. Un gráfico de la relación puede verse en la Figura 3.8.

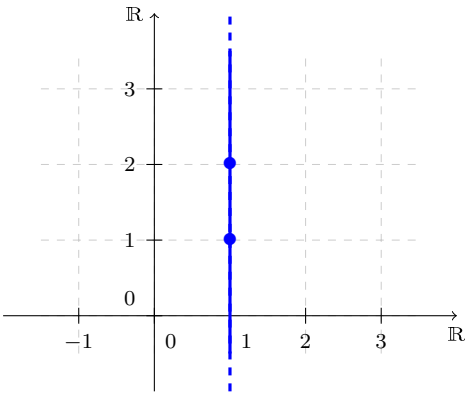


Figura 3.8: Gráfico de una relación que no es función.

3.4. Desplazamientos verticales y horizontales, y reflexiones

Si conocemos el gráfico de una función f podemos determinar con facilidad el gráfico de las siguientes funciones:

$$\begin{aligned}
g(x) &= f(x) + c && \text{desplazamiento vertical hacia arriba del gráfico de } f \\
h(x) &= f(x) - c && \text{desplazamiento vertical hacia abajo del gráfico de } f \\
k(x) &= f(x + c) && \text{desplazamiento horizontal hacia la izquierda del gráfico de } f \\
l(x) &= f(x - c) && \text{desplazamiento horizontal hacia la derecha del gráfico de } f \\
p(x) &= -f(x) && \text{reflexión respecto del eje } x \text{ del gráfico de } f \\
q(x) &= f(-x) && \text{reflexión respecto del eje } y \text{ del gráfico de } f
\end{aligned}$$

donde $c > 0$. Vamos a ejemplificar cada una de estas situaciones con la función $f : [-2, 2] \to \mathbb{R}$ definida por

$$f(x) = \frac{x^3}{2} - \frac{13}{8} \cdot x + \frac{3}{4}.$$

El gráfico de f puede verse en la Figura 3.9.

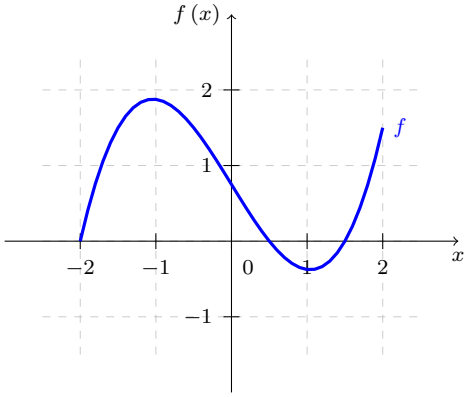


Figura 3.9: Gráfico de una función para ejemplificar desplazamientos y reflexiones.

3.4.1. Desplazamientos verticales

Las funciones g y h están definidas en los mismos puntos en los que está definida f, por lo que el dominio coincide, es decir,

$$g : [-2, 2] \to \mathbb{R},$$
$$h : [-2, 2] \to \mathbb{R}.$$

Además recordar que

$$\begin{aligned} g(x) &= f(x) + c, \\ h(x) &= f(x) - c, \end{aligned}$$

es decir que en cada x el valor de $g(x)$ está c unidades hacia arriba de $f(x)$, y el valor de $h(x)$ está c unidades por debajo de $f(x)$. Esto produce que el gráfico de g sea un desplazamiento del gráfico de f en c unidades hacia arriba, y que el gráfico de h sea un desplazamiento del gráfico de f en c unidades hacia abajo. Ver Figura 3.10 para el caso $c = 1$.

3.4.2. Desplazamientos horizontales

La función k definida por

$$k(x) = f(x + c)$$

se puede calcular siempre que $x + c \in [-2, 2]$, es decir, $x \in [-2 - c, 2 - c]$, por lo que

$$\mathrm{Dom}(k) = [-2 - c, 2 - c].$$

Es claro que el gráfico de k es un desplazamiento del gráfico de f hacia la izquierda en c unidades.

La función l definida por

$$l(x) = f(x - c)$$

se puede calcular siempre que $x - c \in [-2, 2]$, es decir, $x \in [-2 + c, 2 + c]$, por lo que

$$\mathrm{Dom}(l) = [-2 + c, 2 + c].$$

Es claro que el gráfico de l es un desplazamiento del gráfico de f hacia la derecha en c unidades.

Ver Figura 3.11 para el caso $c = 1$. En este caso, $\mathrm{Dom}(k) = [-3, 1]$ y $\mathrm{Dom}(l) = [-1, 3]$.

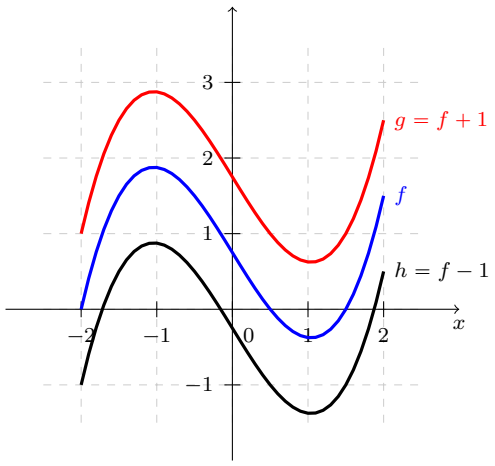


Figura 3.10: Ejemplo de una función que es el resultado de un desplazamiento vertical.

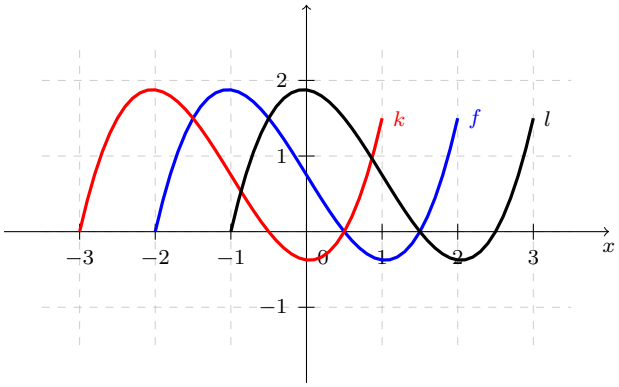


Figura 3.11: Ejemplo de una función que es el resultado de un desplazamiento horizontal.

3.4.3. Reflexiones

La función p está definida en los mismos puntos en los que está definida f, por lo que el dominio coincide, es decir,

$$p : [-2, 2] \to \mathbb{R}.$$

Además recordar que

$$p\,(x) = -f\,(x)\,,$$

es decir que en cada x el valor de $p\,(x)$ es el opuesto de $f\,(x)$, por lo que el gráfico de p es una reflexión del gráfico de f respecto al eje x (ver Figura 3.12).

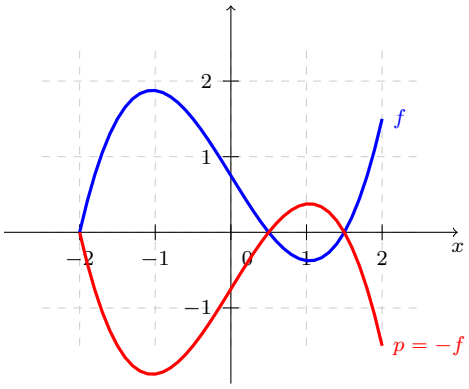


Figura 3.12: Ejemplo de una función que es el resultado de una reflexión respecto del eje x.

La función q definida por

$$q(x) = f(-x),$$

se puede calcular siempre que $-x \in [-2, 2]$, es decir, $x \in [-2, 2]$, por lo que

$$\text{Dom}(q) = [-2, 2].$$

Es claro que el gráfico de q es una reflexión del gráfico de f respecto del eje y (ver Figura 3.13).

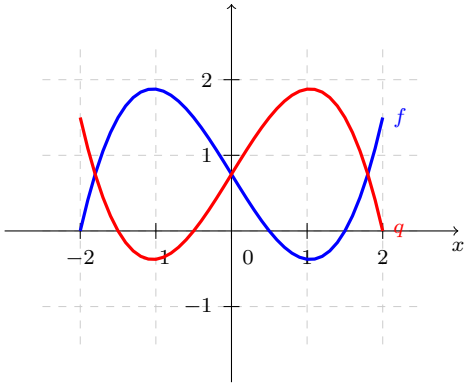


Figura 3.13: Ejemplo de una función que es el resultado de una reflexión respecto del eje y.

3.5. Clasificación de funciones

Definición 3.2

Diremos que $f : A \to B$ es una función inyectiva si

$$\forall u, v \in A, \quad u \neq v \Rightarrow f(u) \neq f(v).$$

Utilizando la Proposición 1.1-(l) (contrarrecíproca de la implicación), se puede ver que la inyectividad es equivalente a:

$$\forall u, v \in A, \quad f(u) = f(v) \Rightarrow u = v.$$

Ejemplo 3.8

(a) Sean $A = \{1, 2, 3, 4\}$, $B = \{5, 6, 7\}$ y $f : A \to B$ definida por:

$$f = \{(1, 5), (2, 5), (3, 6), (4, 7)\}.$$

Como f se compone de pocos elementos, podemos graficar a f utilizando diagramas de Venn (ver Figura 3.14). Notar que f no es inyectiva, pues $1 \neq 2$ pero $f(1) = 5 = f(2)$.

Si hubiéramos hecho una representación cartesiana de f, nos hubiéramos dado cuenta que f no es inyectiva pues hay una recta horizontal que corta el gráfico de f en dos puntos, a saber, en $(1, 5)$ y $(2, 5)$ (ver la línea de trazo azul en la Figura 3.15), lo que significa que hay un elemento de B que es alcanzado en más de una ocasión por la función.

(b) Sea $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = x^2$.

Notar que esta función tampoco es inyectiva pues $-1 \neq 1$ pero $f(-1) = 1 = f(1)$. Si hacemos un gráfico de f nos daremos cuenta que existen rectas horizontales que cortan al gráfico de f en más de una ocasión (ver la línea de trazo azul en la Figura 3.16).

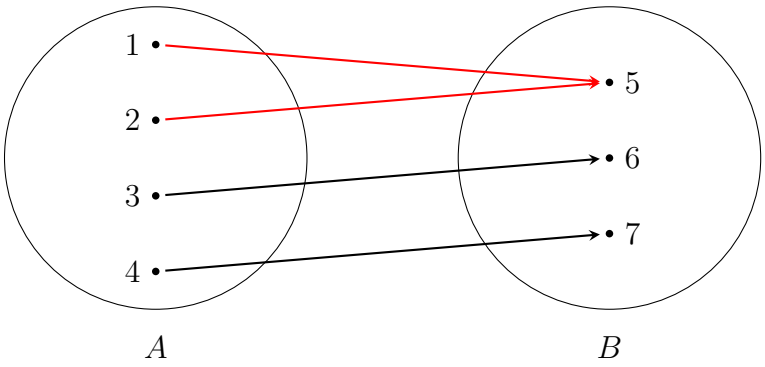


Figura 3.14: Diagrama de Venn de una función no inyectiva.

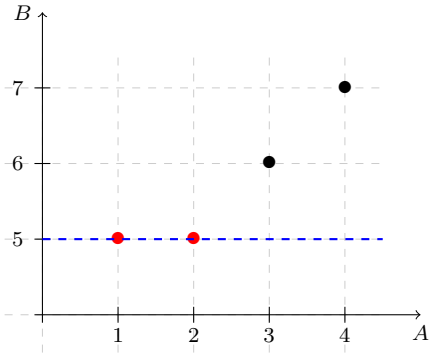


Figura 3.15: Representación cartesiana de una función no inyectiva.

(c) Si $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = 2 \cdot x + 1$.

El gráfico de f es una recta, por lo que sospechamos que f es inyectiva. Vamos a demostrar entonces que f es inyectiva:

$$\begin{aligned} f(u) = f(v) &\Rightarrow 2 \cdot u + 1 = 2 \cdot v + 1 \text{ por definición de } f \\ &\Rightarrow 2 \cdot u = 2 \cdot v \text{ sumando } (-1) \text{ a ambos miembros} \\ &\Rightarrow u = v \text{ dividiendo por 2 a ambos miembros} \end{aligned}$$

Luego, hemos demostrado que f es inyectiva.

Definición 3.3
Diremos que una función $f : A \to B$ es sobreyectiva si $\operatorname{Im}(f) = B$, *es decir*[6],

$$\text{para cada } y \in B, \exists x \in A : y = f(x).$$

Ejemplo 3.9

(a) Sean $A = \{a, b, c, d\}$, $B = \{1, 2\}$ y $f : A \to B$ definida por:

$$f = \{(a, 1), (b, 1), (c, 2), (d, 2)\}.$$

Como f se compone de pocos elementos, podemos graficar a f utilizando diagramas de Venn (ver Figura 3.17). Notar que f es sobreyectiva pues $1 = f(a)$ y $2 = f(c)$. Es decir, a cada elemento de B llega al menos una flecha.

[6]Notar que por Definición 2.2-(b) el conjunto $\operatorname{Im}(f)$ es un subconjunto de B. Por lo tanto la igualdad se da cuando $B \subset \operatorname{Im}(f)$, que es lo que expresa el "es decir".

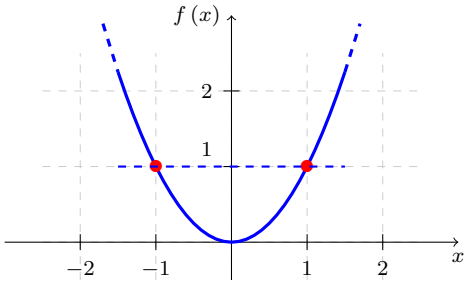


Figura 3.16: Representación cartesiana de una función no inyectiva.

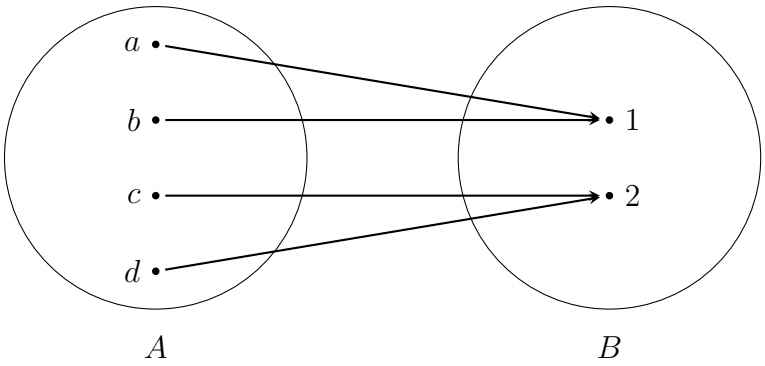


Figura 3.17: Diagrama de Venn de una función sobreyectiva.

(b) Sea $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = x^2$.

Notar que esta función no es sobreyectiva, pues no existe ningún $x \in \mathbb{R}$ tal que $x^2 = -1$ (pues todo número elevado al cuadrado es no negativo). Si hacemos un gráfico cartesiano de f nos daremos cuenta que existen rectas horizontales que no cortan el gráfico de f (ver línea de trazo azul en la Figura 3.18).

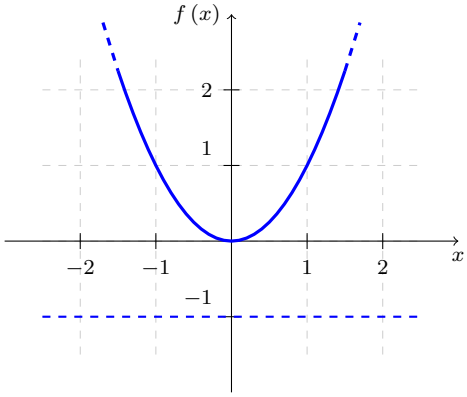


Figura 3.18: Representación cartesiana de una función no sobreyectiva.

(c) Sea $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = x^3 - 1$.

Veamos si f es sobreyectiva. Sea $y \in \mathbb{R}$ y busquemos un elemento en el dominio que a través de f alcance a y:

$$\begin{aligned} y = f(x) &\Leftrightarrow y = x^3 - 1 \text{ por definición de } f \\ &\Leftrightarrow y + 1 = x^3 \text{ pasando de término} \\ &\Leftrightarrow \sqrt[3]{y+1} = x \text{ calculando la raíz cúbica} \end{aligned}$$

Luego hemos encontrado un $x \in \mathbb{R}$ tal que $y = f(x)$, por lo que f es sobreyectiva.

Definición 3.4
Diremos que una función $f : A \to B$ es biyectiva si satisface que es simultáneamente inyectiva y sobreyectiva.

Ejemplo 3.10
Consideremos $A = \{1, 2, 3, 4\}$, $B = \{a, b, c, d\}$ y $f : A \to B$ definida por

$$f = \{(1, a), (2, b), (3, c), (4, d)\}.$$

Como f se compone de pocos elementos, podemos graficar a f utilizando diagramas de Venn (ver Figura 3.19).

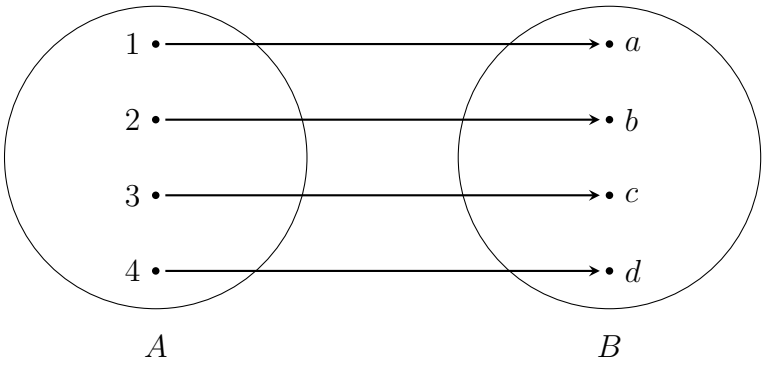


Figura 3.19: Diagrama de Venn de una función biyectiva.

Notemos que a cada elemento de B llega al menos una flecha (esto dice que f es sobreyectiva). Además, a cada elemento de B llega exactamente una flecha (esto dice que f es inyectiva). Esto nos dice que f es biyectiva.

3.6. Composición de funciones

Sean dos funciones $f : A \to B$ y $g : B \to C$. Como las funciones son en particular relaciones, queda definida la relación $g \circ f$ tal como se definió en la Sección 2.4. Lo que veremos a continuación es que la relación $g \circ f$ es en realidad una función.

Proposición 3.1
Sean dos funciones $f : A \to B$ y $g : B \to C$. Entonces la relación $g \circ f \subset A \times C$ es una función de A en C tal que:

$$\forall a \in A, \quad (g \circ f)(a) = g(f(a)).$$

Demostración.
Primero veamos que $g \circ f$ satisface la condición de existencia. Sea $a \in A$ fijo. Como f es función se tiene que existe $b \in B$ tal que $(a, b) \in f$ (en efecto, el único b que satisface esto es $f(a)$). Luego, como $b \in B$ y g es función, se tiene que existe $c \in C$ tal que $(b, c) \in g$ (de hecho, el único c que satisface esto es $g(b)$). Por la Definición 2.3 (composición de relaciones) se tiene que $(a, c) \in g \circ f$ (de hecho, $c = g(b) = g(f(a))$).

Ahora veamos que $g \circ f$ satisface la condición de unicidad. Supongamos que $(a, c), (a, \hat{c}) \in g \circ f$. Por Definición 2.3 (composición de relaciones) se tiene que:

$$\begin{aligned} (a, c) \in g \circ f &\Rightarrow \exists b \in B : (a, b) \in f \text{ y } (b, c) \in g \\ (a, \hat{c}) \in g \circ f &\Rightarrow \exists \hat{b} \in B : \left(a, \hat{b}\right) \in f \text{ y } \left(\hat{b}, \hat{c}\right) \in g \end{aligned}$$

Como f es función y $(a,b), \left(a,\hat{b}\right) \in f$ se tiene que $b = \hat{b}$. Luego $(b,c), (b,\hat{c}) \in g$, pero como g es función se deduce que $c = \hat{c}$.

Luego $g \circ f$ es una función y para cada $a \in A$ se tiene que $(g \circ f)(a) = g(f(a))$. ■

Observación 3.1
Sea $f : A \to B$ una función y $\tilde{A} \subset A$. Se define la restricción de f a $\tilde{A}$ a la función $f|_{\tilde{A}} : \tilde{A} \to B$ definida por:

$$f|_{\tilde{A}}(x) = f(x), \quad x \in \tilde{A}$$

En otras palabras, $f|_{\tilde{A}}$ es considerar a la función f definida en un subconjunto de A.

Observación 3.2
Sean dos funciones $f : A \to B$ y $g : C \to D$ tal que $\mathrm{Im}(f) \subset \mathrm{Dom}(g)$. Aún cuando no se satisfacen las condiciones de la Proposición 3.1, se puede extender el resultado de la Proposición 3.1 considerando las funciones $f : A \to \mathrm{Im}(f)$ y $g|_{\mathrm{Im}(f)} : \mathrm{Im}(f) \to D$.

Ejemplo 3.11
(a) Sean $A = \{1,2,3\}$, $B = \{a,b,c,d\}$, $C = \{5,6\}$, y las funciones $f : A \to B$ y $g : B \to C$ definidas de la siguiente manera:

$$\begin{aligned} f &= \{(1,a),(2,b),(3,d)\}, \\ g &= \{(a,5),(b,5),(c,5),(d,6)\}, \end{aligned}$$

entonces

$$g \circ f = \{(1,5),(2,5),(3,6)\}.$$

El diagrama de Venn correspondiente puede verse en la Figura 3.20.

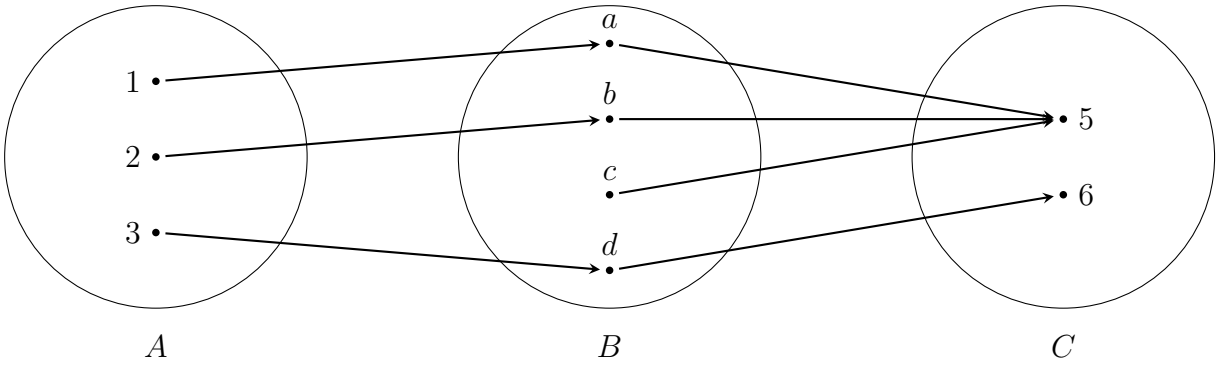


Figura 3.20: Ejemplo de composición de funciones.

(b) Sean $A = \{1,2,3\}$, $B = \{a,b,c\}$, $C = \{a,b,c,d\}$, $D = \{5,6\}$, y las funciones $f : A \to B$ y $g : C \to D$ definidas de la siguiente manera:

$$\begin{aligned} f &= \{(1,a),(2,b),(3,c)\}, \\ g &= \{(a,5),(b,5),(c,6),(d,5)\}, \end{aligned}$$

entonces

$$g \circ f = \{(1,5),(2,5),(3,6)\}.$$

El diagrama de Venn correspondiente puede verse en la Figura 3.21.

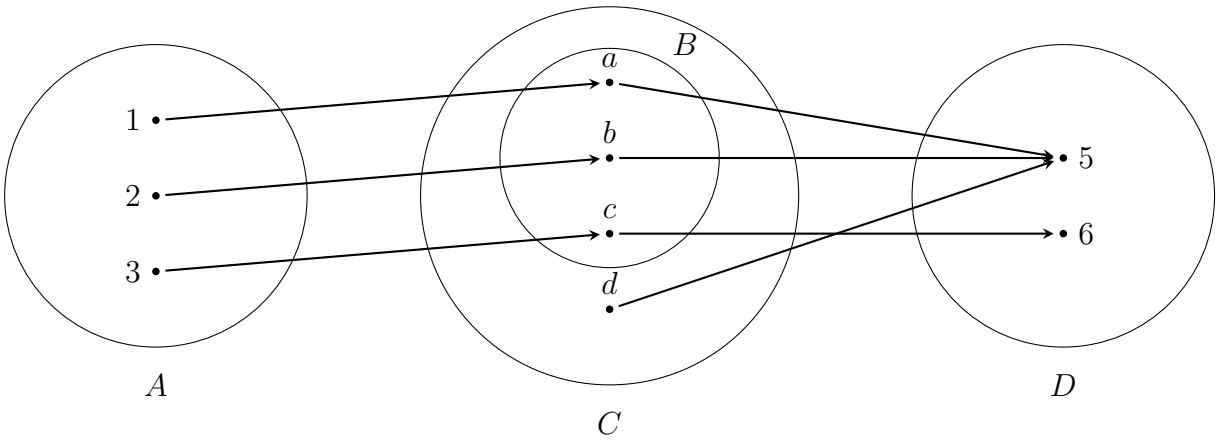


Figura 3.21: Ejemplo de composición de funciones.

(c) Sean $f : \mathbb{R} \to \mathbb{R}$ y $g : \mathbb{R} \to \mathbb{R}$ definidas por

$$\begin{aligned} f(x) &= x^2 + 1, \\ g(x) &= \sqrt[3]{x+1}. \end{aligned}$$

Luego,

$$\begin{aligned} (g \circ f)(x) &= g(f(x)) \text{ por Proposición 3.1} \\ &= g\left(x^2+1\right) \text{ por definición de } f \\ &= \sqrt[3]{(x^2+1)+1} \text{ por definición de } g \\ &= \sqrt[3]{x^2+2}. \end{aligned}$$

(d) Sean $f : \mathbb{R} \to (-1, \infty)$ y $g : \mathbb{R} - \{0\} \to \mathbb{R}$ definidas por

$$\begin{aligned} f(x) &= x^2 + 1, \\ g(x) &= \frac{x+1}{x}. \end{aligned}$$

Se puede ver que $\text{Im}(f) = [1, \infty)$ y que $\text{Dom}(g) = \mathbb{R} - \{0\}$. Como se cumple que $\text{Im}(f) \subset \text{Dom}(g)$ la composición puede realizarse, quedando:

$$\begin{aligned} (g \circ f)(x) &= g(f(x)) \text{ por Proposición 3.1 y Observación 3.2} \\ &= g\left(x^2+1\right) \text{ por definición de } f \\ &= \frac{x^2+1+1}{x^2+1} \text{ por definición de } g \\ &= \frac{x^2+2}{x^2+1}. \end{aligned}$$

Proposición 3.2
Sean $f : A \to B$, $g : B \to C$ y $h : C \to D$ funciones. Entonces:

(a) La composición es asociativa: $(h \circ g) \circ f = h \circ (g \circ f)$.

(b) Si f y g son inyectivas, entonces $g \circ f$ es inyectiva.

(c) Si f y g son sobreyectivas, entonces $g \circ f$ es sobreyectiva.

Demostración.
(a) Esta es una consecuencia directa de la Proposición 2.1-(a).

(b) Sean $u, v \in A$. Ahora

$$\begin{aligned} (g \circ f)(u) = (g \circ f)(v) &\Rightarrow g(f(u)) = g(f(v)) \text{ por Proposición 3.1} \\ &\Rightarrow f(u) = f(v) \text{ pues } g \text{ es inyectiva} \\ &\Rightarrow u = v \text{ pues } f \text{ es inyectiva} \end{aligned}$$

Luego $g \circ f$ es inyectiva.

(c) Sean w un elemento de C. Ahora:

$$\begin{aligned} &\exists v \in B : w = g(v) \text{ pues } g \text{ es sobreyectiva} \\ &\exists u \in A : v = f(u) \text{ pues } f \text{ es sobreyectiva} \\ &w = g(v) = g(f(u)) = (g \circ f)(u) \text{ por lo de arriba y por la Proposición 3.1} \end{aligned}$$

Luego $g \circ f$ es sobreyectiva. ■

3.7. Funciones inversas

Definición 3.5
Diremos que una función $f : A \to B$ admite inversa si y sólo si existe una función $g : B \to A$ tal que

$$g \circ f = i_A{}^{7}, \qquad f \circ g = i_B.$$

Proposición 3.3
Una función $f : A \to B$ admite inversa si y sólo si f es una función biyectiva. Además la relación inversa f^{-1} es la única función inversa de f.

Demostración.
Supongamos primero que f admite inversa. Por Definición 3.5 existe una función $g : B \to A$ tal que $g \circ f = i_A$ y $f \circ g = i_B$. Veamos primero que f es inyectiva: en efecto, si $x, \hat{x} \in A$:

$$\begin{aligned} f(x) = f(\hat{x}) &\Rightarrow g(f(x)) = g(f(\hat{x})) \\ &\Rightarrow i_A(x) = i_A(\hat{x}) \\ &\Rightarrow x = \hat{x} \end{aligned}$$

Veamos ahora que f es sobreyectiva. Tomemos $y \in B$, luego:

$$i_B(y) = y \Rightarrow (f \circ g)(y) = y \Rightarrow f(g(y)) = y.$$

Esto dice que existe un elemento en A, a saber $g(y)$, tal que $f(g(y)) = y$, lo cual implica que f es sobreyectiva. Como f es inyectiva y sobreyectiva tenemos que f es biyectiva.

Supongamos ahora que f es biyectiva. Veamos que f^{-1} (la relación inversa de f) es en realidad una función, para lo cual debemos chequear las condiciones de existencia y unicidad. Comprobemos la existencia:

$$\begin{aligned} y \in B &\Rightarrow \exists x \in A : f(x) = y \text{ pues } f \text{ es sobreyectiva} \\ &\Rightarrow \exists x \in A : (x, y) \in f \end{aligned}$$

[7] Recordemos que dado un conjunto A, la función $i_A : A \to A$ se definía como la función identidad, es decir $i_A(x) = x$ para cada $x \in A$.

$$\Rightarrow \quad \exists x \in A : (y, x) \in f^{-1} \text{ por Definición 2.2-(c) (relación inversa)}$$

Comprobemos la unicidad: sean $(b, a), (b, \hat{a}) \in f^{-1}$, luego

$$\begin{aligned}(b, a), (b, \hat{a}) \in f^{-1} &\Rightarrow (a, b), (\hat{a}, b) \in f \text{ por Definición 2.2-(c) (relación inversa)} \\ &\Rightarrow b = f(a) = f(\hat{a}) \\ &\Rightarrow a = \hat{a} \text{ pues } f \text{ es inyectiva}\end{aligned}$$

Veamos ahora que $f^{-1} \circ f = i_A$:

$$\begin{aligned}x \in A &\Leftrightarrow (x, f(x)) \in f \text{ pues } f \text{ es función} \\ &\Leftrightarrow (f(x), x) \in f^{-1} \text{ por Definición 2.2-(c) (relación inversa)} \\ &\Leftrightarrow f^{-1}(f(x)) = x \text{ pues } f^{-1} \text{ es función} \\ &\Leftrightarrow \left(f^{-1} \circ f\right)(x) = x \text{ por Proposición 3.1} \\ &\Leftrightarrow \left(f^{-1} \circ f\right)(x) = i_A(x)\end{aligned}$$

Análogamente veamos que $f \circ f^{-1} = i_B$:

$$\begin{aligned}y \in B &\Leftrightarrow \left(y, f^{-1}(y)\right) \in f^{-1} \text{ pues } f^{-1} \text{ es función} \\ &\Leftrightarrow \left(f^{-1}(y), y\right) \in f \text{ por Definición 2.2-(c) (relación inversa)} \\ &\Leftrightarrow f\left(f^{-1}(y)\right) = y \text{ pues } f \text{ es función} \\ &\Leftrightarrow \left(f \circ f^{-1}\right)(y) = y \text{ por Proposición 3.1} \\ &\Leftrightarrow \left(f \circ f^{-1}\right)(y) = i_B(y)\end{aligned}$$

Luego f^{-1} es una función inversa para f. Supongamos ahora que existe otra función $g : B \to A$ que es inversa de f. Luego se tiene que

$$\begin{aligned}g &= g \circ i_B \\ &= g \circ \left(f \circ f^{-1}\right) \text{ pues } f^{-1} \text{ es una inversa de } f \\ &= (g \circ f) \circ f^{-1} \text{ por Proposición 3.2-(a) (asociativa de la composición)} \\ &= i_A \circ f^{-1} \text{ pues } g \text{ es una inversa de } f \\ &= f^{-1}\end{aligned}$$

Por lo tanto f^{-1} es la única función inversa de f. ■

Una función biyectiva establece una correspondencia biunívoca entre A y B, es decir A y B son "iguales" salvo por el nombre de los elementos.

Ejemplo 3.12
Consideremos la función $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = 2 \cdot x + 1$ del Ejemplo 3.8-(c). Se había demostrado que f es inyectiva. Veamos si es sobreyectiva, para lo cual tomemos $y \in \mathbb{R}$. Buscamos $x \in \mathbb{R}$ tal que $y = f(x)$, es decir:

$$\begin{aligned}y = f(x) &\Leftrightarrow y = 2 \cdot x + 1 \\ &\Leftrightarrow y - 1 = 2 \cdot x \\ &\Leftrightarrow \frac{y - 1}{2} = x\end{aligned}$$

Esto último dice que hemos encontrado el x buscado, o sea f resulta sobreyectiva. Por lo tanto f es biyectiva y en consecuencia admite función inversa f^{-1}. El procedimiento anterior nos da también la fórmula de la función inversa de f:

$$f^{-1}(y) = \frac{y - 1}{2}.$$

Proposición 3.4
Sean $f : A \to B$ y $g : B \to C$ funciones biyectivas. Entonces $g \circ f$ es biyectiva y además:

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

Demostración.

Por Proposición 3.2-(b) y 3.2-(c) se tiene que $g \circ f$ es una función inyectiva y sobreyectiva, y por lo tanto biyectiva. La fórmula es una consecuencia directa de la Proposición 2.1-(b). ■

4. LOS NÚMEROS REALES

4.1. Concepto

En este capítulo estudiaremos los números reales denotados por $\mathbb{R}$. La construcción que veremos es una formalización de lo que hemos visto en la escuela secundaria. Por el momento no nos interesa estudiar quiénes son los elementos de este conjunto, sino de las propiedades que cumplen.

Por ahora diremos que $\mathbb{R}$ es un conjunto con dos operaciones binarias denominadas suma y producto:

$$\begin{aligned} + &: \mathbb{R} \times \mathbb{R} \to \mathbb{R}, \quad \text{suma}, \\ \cdot &: \mathbb{R} \times \mathbb{R} \to \mathbb{R}, \quad \text{producto}, \end{aligned}$$

y una relación de orden estricto que representaremos con el símbolo $<$.

La suma, el producto y la relación cumplirán ciertas propiedades básicas que llamaremos axiomas y que consideraremos válidos de aquí en adelante:

(S1) Asociativa de la suma:

$$\forall a, b, c \in \mathbb{R}, \quad a + (b + c) = (a + b) + c.$$

(S2) Conmutativa de la suma:

$$\forall a, b \in \mathbb{R}, \quad a + b = b + a.$$

(S3) Existencia del elemento neutro para la suma:

$$\exists 0 \in \mathbb{R} : \forall a \in \mathbb{R}, \quad a + 0 = a.$$

(S4) Existencia del elemento opuesto para la suma:

$$\forall a \in \mathbb{R}, \exists a' \in \mathbb{R} : \quad a + a' = 0.$$

(P1) Asociativa del producto:

$$\forall a, b, c \in \mathbb{R}, \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

(P2) Conmutativa del producto:

$$\forall a, b \in \mathbb{R}, \quad a \cdot b = b \cdot a.$$

(P3) Existencia del elemento neutro para el producto:

$$\exists 1 \in \mathbb{R}, 1 \neq 0 : \forall a \in \mathbb{R}, \quad a \cdot 1 = a.$$

(P4) Existencia del elemento inverso para el producto:

$$\forall a \in \mathbb{R}, a \neq 0, \exists a'' \in \mathbb{R} : \quad a \cdot a'' = 1.$$

(D) Distributiva del producto respecto de la suma:

$$\forall a, b, c \in \mathbb{R}, \quad a \cdot (b + c) = a \cdot b + a \cdot c.$$

(O1) Tricotomía:

$$\forall a, b \in \mathbb{R}, \quad a < b \veebar a = b \veebar a > b.$$

(O2) Transitiva:

$$\forall a, b, c \in \mathbb{R}, \quad a < b \wedge b < c \Rightarrow a < c.$$

(SC) Consistencia de la relación de orden respecto de la suma:

$$\forall a, b, c \in \mathbb{R}, \quad a < b \Rightarrow a + c < b + c.$$

(PC) Consistencia de la relación de orden respecto del producto:

$$\forall a, b, c \in \mathbb{R}, \quad a < b \wedge c > 0 \Rightarrow a \cdot c < b \cdot c.$$

En virtud de los Axiomas (S1)-(PC) diremos que (por el momento) $\mathbb{R}$ es un cuerpo ordenado. También notemos que se pide que $\mathbb{R}$ tenga al menos dos elementos distintos: el 0 y el 1.

Debido a los Axiomas (S1) y (P1) se puede sumar o multiplicar agrupando de cualquier manera. Por ello se suelen ver expresiones tales como:

$$a + b + c,$$
$$a \cdot b \cdot c.$$

En general, si tenemos números reales $a_0, a_1, \ldots, a_n$ se denota la suma y producto entre ellos de la siguiente manera:

$$\begin{aligned} a_1 + a_2 + \ldots + a_n &= \sum_{i=1}^{n} a_i, \\ a_1 \cdot a_2 \cdot \ldots \cdot a_n &= \prod_{i=1}^{n} a_i. \end{aligned}$$

Además existe un orden de precedencia (o preferencia) cuando aparecen operaciones de manera mixta. La operación de producto tiene mayor precedencia que la operación de suma, en el sentido que la operación de producto debe realizarse primero. Por ejemplo:

$$a + b \cdot c,$$

debe realizarse haciendo los siguientes pasos:

$$b \cdot c$$
$$a + b \cdot c$$

En cambio, si queremos modificar la precedencia deben utilizarse los paréntesis, corchetes o llaves. Por ejemplo,

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

debe realizarse haciendo los siguientes pasos:

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

4.2. Propiedades de los elementos neutros, opuestos e inversos

A partir de los Axiomas (S1)-(S4), (P1)-(P4), (D), (O1)-(O2), (SC) y (PC) se pueden demostrar otras propiedades.

Teorema 4.1
Se cumplen las siguientes propiedades:

$$\begin{aligned} 0+0 &= 0, \\ 1\cdot 1 &= 1. \end{aligned}$$

Demostración.
Del Axioma (S3) se tiene que (eligiendo en particular $a = 0$): $0 + 0 = 0$.
Del Axioma (P3) se tiene que (eligiendo en particular $a = 1$): $1 \cdot 1 = 1$. ■

Teorema 4.2
Sean a y b números reales.

(a) Existe un único $x \in \mathbb{R}$ tal que

$$a + x = b. \tag{5}$$

(b) Si $a \neq 0$, existe un único $x \in \mathbb{R}$ tal que

$$a \cdot x = b. \tag{6}$$

Demostración.
(a) Primero analicemos la existencia. Definimos $x = a' + b$, donde a' es el opuesto de a (ver Axioma (S4)). Ahora veamos que este x satisface la ecuación (5):

$$\begin{aligned} a + x &= a + (a' + b) \text{ por definición de } x \\ &= (a + a') + b \text{ por Axioma (S1) (asociativa de la suma)} \\ &= 0 + b \text{ por Axioma (S4) (elemento opuesto para la suma)} \\ &= b + 0 \text{ por Axioma (S2) (conmutativa de la suma)} \\ &= b \text{ por Axioma (S3) (elemento neutro de la suma)} \end{aligned}$$

Ahora analicemos la unicidad. Supongamos que existe un elemento $y \in \mathbb{R}$ tal que

$$a + y = b. \tag{7}$$

Ahora se tiene que:

$$\begin{aligned} x &= a' + b \text{ por la definición de } x \\ &= a' + (a + y) \text{ pues } y \text{ satisface (7)} \\ &= (a' + a) + y \text{ por Axioma (S1) (asociativa de la suma)} \\ &= (a + a') + y \text{ por Axioma (S2) (conmutativa de la suma)} \\ &= 0 + y \text{ por Axioma (S4) (elemento neutro de la suma)} \\ &= y + 0 \text{ por Axioma (S2) (conmutativa de la suma)} \\ &= y \text{ por Axioma (S3) (elemento neutro de la suma)} \end{aligned}$$

(b) Primero analicemos la existencia. Definimos $x = a'' \cdot b$, donde a'' es el inverso de a (ver Axioma (P4) junto al hecho que $a \neq 0$). Ahora veamos que este x satisface la ecuación (6):

$$\begin{aligned} a \cdot x &= a \cdot (a'' \cdot b) \text{ por definición de } x \\ &= (a \cdot a'') \cdot b \text{ por Axioma (P1) (asociativa del producto)} \\ &= 1 \cdot b \text{ por Axioma (P4) (elemento inverso del producto)} \\ &= b \cdot 1 \text{ por Axioma (P2) (conmutativa del producto)} \\ &= b \text{ por Axioma (P3) (elemento neutro del producto)} \end{aligned}$$

Ahora analicemos la unicidad. Supongamos que existe un elemento $y \in \mathbb{R}$ tal que

$$a \cdot y = b. \tag{8}$$

Ahora se tiene que:

$$\begin{aligned} x &= a'' \cdot b \text{ por definición de } x \\ &= a'' \cdot (a \cdot y) \text{ pues } y \text{ satisface (8)} \\ &= (a'' \cdot a) \cdot y \text{ por Axioma (P1) (asociativa del producto)} \\ &= (a \cdot a'') \cdot y \text{ por Axioma (P2) (conmutativa del producto)} \\ &= 1 \cdot y \text{ por Axioma (P4) (elemento inverso del producto)} \\ &= y \cdot 1 \text{ por Axioma (P2) (conmutativa del producto)} \\ &= y \text{ por Axioma (P3) (elemento neutro del producto)} \end{aligned}$$

Esto concluye la demostración. ■

Corolario 4.1 (Unicidad del elemento opuesto e inverso)

(a) Dado $a \in \mathbb{R}$ existe un único elemento opuesto de a, es decir, existe un único a' tal que

$$a + a' = 0.$$

(b) Dado $a \in \mathbb{R}$ tal que $a \neq 0$, existe un único elemento inverso de a, es decir, existe un único a'' tal que

$$a \cdot a'' = 1.$$

Demostración.
(a) Utilizar el Teorema 4.2-(a) con $b = 0$.

(b) Utilizar el Teorema 4.2-(b) con $b = 1$. ■

Debido al Corolario 4.1, se realiza la siguiente definición.

Definición 4.1 (Notación para el elemento opuesto e inverso)

(a) Dado $a \in \mathbb{R}$, al único número real a' que verifica $a + a' = 0$ lo denotaremos por $-a$. Además, también como notación, en lugar de escribir $b + (-a)$ vamos a escribir $b - a$.

(b) Dado $a \in \mathbb{R}$ tal que $a \neq 0$, al único número real a'' que verifica $a \cdot a'' = 1$ lo denotaremos por a^{-1}.

Teorema 4.3 (Unicidad del elemento neutro para la suma y el producto)

(a) Supongamos que existe un número real 0^* tal que $a + 0^* = a$ para todo $a \in \mathbb{R}$. Entonces $0^* = 0$.

(b) Supongamos que existe un número real $1^* \neq 0$ tal que $a \cdot 1^* = a$ para todo $a \in \mathbb{R}$. Entonces $1^* = 1$.

Demostración.
(a) Por el Teorema 4.1 se tiene que

$$0 + 0 = 0.$$

Por hipótesis, 0^* es también un elemento neutro para la suma. En particular vale que:

$$0 + 0^* = 0.$$

Luego 0 y 0^* son soluciones de la ecuación $0 + x = 0$. Por Teorema 4.2-(a) se obtiene que $0 = 0^*$.

(b) Por el Teorema 4.1 se tiene que

$$1 \cdot 1 = 1.$$

Por hipótesis, 1^* es también un elemento neutro para el producto. En particular vale que:

$$1 \cdot 1^* = 1.$$

Luego 1 y 1^* son soluciones de la ecuación $1 \cdot x = 1$. Por Teorema 4.2-(b) se obtiene que $1 = 1^*$.■

4.3. Propiedades básicas

Teorema 4.4 (Propiedad cancelativa)
Sean a, b y c números reales.

(a) $a + b = a + c \Leftrightarrow b = c$.

(b) Si $a \neq 0$, *entonces* $a \cdot b = a \cdot c \Leftrightarrow b = c$.

Demostración.
(a) Si suponemos que $b = c$, entonces es obvio que $a + b = a + c$.
Asumamos ahora que $a + b = a + c$. Sea $d = a + b$ (o lo que es lo mismo, $d = a + c$). Ahora

$$\begin{aligned} a + b &= d, \\ a + c &= d. \end{aligned}$$

Luego, por Teorema 4.2-(a) tenemos que $b = c$.

(b) Si suponemos que $b = c$, entonces es obvio que $a \cdot b = a \cdot c$.
Asumamos ahora que $a \cdot b = a \cdot c$. Sea $d = a \cdot b$ (o lo que es lo mismo, $d = a \cdot c$). Ahora

$$\begin{aligned} a \cdot b &= d, \\ a \cdot c &= d. \end{aligned}$$

Luego, por Teorema 4.2-(b) tenemos que $b = c$. ■

Definición 4.2
Dado $a \in \mathbb{R}$, denotaremos

(a) $a^2 = a \cdot a, \quad 2 \cdot a = a + a.$

(b) $a^3 = a \cdot a \cdot a, \quad 3 \cdot a = a + a + a.$

(c) $a^4 = a \cdot a \cdot a \cdot a, \quad 4 \cdot a = a + a + a + a.$

$\vdots$

Teorema 4.5 (Propiedades)
Sean a, b, c y d números reales.

(a) $a = b \Leftrightarrow a - b = 0$.

(b) $a + a = a \Leftrightarrow a = 0$.

(c) $a = -(-a)$.

(d) $0 = -0$.

(e) $a \cdot 0 = 0$.

(f) $(-1) \cdot a = -a$.

(g) $a = b \Leftrightarrow -a = -b$.

(h) $a = 0 \Leftrightarrow -a = 0$ *(o equivalentemente* $a \neq 0 \Leftrightarrow -a \neq 0$*).*

(i) $a \cdot b = 0 \Leftrightarrow a = 0$ *o* $b = 0$ *(o equivalentemente* $a \cdot b \neq 0 \Leftrightarrow a \neq 0$ *y* $b \neq 0$*).*

(j) $-(a + b) = (-a) + (-b) = -a - b$.

(k) $-(a - b) = b - a$.

(l) $a + b = a - (-b)$.

(m) $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$. *Luego no hay ambigüedad en escribir* $-(a \cdot b) = -a \cdot b$.

(n) $(-a) \cdot (-b) = a \cdot b$.

(ñ) $(-a) \cdot (-b) \cdot (-c) = -(a \cdot b \cdot c)$.

(o) $a \cdot (b - c) = a \cdot b - a \cdot c$.

(p) $(a + b) \cdot (c + d) = a \cdot c + a \cdot d + b \cdot c + b \cdot d$.

(q) $(a + b) \cdot (a - b) = a^2 - b^2$.

(r) $a^2 = 1 \Leftrightarrow a = 1$ *o* $a = -1$.

(s) $1 = 1^{-1}$.

(t) $(-1)^{-1} = -1$.

(u) Si $a \neq 0$ *entonces* $a^{-1} \neq 0$.

(v) Si $a \neq 0$ *entonces* $(-a)^{-1} = -a^{-1}$.

(w) Si $a \neq 0$ *entonces* $(a^{-1})^{-1} = a$.

(x) Si $a \neq 0$ *y* $b \neq 0$ *entonces* $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$.

(y) $(a + b)^2 = a^2 + 2 \cdot a \cdot b + b^2$.

Demostración.
(a) Demostraremos que $a = b \Leftrightarrow a - b = 0$. Vamos a demostrar las dos implicaciones por separado.

$$\begin{aligned} a = b &\Rightarrow a + (-b) = b + (-b) \text{ sumando } -b \text{ a ambos miembros} \\ &\Rightarrow a - b = 0 \text{ por Definición 4.1-(a) y Axioma (S4) (elemento opuesto de la suma)} \end{aligned}$$

$$\begin{aligned} a - b = 0 &\Rightarrow a + (-b) = 0 \text{ por Definición 4.1-(a)} \\ &\Rightarrow [a + (-b)] + b = 0 + b \text{ sumando } b \text{ a ambos miembros} \\ &\Rightarrow a + [(-b) + b] = 0 + b \text{ por Axioma (S1) (asociativa de la suma)} \\ &\Rightarrow a + [b + (-b)] = b + 0 \text{ por Axioma (S2) (conmutativa de la suma)} \\ &\Rightarrow a + 0 = b + 0 \text{ por Axioma (S4) (elemento opuesto de la suma)} \\ &\Rightarrow a = b \text{ por Axioma (S3) (elemento neutro de la suma)} \end{aligned}$$

(b) Tenemos que demostrar que $a + a = a \Leftrightarrow a = 0$. Vamos a demostrar las dos implicaciones por separado.

Supongamos primero que $a + a = a$. Por otro lado, por Axioma (S3) se tiene que $a + 0 = a$. Luego, a y 0 son soluciones de la ecuación $a + x = a$. Por Teorema 4.2-(a) obtenemos que $a = 0$.

Supongamos ahora que $a = 0$. Ahora

$$\begin{aligned} a + a &= 0 + 0 \text{ por hipótesis} \\ &= 0 \text{ por Teorema 4.1} \\ &= a \text{ por hipótesis} \end{aligned}$$

(c) Demostraremos que $a = -(-a)$.

Por Axioma (S4) se tiene que $a + (-a) = 0$, pero usando el Axioma (S2) se deduce que:

$$(-a) + a = 0.$$

Además

$$(-a) + [-(-a)] = 0.$$

Luego a y $-(-a)$ son soluciones de la ecuación $(-a) + x = 0$. Por Teorema 4.2-(a) obtenemos que $a = -(-a)$.

(d) Vamos a demostrar que $0 = -0$.

Por Teorema 4.1 tenemos que $0 + 0 = 0$. Por Corolario 4.1-(a) el opuesto es único, por lo que $0 = -0$.

(e) Demostraremos que $a \cdot 0 = 0$.

$$\begin{aligned} a \cdot 0 &= a \cdot (0 + 0) \text{ por Teorema 4.1} \\ &= a \cdot 0 + a \cdot 0 \text{ por Axioma (D) (distributiva)} \end{aligned}$$

Luego $a \cdot 0 + a \cdot 0 = a \cdot 0$ y por (b) se tiene que $a \cdot 0 = 0$.

(f) Probaremos que $(-1) \cdot a = -a$.

$$a + (-1) \cdot a = a \cdot 1 + (-1) \cdot a \text{ por Axioma (P3) (elemento neutro del producto)}$$

$$
\begin{aligned}
&= a \cdot 1 + a \cdot (-1) \text{ por Axioma (P2) (conmutativa del producto)} \\
&= a \cdot [1 + (-1)] \text{ por Axioma (D) (distributiva)} \\
&= a \cdot 0 \text{ por Axioma (S4) (elemento opuesto de la suma)} \\
&= 0 \text{ por (e)}
\end{aligned}
$$

Por Corolario 4.1-(a) se tiene que $(-1) \cdot a = -a$.

(g) Tenemos que probar que $a = b \Leftrightarrow -a = -b$. Vamos a demostrar las dos implicaciones por separado.

$$
\begin{aligned}
a = b &\Rightarrow (-1) \cdot a = (-1) \cdot b \text{ multiplicando por } -1 \text{ a ambos miembros} \\
&\Rightarrow -a = -b \text{ por (f)}
\end{aligned}
$$

$$
\begin{aligned}
-a = -b &\Rightarrow -(-a) = -(-b) \text{ por lo demostrado arriba} \\
&\Rightarrow a = b \text{ por (c)}
\end{aligned}
$$

(h) Vamos a demostrar que $a = 0 \Leftrightarrow -a = 0$.

$$
\begin{aligned}
a = 0 &\Leftrightarrow -a = -0 \text{ por (g)} \\
&\Leftrightarrow -a = 0 \text{ por (d)}
\end{aligned}
$$

(i) Demostraremos que $a \cdot b = 0 \Leftrightarrow a = 0$ o $b = 0$. Vamos a demostrar las dos implicaciones por separado.

Supongamos primero que $a \cdot b = 0$. Si $b = 0$ listo. Ahora supongamos que $b \neq 0$. Luego existe b^{-1} y

$$
\begin{aligned}
a \cdot b = 0 &\Rightarrow (a \cdot b) \cdot b^{-1} = 0 \cdot b^{-1} \text{ multiplicando ambos miembros por } b^{-1} \\
&\Rightarrow a \cdot \left(b \cdot b^{-1}\right) = 0 \cdot b^{-1} \text{ por Axioma (P1) (asociativa del producto)} \\
&\Rightarrow a \cdot 1 = 0 \cdot b^{-1} \text{ por Axioma (P4) (elemento inverso del producto)} \\
&\Rightarrow a = 0 \cdot b^{-1} \text{ por Axioma (P3) (elemento neutro del producto)} \\
&\Rightarrow a = b^{-1} \cdot 0 \text{ por Axioma (P2) (conmutativa del producto)} \\
&\Rightarrow a = 0 \text{ por (e)}
\end{aligned}
$$

Supongamos ahora que $a = 0$ o $b = 0$. Debido al Axioma (P2) podemos asumir, sin pérdida de generalidad, que $b = 0$. Ahora $a \cdot b = a \cdot 0 = 0$ debido a (e).

(j) Vamos a probar que $-(a + b) = (-a) + (-b) = -a - b$.

$$
\begin{aligned}
-(a + b) &= (-1) \cdot (a + b) \text{ por (f)} \\
&= (-1) \cdot a + (-1) \cdot b \text{ por Axioma (D) (distributiva)} \\
&= (-a) + (-b) \text{ por (f)}
\end{aligned}
$$

La igualdad $(-a) + (-b) = -a - b$ surge de la Definición 4.1-(a).

(k) Demostraremos que $-(a - b) = b - a$.

$$
-(a - b) = -a - (-b) \text{ por (j)}
$$

$$
\begin{aligned}
&= -a + b \text{ por (c)} \\
&= b - a \text{ por Axioma (S2) (conmutativa de la suma)}
\end{aligned}
$$

(l) Probaremos que $a + b = a - (-b)$.

$$
\begin{aligned}
a + b &= a + [-(-b)] \text{ por (c)} \\
&= a - (-b) \text{ por Definición 4.1-(a)}
\end{aligned}
$$

(m) Vamos a demostrar que $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$.

$$
\begin{aligned}
-(a \cdot b) &= (-1) \cdot (a \cdot b) \text{ por (f)} \\
&= [(-1) \cdot a] \cdot b \text{ por Axioma (P1) (asociativa del producto)} \\
&= (-a) \cdot b \text{ por (f)}
\end{aligned}
$$

$$
\begin{aligned}
-(a \cdot b) &= (-1) \cdot (a \cdot b) \text{ por (f)} \\
&= (a \cdot b) \cdot (-1) \text{ por Axioma (P2) (conmutativa del producto)} \\
&= a \cdot [b \cdot (-1)] \text{ por Axioma (P1) (asociativa del producto)} \\
&= a \cdot [(-1) \cdot b] \text{ por Axioma (P2) (conmutativa del producto)} \\
&= a \cdot (-b) \text{ por (f)}
\end{aligned}
$$

(n) Vamos a probar que $(-a) \cdot (-b) = a \cdot b$.

$$
\begin{aligned}
[-(a \cdot b)] + (-a) \cdot (-b) &= (-a) \cdot b + (-a) \cdot (-b) \text{ por (m)} \\
&= (-a) \cdot [b + (-b)] \text{ por Axioma (D) (distributiva)} \\
&= (-a) \cdot 0 \text{ por Axioma (S4) (elemento opuesto de la suma)} \\
&= 0 \text{ por (e)}
\end{aligned}
$$

Luego:

$$
\begin{aligned}
(-a) \cdot (-b) &= -[-(a \cdot b)] \text{ por Corolario 4.1-(a)} \\
&= a \cdot b \text{ por (c)}
\end{aligned}
$$

(ñ) Demostraremos que $(-a) \cdot (-b) \cdot (-c) = -(a \cdot b \cdot c)$.

$$
\begin{aligned}
(-a) \cdot (-b) \cdot (-c) &= (a \cdot b) \cdot (-c) \text{ por (n)} \\
&= -[(a \cdot b) \cdot c] \text{ por (m)} \\
&= -(a \cdot b \cdot c)
\end{aligned}
$$

(o) Probaremos que $a \cdot (b - c) = a \cdot b - a \cdot c$.

$$
\begin{aligned}
a \cdot (b - c) &= a \cdot [b + (-c)] \text{ por Definición 4.1-(a)} \\
&= a \cdot b + a \cdot (-c) \text{ por Axioma (D) (distributiva)} \\
&= a \cdot b + [-(a \cdot c)] \text{ por (m)}
\end{aligned}
$$

$$\begin{aligned} &= a \cdot b - (a \cdot c) \text{ por Definición 4.1-(a)} \\ &= a \cdot b - a \cdot c \text{ por (m)} \end{aligned}$$

(p) Vamos a demostrar que $(a+b)\cdot(c+d) = a\cdot c + a\cdot d + b\cdot c + b\cdot d$.

$$\begin{aligned} (a+b)\cdot(c+d) &= (a+b)\cdot c + (a+b)\cdot d \text{ por Axioma (D) (distributiva)} \\ &= c\cdot(a+b) + d\cdot(a+b) \text{ por Axioma (P2) (conmutativa del producto)} \\ &= (c\cdot a + c\cdot b) + (d\cdot a + d\cdot b) \text{ por Axioma (D) (distributiva)} \\ &= c\cdot a + c\cdot b + d\cdot a + d\cdot b \text{ por Axioma (S1) (asociativa de la suma)} \\ &= a\cdot c + b\cdot c + a\cdot d + b\cdot d \text{ por Axioma (P2) (conmutativa del producto)} \\ &= a\cdot c + a\cdot d + b\cdot c + b\cdot d \text{ por Axioma (S2) (conmutativa de la suma)} \end{aligned}$$

(q) Vamos a probar que $(a+b)\cdot(a-b) = a^2 - b^2$.

$$\begin{aligned} (a+b)\cdot(a-b) &= (a+b)\cdot[a+(-b)] \text{ por Definición 4.1-(a)} \\ &= a\cdot a + a\cdot(-b) + b\cdot a + b\cdot(-b) \text{ por (p)} \\ &= a\cdot a - a\cdot b + b\cdot a - b\cdot b \text{ por (m)} \\ &= a\cdot a - a\cdot b + a\cdot b - b\cdot b \text{ por Axioma (P2) (conmutativa del producto)} \\ &= a\cdot a + a\cdot b - a\cdot b - b\cdot b \text{ por Axioma (S2) (conmutativa de la suma)} \\ &= a\cdot a + 0 - b\cdot b \text{ por (a)} \\ &= a\cdot a - b\cdot b \text{ por Axioma (S3) (elemento neutro de la suma)} \\ &= a^2 - b^2 \text{ por Definición 4.2} \end{aligned}$$

(r) Demostraremos que $a^2 = 1 \Leftrightarrow a = 1$ o $a = -1$.

$$\begin{aligned} a^2 = 1 &\Leftrightarrow a^2 = 1\cdot 1 \text{ por Teorema 4.1} \\ &\Leftrightarrow a^2 = 1^2 \text{ por Definición 4.2} \\ &\Leftrightarrow a^2 - 1^2 = 0 \text{ por (a)} \\ &\Leftrightarrow (a+1)\cdot(a-1) = 0 \text{ por (q)} \\ &\Leftrightarrow a+1 = 0 \text{ o } a-1 = 0 \text{ por (i)} \\ &\Leftrightarrow a-(-1) = 0 \text{ o } a-1 = 0 \text{ por (c)} \\ &\Leftrightarrow a = -1 \text{ o } a = 1 \text{ por (a)} \end{aligned}$$

(s) Probaremos que $1 = 1^{-1}$.
Como $1 \neq 0$ existe 1^{-1} tal que $1\cdot 1^{-1} = 1$ (por Axioma (P3) y Axioma (P4)).
Por otro lado, del Teorema 4.1 tenemos que $1\cdot 1 = 1$.
Por Corolario 4.1-(b) se tiene que $1 = 1^{-1}$.

(t) Vamos a demostrar que $(-1)^{-1} = -1$.
Recordemos que como $1 \neq 0$ (por Axioma (P3)) se tiene que $-1 \neq 0$ (por (h)).
Ahora, por (n) se tiene que $(-1)\cdot(-1) = 1\cdot 1$. Entonces

$$\begin{aligned} (-1)\cdot(-1) = 1\cdot 1 &\Rightarrow (-1)\cdot(-1) = 1 \text{ por Teorema 4.1} \\ &\Rightarrow (-1)^{-1} = -1 \text{ por Corolario 4.1-(b)} \end{aligned}$$

(u) Vamos a probar que si $a \neq 0$ entonces $a^{-1} \neq 0$.

Asumiendo que $a \neq 0$, por Axioma (P4), sabemos que existe a^{-1}. Si ocurriera que $a^{-1} = 0$ tendríamos que:

$$\begin{aligned} 1 &= a \cdot a^{-1} \text{ por Axioma (P4)} \\ &= a \cdot 0 \\ &= 0 \text{ por (e)} \end{aligned}$$

Pero esto es una contradicción pues $1 \neq 0$ (por Axioma (P3)).

(v) Demostraremos que si $a \neq 0$ entonces $(-a)^{-1} = -a^{-1}$.

Debido a (h), como $a \neq 0$ se tiene que $-a \neq 0$, por lo que existe $(-a)^{-1}$ (por Axioma (P4)). Ahora

$$\begin{aligned} (-a) \cdot \left(-a^{-1}\right) &= a \cdot a^{-1} \text{ por (n)} \\ &= 1 \text{ por Axioma (P4) (elemento inverso para el producto)} \end{aligned}$$

Luego, por Corolario 4.1-(b) tenemos que $(-a)^{-1} = -a^{-1}$.

(w) Probaremos que si $a \neq 0$ entonces $(a^{-1})^{-1} = a$.

Como $a \neq 0$ sabemos que $a^{-1} \neq 0$ por (u). Por Axioma (P4) sabemos que existe $(a^{-1})^{-1}$.

Además sabemos que $a \cdot a^{-1} = 1$, pero usando el Axioma (P2) se deduce que $a^{-1} \cdot a = 1$. Por Corolario 4.1-(b) el inverso es único, por lo que $(a^{-1})^{-1} = a$.

(x) Vamos a demostrar que si $a \neq 0$ y $b \neq 0$ entonces $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$.

Por Axioma (P4), como a y b son distintos de 0, entonces existen a^{-1} y b^{-1}. Además por (i) se tiene que $a \cdot b \neq 0$, por lo que existe $(a \cdot b)^{-1}$ por Axioma (P4). Ahora:

$$\begin{aligned} (a \cdot b) \cdot \left(a^{-1} \cdot b^{-1}\right) &= a \cdot b \cdot a^{-1} \cdot b^{-1} \text{ por Axioma (P1) (asociativa del producto)} \\ &= a \cdot a^{-1} \cdot b \cdot b^{-1} \text{ por Axioma (P2) (conmutativa del producto)} \\ &= \left(a \cdot a^{-1}\right) \cdot \left(b \cdot b^{-1}\right) \text{ por Axioma (P1) (asociativa del producto)} \\ &= 1 \cdot 1 \text{ por Axioma (P4) (elemento inverso para el producto)} \\ &= 1 \text{ por Axioma (P3) (elemento neutro del producto)} \end{aligned}$$

Luego, por Corolario 4.1-(b) tenemos que $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$.

(y) Vamos a probar que $(a+b)^2 = a^2 + 2 \cdot a \cdot b + b^2$.

$$\begin{aligned} (a+b)^2 &= (a+b) \cdot (a+b) \text{ por Definición 4.2} \\ &= a \cdot a + a \cdot b + b \cdot a + b \cdot b \text{ por (p)} \\ &= a \cdot a + a \cdot b + a \cdot b + b \cdot b \text{ por Axioma (S2) (conmutativa de la suma)} \\ &= a^2 + 2 \cdot a \cdot b + b^2 \text{ por Definición 4.2} \end{aligned}$$

■

4.4. Fracciones

Definición 4.3 (Fracciones)

Sean a y b números reales con $b \neq 0$. El número $a \cdot b^{-1}$ se denota de la siguiente manera:

$$a \cdot b^{-1} = \frac{a}{b} = a/b.$$

Teorema 4.6 (Propiedades de las fracciones)
Sean a, b, c y d números reales. Luego,

(a) Si $b \neq 0$ entonces $b^{-1} = \dfrac{1}{b}$.

(b) Si $b \neq 0$ entonces $\dfrac{0}{b} = 0$.

(c) $\dfrac{b}{1} = b$.

(d) Si $b \neq 0$ entonces

$$\begin{aligned} -\frac{a}{b} &= \frac{(-a)}{b} = \frac{a}{(-b)}, \\ \frac{(-a)}{(-b)} &= \frac{a}{b}. \end{aligned}$$

(e) Si $b \neq 0$ y $d \neq 0$ entonces

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow a \cdot d = b \cdot c.$$

(f) Si $b \neq 0$ y $d \neq 0$ entonces

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}.$$

(g) Si $b \neq 0$ y $d \neq 0$ entonces

$$\left(\frac{b}{d}\right)^{-1} = \frac{d}{b}.$$

(h) Si $b \neq 0$, $c \neq 0$ y $d \neq 0$ entonces

$$\frac{\dfrac{a}{b}}{\dfrac{c}{d}} = \frac{a \cdot d}{b \cdot c}.$$

(i) Si $b \neq 0$ y $d \neq 0$ entonces

$$\frac{a}{b} \pm \frac{c}{d} = \frac{a \cdot d \pm b \cdot c}{b \cdot d}.$$

Demostración.
(a) Demostraremos que si $b \neq 0$ entonces $b^{-1} = \dfrac{1}{b}$.

$$\begin{aligned} b^{-1} &= b^{-1} \cdot 1 \text{ por Axioma (P3) (elemento neutro del producto)} \\ &= 1 \cdot b^{-1} \text{ por Axioma (P2) (conmutativa del producto)} \\ &= \frac{1}{b} \text{ por Definición 4.3} \end{aligned}$$

(b) Probaremos que si $b \neq 0$ entonces $\dfrac{0}{b} = 0$.

Como $b \neq 0$ entonces existe b^{-1}. Ahora:

$$\begin{aligned} \frac{0}{b} &= 0 \cdot b^{-1} \text{ por Definición 4.3} \\ &= b^{-1} \cdot 0 \text{ por Axioma (P2) (conmutativa del producto)} \\ &= 0 \text{ por Teorema 4.5-(e)} \end{aligned}$$

(c) Vamos a demostrar que $\frac{b}{1} = b$.
Recordemos que como $1 \neq 0$, existe 1^{-1}. Ahora:

$$\begin{aligned} \frac{b}{1} &= b \cdot 1^{-1} \text{ por Definición 4.3} \\ &= b \cdot 1 \text{ por Teorema 4.5-(s)} \\ &= b \text{ por Axioma (P3) (elemento neutro del producto)} \end{aligned}$$

(d) Vamos a probar que si $b \neq 0$ entonces $-\frac{a}{b} = \frac{(-a)}{b} = \frac{a}{(-b)}$:
Como $b \neq 0$ entonces existe b^{-1}. Ahora:

$$\begin{aligned} -\frac{a}{b} &= -a \cdot b^{-1} \text{ por Definición 4.3} \\ &= (-a) \cdot b^{-1} \text{ por Teorema 4.5-(m)} \\ &= \frac{(-a)}{b} \text{ por Definición 4.3} \end{aligned}$$

$$\begin{aligned} -\frac{a}{b} &= -a \cdot b^{-1} \text{ por Definición 4.3} \\ &= a \cdot \left(-b^{-1}\right) \text{ por Teorema 4.5-(m)} \\ &= a \cdot (-b)^{-1} \text{ por Teorema 4.5-(v)} \\ &= \frac{a}{(-b)} \text{ por Definición 4.3} \end{aligned}$$

Vamos a probar que si $b \neq 0$ entonces $\frac{(-a)}{(-b)} = \frac{a}{b}$.

$$\begin{aligned} \frac{(-a)}{(-b)} &= (-a) \cdot (-b)^{-1} \text{ por Definición 4.3} \\ &= (-a) \cdot \left(-b^{-1}\right) \text{ por Teorema 4.5-(v)} \\ &= a \cdot b^{-1} \text{ por Teorema 4.5-(n)} \\ &= \frac{a}{b} \text{ por Definición 4.3} \end{aligned}$$

(e) Demostraremos que si $b \neq 0$ y $d \neq 0$ entonces $\frac{a}{b} = \frac{c}{d} \Leftrightarrow a \cdot d = b \cdot c$.
Como $b \neq 0$ y $d \neq 0$ entonces existen b^{-1} y d^{-1}. Luego:

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow a \cdot b^{-1} = c \cdot d^{-1} \text{ por Definición 4.3}$$

$\Leftrightarrow \quad \left(a \cdot b^{-1}\right) \cdot b = \left(c \cdot d^{-1}\right) \cdot b$ por Teorema 4.4-(b)
$\Leftrightarrow \quad a \cdot b^{-1} \cdot b = c \cdot d^{-1} \cdot b$ por Axioma (P1) (asociativa del producto)
$\Leftrightarrow \quad a \cdot 1 = c \cdot d^{-1} \cdot b$ por Axiomas (P2) y (P4) (conm. y elem. inverso del producto)
$\Leftrightarrow \quad a = c \cdot d^{-1} \cdot b$ por Axioma (P3) (elemento neutro del producto)
$\Leftrightarrow \quad a \cdot d = c \cdot d^{-1} \cdot b \cdot d$ por Teorema 4.4-(b)
$\Leftrightarrow \quad a \cdot d = c \cdot d \cdot d^{-1} \cdot b$ por Axioma (P2) (conmutativa del producto)
$\Leftrightarrow \quad a \cdot d = c \cdot 1 \cdot b$ por Axiomas (P1) y (P4) (asociativa y elemento inverso del producto)
$\Leftrightarrow \quad a \cdot d = c \cdot b$ por Axioma (P3) (elemento neutro del producto)
$\Leftrightarrow \quad a \cdot d = b \cdot c$ por Axioma (P2) (conmutativa del producto)

(f) Probaremos que si $b \neq 0$ y $d \neq 0$ entonces $\dfrac{a}{b} \cdot \dfrac{c}{d} = \dfrac{a \cdot c}{b \cdot d}$.

Como $b \neq 0$ y $d \neq 0$ entonces existen b^{-1} y d^{-1}. Ahora:

$$\begin{aligned} \frac{a}{b} \cdot \frac{c}{d} &= a \cdot b^{-1} \cdot c \cdot d^{-1} \text{ por Definición 4.3 y Axioma (P1) (asociativa del producto)} \\ &= a \cdot c \cdot b^{-1} \cdot d^{-1} \text{ por Axioma (P2) (conmutativa del producto)} \\ &= a \cdot c \cdot (b \cdot d)^{-1} \text{ por Teorema 4.5-(x)} \\ &= \frac{a \cdot c}{b \cdot d} \text{ por Axioma (P1) (asociativa del producto) y Definición 4.3} \end{aligned}$$

(g) Vamos a demostrar que si $b \neq 0$ y $d \neq 0$ entonces $\left(\dfrac{b}{d}\right)^{-1} = \dfrac{d}{b}$.

Como $b \neq 0$ y $d \neq 0$ entonces existen b^{-1} y d^{-1}. Además $d^{-1} \neq 0$ por Teorema 4.5-(u). Luego $b \cdot d^{-1} \neq 0$ por Teorema 4.5-(i), por lo que $b/d \neq 0$ y por lo tanto existe $(b/d)^{-1}$. Ahora:

$$\begin{aligned} \frac{b}{d} \cdot \frac{d}{b} &= b \cdot d^{-1} \cdot d \cdot b^{-1} \text{ por Definición 4.3 y Axioma (P1) (asociativa del producto)} \\ &= b \cdot 1 \cdot b^{-1} \text{ por Axioma (P1) y (P4) (asociativa y elemento inverso del producto)} \\ &= b \cdot b^{-1} \text{ por Axioma (P3) (elemento neutro del producto)} \\ &= 1 \text{ por Axioma (P4) (elemento inverso del producto)} \end{aligned}$$

Luego, por el Corolario 4.1-(b) se tiene que

$$\left(\frac{b}{d}\right)^{-1} = \frac{d}{b}.$$

(h) Vamos a probar que si $b \neq 0$, $c \neq 0$ y $d \neq 0$ entonces $\dfrac{\dfrac{a}{b}}{\dfrac{c}{d}} = \dfrac{a \cdot d}{b \cdot c}$.

Como $b \neq 0$ entonces existe b^{-1}.

Como $d \neq 0$ entonces existe d^{-1} y además $d^{-1} \neq 0$ debido al Teorema 4.5-(u).

Como $c \neq 0$ y $d^{-1} \neq 0$ entonces $c \cdot d^{-1} \neq 0$, debido al Teorema 4.5-(i). Luego $c/d \neq 0$, por lo cual existe su inverso. Ahora:

$$\frac{\dfrac{a}{b}}{\dfrac{c}{d}} = \frac{a}{b} \cdot \left(\frac{c}{d}\right)^{-1} \text{ por Definición 4.3}$$

$$= \frac{a}{b} \cdot \frac{d}{c} \text{ por (g)}$$
$$= \frac{a \cdot d}{b \cdot c} \text{ por (f)}$$

(i) Demostraremos que si $b \neq 0$ y $d \neq 0$ entonces $\frac{a}{b} \pm \frac{c}{d} = \frac{a \cdot d \pm b \cdot c}{b \cdot d}$.

Como $b \neq 0$ y $d \neq 0$ entonces existen b^{-1} y d^{-1}. Ahora:

$$\begin{aligned}
\frac{a}{b} + \frac{c}{d} &= a \cdot b^{-1} + c \cdot d^{-1} \text{ por Definición 4.3} \\
&= a \cdot b^{-1} \cdot 1 + c \cdot d^{-1} \cdot 1 \text{ por Axioma (P1) y (P3) (asoc. y elem. neutro del producto)} \\
&= a \cdot b^{-1} \cdot d \cdot d^{-1} + c \cdot d^{-1} \cdot b \cdot b^{-1} \text{ por Axioma (P4) (elemento inverso del producto)} \\
&= a \cdot d \cdot b^{-1} \cdot d^{-1} + b \cdot c \cdot b^{-1} \cdot d^{-1} \text{ por Axioma (P2) (conmutativa del producto)} \\
&= (a \cdot d) \cdot \left(b^{-1} \cdot d^{-1}\right) + (b \cdot c) \cdot \left(b^{-1} \cdot d^{-1}\right) \text{ por Axioma (P1) (asociativa del producto)} \\
&= (a \cdot d) \cdot (b \cdot d)^{-1} + (b \cdot c) \cdot (b \cdot d)^{-1} \text{ por Teorema 4.5-(x)} \\
&= (a \cdot d + b \cdot c) \cdot (b \cdot d)^{-1} \text{ por Axioma (P2) (conmutativa) y (D) (distributiva)} \\
&= \frac{a \cdot d + b \cdot c}{b \cdot d} \text{ por Definición 4.3}
\end{aligned}$$

$$\begin{aligned}
\frac{a}{b} - \frac{c}{d} &= a \cdot b^{-1} - c \cdot d^{-1} \text{ por Definición 4.3} \\
&= a \cdot b^{-1} \cdot 1 - c \cdot d^{-1} \cdot 1 \text{ por Axioma (P1) y (P3) (asoc. y elem. neutro del producto)} \\
&= a \cdot b^{-1} \cdot d \cdot d^{-1} - c \cdot d^{-1} \cdot b \cdot b^{-1} \text{ por Axioma (P4) (elemento inverso del producto)} \\
&= a \cdot d \cdot b^{-1} \cdot d^{-1} - b \cdot c \cdot b^{-1} \cdot d^{-1} \text{ por Axioma (P2) (conmutativa del producto)} \\
&= (a \cdot d) \cdot \left(b^{-1} \cdot d^{-1}\right) - (b \cdot c) \cdot \left(b^{-1} \cdot d^{-1}\right) \text{ por Axioma (P1) (asociativa del producto)} \\
&= (a \cdot d) \cdot (b \cdot d)^{-1} - (b \cdot c) \cdot (b \cdot d)^{-1} \text{ por Teorema 4.5-(x)} \\
&= (a \cdot d - b \cdot c) \cdot (b \cdot d)^{-1} \text{ por Axioma (P2) (conmutativa del producto) y Teorema 4.5-(o)} \\
&= \frac{a \cdot d - b \cdot c}{b \cdot d} \text{ por Definición 4.3}
\end{aligned}$$

■

4.5. Propiedades del orden $<$

Teorema 4.7 (Propiedades de $<$)
Sean a, b, c y d números reales.

(a) $a + c < b + c \Rightarrow a < b$.

(b) $a > 0 \Leftrightarrow -a < 0$.

(c) $a < 0 \Leftrightarrow -a > 0$.

(d) $1 > 0$.

(e) $a > 0 \Leftrightarrow a^{-1} > 0$.

(f) *Si* $a < b$ *y* $c < d$ *entonces* $a + c < b + d$.

(g) $a < b \Leftrightarrow -b < -a$.

(h) $a + a = 0 \Leftrightarrow a = 0$.

(i) $a = 0 \Leftrightarrow a^2 = 0$.

(j) $a \neq 0 \Leftrightarrow a^2 > 0$.

(k) *Si* $a > 0$ *y* $b > 0$ *entonces* $a \cdot b > 0$.

(l) *Si* $a > 0$ *y* $b < 0$ *entonces* $a \cdot b < 0$.

(m) *Si* $a < 0$ *y* $b > 0$ *entonces* $a \cdot b < 0$.

(n) *Si* $a < 0$ *y* $b < 0$ *entonces* $a \cdot b > 0$.

(ñ) *Si* $a < b$ *y* $c < 0$ *entonces* $a \cdot c > b \cdot c$.

(o) *Supongamos que* $c > 0$. *Luego:*

$$a \cdot c < b \cdot c \Rightarrow a < b.$$

(p) *Supongamos que* $a > 0$ *y* $b > 0$. *Luego:*

$$a < b \Leftrightarrow b^{-1} < a^{-1}.$$

(q) *Supongamos que* $a > 0$ *y* $b > 0$. *Luego:*

$$a < b \Leftrightarrow a^2 < b^2.$$

(r) $a^2 + b^2 = 0 \Leftrightarrow a = b = 0$.

(s) *No existe* $x \in \mathbb{R}$ *tal que* $x^2 + 1 = 0$.

(t) *No existe ningún* $z \in \mathbb{R}$ *tal que* $x \leqslant z$ *cualquiera sea* $x \in \mathbb{R}$.

Demostración.
(a) Demostraremos que $a + c < b + c \Rightarrow a < b$.

$$\begin{aligned} a + c < b + c &\Rightarrow a + c + (-c) < b + c + (-c) \text{ por Axioma (S1) y Axioma (SC)} \\ &\Rightarrow a + 0 < b + 0 \text{ por Axioma (S1) y (S4) (asoc. y elem. opuesto de la suma)} \\ &\Rightarrow a < b \text{ por Axioma (S3) (elemento neutro de la suma)} \end{aligned}$$

Esta es una propiedad cancelativa para la suma en desigualdades.

(b) Probaremos que $a > 0 \Leftrightarrow -a < 0$.

$$\begin{aligned} 0 < a &\Leftrightarrow 0 + (-a) < a + (-a) \text{ por (SC) y (a)} \\ &\Leftrightarrow -a < a + (-a) \text{ por Axioma (S2) y (S3) (conmutativa y elemento neutro de la suma)} \\ &\Leftrightarrow -a < 0 \text{ por Axioma (S4) (elemento opuesto de la suma)} \end{aligned}$$

(c) Vamos a demostrar que $a < 0 \Leftrightarrow -a > 0$.

$$\begin{aligned} a < 0 &\Leftrightarrow -(-a) < 0 \text{ por Teorema 4.5-(c)} \\ &\Leftrightarrow -a > 0 \text{ por (b)} \end{aligned}$$

(d) Vamos a probar que $1 > 0$.

Por (O1) sabemos que $1 < 0 \veebar 1 = 0 \veebar 1 > 0$. Por (P3) sabemos que $1 \neq 0$, por lo que nos quedan sólo dos opciones: $1 < 0$ o $1 > 0$. Si suponemos que $1 < 0$, el Teorema 4.7-(c) nos dice que $-1 > 0$. Como $1 < 0$ y $-1 > 0$ se tiene que $1 \cdot (-1) < 0 \cdot (-1)$ por (PC). Luego:

$$\begin{aligned} 1 \cdot (-1) < 0 \cdot (-1) &\Rightarrow -1 \cdot 1 < 0 \cdot (-1) \text{ por Teorema 4.5-(m)} \\ &\Rightarrow -1 < 0 \cdot (-1) \text{ por Axioma (P3) (elemento neutro del producto)} \\ &\Rightarrow -1 < 0 \text{ por Axioma (P2) (conmutativa) y Teorema 4.5-(e)} \\ &\Rightarrow 1 > 0 \text{ por (b)} \end{aligned}$$

lo cual es una contradicción, pues habíamos asumido que $1 < 0$. Por lo tanto debe ocurrir que $1 > 0$.

(e) Demostraremos que $a > 0 \Leftrightarrow a^{-1} > 0$. Vamos a probar las dos implicaciones por separado.

Probemos primero que $a > 0 \Rightarrow a^{-1} > 0$.

Por Axioma (O1) se tiene que $a^{-1} < 0 \veebar a^{-1} = 0 \veebar a^{-1} > 0$. Debido al Teorema 4.5-(u) se ve que $a \neq 0$. Si suponemos ahora que $a^{-1} < 0$, como $a > 0$ tenemos que $a^{-1} \cdot a < 0 \cdot a$ por (PC). Luego:

$$\begin{aligned} a^{-1} \cdot a < 0 \cdot a &\Rightarrow 1 < 0 \cdot a \text{ por Axiomas (P2) y (P4) (conm. y elem. inverso del producto)} \\ &\Rightarrow 1 < 0 \text{ por Axiomas (P2) (conmutativa) y Teorema 4.5-(e)} \end{aligned}$$

lo cual es una contradicción por (d). Por lo tanto debe ocurrir que $a^{-1} > 0$.

Probemos ahora que $a^{-1} > 0 \Rightarrow a > 0$.

$$\begin{aligned} a^{-1} > 0 &\Rightarrow \left(a^{-1}\right)^{-1} > 0 \text{ por lo probado anteriormente} \\ &\Rightarrow a > 0 \text{ por Teorema 4.5-(w)} \end{aligned}$$

(f) Probaremos que si $a < b$ y $c < d$ entonces $a + c < b + d$.

Por (SC) se tiene que:

$$\begin{aligned} a < b &\Rightarrow a + c < b + c, \\ c < d &\Rightarrow c + b < d + b. \end{aligned}$$

Usando el Axioma (S2) (conmutativa de la suma) y el Axioma (O2) (transitiva) se tiene que $a + c < b + d$.

(g) Vamos a demostrar que $a < b \Leftrightarrow -b < -a$.

$$\begin{aligned} a < b &\Leftrightarrow a + (-a) < b + (-a) \text{ por Axioma (SC) y (a)} \\ &\Leftrightarrow 0 < b + (-a) \text{ por Axioma (S4) (elemento inverso de la suma)} \\ &\Leftrightarrow 0 + (-b) < b + (-a) + (-b) \text{ por Axioma (S1), Axioma (SC) y (a)} \\ &\Leftrightarrow -b < b + (-a) + (-b) \text{ por Axiomas (S2) y (S3) (conm. y elem. neutro de la suma)} \\ &\Leftrightarrow -b < (-a) + b + (-b) \text{ por Axioma (S2) (conmutativa de la suma)} \\ &\Leftrightarrow -b < (-a) + 0 \text{ por Axioma (S4) (elemento opuesto de la suma)} \\ &\Leftrightarrow -b < -a \text{ por Axioma (S3) (elemento neutro de la suma)} \end{aligned}$$

(h) Vamos a probar que $a + a = 0 \Leftrightarrow a = 0$. Vamos a demostrar las dos implicaciones por separado.

Veamos primero que $a + a = 0 \Rightarrow a = 0$.

Suponiendo que $a \neq 0$ tenemos dos opciones: $a > 0$ o $a < 0$. En el caso que $a > 0$ tenemos que:

$$\begin{aligned} a > 0 &\Rightarrow a + a > a + 0 \text{ por Axioma (SC)} \\ &\Rightarrow a + a > a \text{ por Axioma (S3) (elemento neutro de la suma)} \\ &\Rightarrow a + a > 0 \text{ pues estamos asumiendo que } a > 0 \text{ y Axioma (O2) (transitiva)} \end{aligned}$$

lo cual es una contradicción. Análogamente, en el caso que $a < 0$ tenemos que:

$$\begin{aligned} a < 0 &\Rightarrow a + a < a + 0 \text{ por Axioma (SC)} \\ &\Rightarrow a + a < a \text{ por Axioma (S3) (elemento neutro de la suma)} \\ &\Rightarrow a + a < 0 \text{ pues estamos asumiendo que } a < 0 \text{ y Axioma (O2)} \end{aligned}$$

lo cual es una contradicción. La única posibilidad que queda es que $a = 0$.
Ahora vamos a probar que $a = 0 \Rightarrow a + a = 0$.

$$\begin{aligned} a + a &= 0 + 0 \text{ por hipótesis} \\ &= 0 \text{ por Teorema 4.1} \end{aligned}$$

(i) Demostraremos que $a = 0 \Leftrightarrow a^2 = 0$.
Esto es una consecuencia directa del Teorema 4.5-(i) para el caso $a = b$.

(j) Probaremos que $a \neq 0 \Leftrightarrow a^2 > 0$. Vamos a probar las dos implicaciones por separado.
Si asumimos que $a^2 > 0$, en particular vale que $a^2 \neq 0$. Pero por (i) se tiene que $a \neq 0$.
Probemos ahora que $a \neq 0 \Rightarrow a^2 > 0$. Si suponemos primero que $a > 0$ tenemos que:

$$\begin{aligned} 0 < a &\Rightarrow 0 \cdot a < a \cdot a \text{ por Axioma (PC)} \\ &\Rightarrow a \cdot 0 < a \cdot a \text{ por Axioma (P2) (conmutativa del producto)} \\ &\Rightarrow 0 < a \cdot a \text{ por Teorema 4.5-(e)} \\ &\Rightarrow 0 < a^2 \text{ por Definición 4.2} \end{aligned}$$

Si suponemos ahora que $a < 0$ tenemos que:

$$\begin{aligned} a < 0 &\Rightarrow -a > 0 \text{ por Teorema 4.7-(c)} \\ &\Rightarrow (-a)^2 > 0 \text{ por lo demostrado anteriormente} \\ &\Rightarrow a^2 > 0 \text{ por Teorema 4.5-(n)} \end{aligned}$$

(k) Vamos a demostrar que si $a > 0$ y $b > 0$ entonces $a \cdot b > 0$.
Si ocurriese que $a \cdot b = 0$ entonces $a = 0$ o $b = 0$ por Teorema 4.5-(i) lo cual es una contradicción.
Para el caso que $a \cdot b < 0$ se tiene que:

$$\begin{aligned} a \cdot b < 0 &\Rightarrow a^{-1} \cdot a \cdot b < a^{-1} \cdot 0 \text{ por Axioma (P1) (asociativa) y Axioma (PC)} \\ &\Rightarrow 1 \cdot b < a^{-1} \cdot 0 \text{ por Axiomas (P2) y (P4) (conm. y elem. inverso del producto)} \\ &\Rightarrow b < a^{-1} \cdot 0 \text{ por Axiomas (P2) y (P3) (conmutativa y elemento neutro del producto)} \\ &\Rightarrow b < 0 \text{ por Teorema 4.5-(e)} \end{aligned}$$

lo cual es una contradicción. Por lo tanto $a \cdot b > 0$.

(l) Vamos a probar que si $a > 0$ y $b < 0$ entonces $a \cdot b < 0$.

Como $b < 0$ entonces $-b > 0$ por Teorema 4.7-(c). Por (k) se tiene que $a \cdot (-b) > 0$. Luego:

$$\begin{aligned} a \cdot (-b) > 0 &\Rightarrow -a \cdot b > 0 \text{ por Teorema 4.5-(m)} \\ &\Rightarrow a \cdot b < 0 \text{ por Teorema 4.7-(c)} \end{aligned}$$

(m) Demostraremos que si $a < 0$ y $b > 0$ entonces $a \cdot b < 0$.

$$\begin{aligned} a \cdot b &= b \cdot a \text{ por Axioma (P2) (conmutativa del producto)} \\ &< 0 \text{ por (l), pues } b > 0 \text{ y } a < 0 \end{aligned}$$

(n) Probaremos que si $a < 0$ y $b < 0$ entonces $a \cdot b > 0$.

$$\begin{aligned} a \cdot b &= (-a) \cdot (-b) \text{ por Teorema 4.5-(n)} \\ &> 0 \text{ por (k), pues } -a > 0 \text{ y } -b > 0 \text{ por Teorema 4.7-(c)} \end{aligned}$$

(ñ) Vamos a demostrar que si $a < b$ y $c < 0$ entonces $a \cdot c > b \cdot c$.

Por Teorema 4.7-(c) sabemos que $c < 0$ implica que $-c > 0$. Luego, por (PC) tenemos que $a \cdot (-c) < b \cdot (-c)$. Ahora

$$\begin{aligned} a \cdot (-c) < b \cdot (-c) &\Rightarrow -a \cdot c < -b \cdot c \text{ por Teorema 4.5-(m)} \\ &\Rightarrow b \cdot c < a \cdot c \text{ por Teorema 4.7-(g)} \end{aligned}$$

(o) Vamos a probar que si $c > 0$, se tiene que $a \cdot c < b \cdot c \Rightarrow a < b$.

Por (e), el hecho que $c > 0$ implica que $c^{-1} > 0$. Luego:

$$\begin{aligned} a \cdot c < b \cdot c &\Rightarrow a \cdot c \cdot c^{-1} < b \cdot c \cdot c^{-1} \text{ por Axioma (P1) y Axioma (PC)} \\ &\Rightarrow a \cdot 1 < b \cdot 1 \text{ por Axioma (P1) y (P4) (asoc. y elem. inverso del producto)} \\ &\Rightarrow a < b \text{ por Axioma (P3) (elemento neutro del producto)} \end{aligned}$$

Esta es una propiedad cancelativa para el producto en desigualdades.

(p) Demostraremos que si $a > 0$ y $b > 0$, se tiene que $a < b \Leftrightarrow b^{-1} < a^{-1}$.

Como $a > 0$ y $b > 0$ entonces $a^{-1} > 0$ y $b^{-1} > 0$ por Teorema 4.7-(e). Ahora:

$$\begin{aligned} a < b &\Leftrightarrow a \cdot a^{-1} < b \cdot a^{-1} \text{ por Axioma (PC) y (o)} \\ &\Leftrightarrow 1 < b \cdot a^{-1} \text{ por Axioma (P4) (elemento inverso del producto)} \\ &\Leftrightarrow 1 \cdot b^{-1} < b \cdot a^{-1} \cdot b^{-1} \text{ por Axioma (P1), Axioma (PC) y (o)} \\ &\Leftrightarrow b^{-1} \cdot 1 < a^{-1} \cdot b \cdot b^{-1} \text{ por Axioma (P2) (conmutativa del producto)} \\ &\Leftrightarrow b^{-1} \cdot 1 < a^{-1} \cdot 1 \text{ por Axioma (P4) (elemento inverso del producto)} \\ &\Leftrightarrow b^{-1} < a^{-1} \text{ por Axioma (P3) (elemento neutro del producto)} \end{aligned}$$

(q) Demostraremos que si $a > 0$ y $b > 0$, se tiene que $a < b \Leftrightarrow a^2 < b^2$. Vamos a probar las dos implicaciones por separado.

Demostremos primero que $a < b \Rightarrow a^2 < b^2$.

$$a < b \wedge a > 0 \Rightarrow a \cdot a < b \cdot a \text{ por Axioma (PC)}$$

$$a < b \wedge b > 0 \quad \Rightarrow \quad a \cdot b < b \cdot b \text{ por Axioma (PC)}$$

Por Axioma (P2) (conmutativa del producto) y (O2) se tiene que $a^2 < b^2$.

Demostremos ahora que $a^2 < b^2 \Rightarrow a < b$.

Si $a > b$ entonces $a^2 > b^2$ por lo demostrado anteriormente, lo cual es una contradicción. Por otro lado, si $a = b$ entonces $a^2 = b^2$, lo cual también es una contradicción. La única posibilidad que queda es que $a < b$.

(r) Probaremos que $a^2 + b^2 = 0 \Leftrightarrow a = b = 0$. Vamos a demostrar las dos implicaciones por separado.

Probemos primero que $a^2 + b^2 = 0 \Rightarrow a = b = 0$.

Si ocurriese que $a \neq 0$ entonces $a^2 > 0$ por (j). Luego

$$\begin{aligned} 0 < a^2 \quad &\Rightarrow \quad 0 + b^2 < a^2 + b^2 \text{ por Axioma (SC)} \\ &\Rightarrow \quad b^2 < a^2 + b^2 \text{ por Axiomas (S2) y (S3) (conmutativa y elemento neutro de la suma)} \\ &\Rightarrow \quad b^2 < 0 \text{ por hipótesis} \end{aligned}$$

lo cual es una contradicción pues $b^2 \geqslant 0$ por (i) y (j). Por lo tanto, $a = 0$. Luego de la hipótesis se deduce:

$$\begin{aligned} a^2 + b^2 = 0 \quad &\Rightarrow \quad 0 + b^2 = 0 \text{ por (i)} \\ &\Rightarrow \quad b^2 = 0 \text{ por Axiomas (S2) y (S3) (conmutativa y elemento neutro del producto)} \\ &\Rightarrow \quad b = 0 \text{ por (i)} \end{aligned}$$

Probemos ahora que $a = b = 0 \Rightarrow a^2 + b^2 = 0$.

$$\begin{aligned} a^2 + b^2 \quad &= \quad 0 + 0 \text{ por hipótesis y por (i)} \\ &= \quad 0 \text{ por Teorema 4.1} \end{aligned}$$

(s) Vamos a demostrar que no existe $x \in \mathbb{R}$ tal que $x^2 + 1 = 0$.

Supongamos que existe $x \in \mathbb{R}$ tal que $x^2 + 1 = 0$. Ahora:

$$\begin{aligned} 0 \quad &= \quad x^2 + 1 \\ &= \quad x^2 + 1^2 \text{ por Teorema 4.1} \end{aligned}$$

Por (r) se deduce que $x = 0$ y que $1 = 0$, lo cual es una contradicción debido a (P3). Por lo tanto tal x no puede existir.

(t) Vamos a probar que no existe ningún $z \in \mathbb{R}$ tal que $x \leqslant z$ cualquiera sea $x \in \mathbb{R}$.

Supongamos que existe $z \in \mathbb{R}$ tal que $x \leqslant z$ para todo $x \in \mathbb{R}$. Ahora por Teorema 4.7-(d) se tiene que $0 < 1$. Ahora

$$\begin{aligned} 0 < 1 \quad &\Rightarrow \quad 0 + z < 1 + z \text{ por Axioma (SC)} \\ &\Rightarrow \quad z < 1 + z \text{ por Axiomas (S2) y (S3) (conmutativa y elemento neutro de la suma)} \end{aligned}$$

lo cual es una contradicción pues $1 + z$ es un número real. ■

4.6. Valor absoluto

Definición 4.4 (Reales positivos y reales no negativos)
Se definen:

$$\begin{aligned} \mathbb{R}_{>0} \quad &= \quad \{x \in \mathbb{R} : x > 0\}, \quad \textit{reales positivos,} \\ \mathbb{R}_{\geqslant 0} \quad &= \quad \{x \in \mathbb{R} : x \geqslant 0\}, \quad \textit{reales no negativos.} \end{aligned}$$

Definición 4.5 (Valor absoluto)
La función $|\cdot| : \mathbb{R} \to \mathbb{R}_{\geqslant 0}$ *definida por:*

$$|x| = \begin{cases} x, & si\ x \geqslant 0, \\ -x, & si\ x < 0. \end{cases}$$

será llamada valor absoluto.

Ejemplo 4.1

(a) $|1| = 1$, pues $1 > 0$.

(b) $|-1| = -(-1) = 1$, pues $-1 < 0$.

(c) $|0| = 0$, por definición de valor absoluto.

Teorema 4.8 (Propiedades del valor absoluto)
Sean a *y* b *números reales.*

(a) $|a| = 0 \Leftrightarrow a = 0$.

(b) $|a| = |-a|$.

(c) $|a - b| = |b - a|$.

(d) $|a^2| = a^2$.

(e) $|a \cdot b| = |a| \cdot |b|$.

(f) Si $a \neq 0$ *entonces* $|a|^{-1} = |a^{-1}|$.

(g) Si $b \neq 0$ *entonces*

$$\left|\frac{a}{b}\right| = \frac{|a|}{|b|}.$$

(h) $-|a| \leqslant a \leqslant |a|$.

(i) $-|a| \leqslant b \leqslant |a| \Leftrightarrow |b| \leqslant |a|$.

(j) Si $b \geqslant 0$, *entonces* $|a| \geqslant b \Leftrightarrow a \geqslant b$ *o* $a \leqslant -b$.

(k) $|a + b| \leqslant |a| + |b|$ *(desigualdad triangular).*

(l) $\Big|\, |a| - |b| \,\Big| \leqslant |a - b|$.

Demostración.
(a) Demostraremos que $|a| = 0 \Leftrightarrow a = 0$. Vamos a probar las dos implicaciones por separado.
Probemos primero que $|a| = 0 \Rightarrow a = 0$.
Si $a > 0$ entonces $|a| = a > 0$ lo cual es una contradicción. Si $a < 0$ entonces $|a| = -a > 0$ por Teorema 4.7-(c), lo cual también es una contradicción. Luego la única opción que queda es que $a = 0$.
Probemos ahora que $a = 0 \Rightarrow |a| = 0$. Por Definición 4.5 se puede ver que $|0| = 0$.

(b) Probaremos que $|a| = |-a|$.
Asumamos primero que $a > 0$, lo cual implica que $-a < 0$ por Teorema 4.7-(b). Ahora

$$\begin{aligned} |-a| &= -(-a) \text{ por Definición 4.5} \\ &= a \text{ por Teorema 4.5-(c)} \end{aligned}$$

$$= |a| \text{ por Definición 4.5}$$

Asumamos ahora que $a = 0$. Sabemos que $0 = -0$ por Teorema 4.5-(d). Luego es inmediato que $|-0| = |0|$.

Finalmente asumamos que $a < 0$, lo cual implica que $-a > 0$ por Teorema 4.7-(c). Ahora

$$\begin{aligned} |-a| &= -a \text{ por Definición 4.5} \\ &= |a| \text{ por Definición 4.5} \end{aligned}$$

En todos los casos se tiene que $|a| = |-a|$.

(c) Vamos a demostrar que $|a - b| = |b - a|$.

$$\begin{aligned} |a - b| &= |-(a - b)| \text{ por (b)} \\ &= |b - a| \text{ por Teorema 4.5-(k)} \end{aligned}$$

(d) Vamos a probar que $|a^2| = a^2$.

Por Teorema 4.7-(i) y 4.7-(j) se tiene que $a^2 \geqslant 0$, con lo cual se tiene que por Definición 4.5: $|a^2| = a^2$.

(e) Demostraremos que $|a \cdot b| = |a| \cdot |b|$.

Asumamos que $a = 0$.

$$\begin{aligned} |a \cdot b| &= |0 \cdot b| \\ &= |0| \text{ por Axioma (P2) (conmutativa) y Teorema 4.5-(e)} \\ &= 0 \text{ por (a)} \\ &= 0 \cdot |b| \text{ por Axioma (P2) (conmutativa) y Teorema 4.5-(e)} \\ &= |0| \cdot |b| \text{ por (a)} \\ &= |a| \cdot |b| \end{aligned}$$

Asumamos que $b = 0$.

$$\begin{aligned} |a \cdot b| &= |a \cdot 0| \\ &= |0 \cdot a| \text{ por Axioma (P2) (conmutativa del producto)} \\ &= |0| \cdot |a| \text{ por caso anterior} \\ &= |b| \cdot |a| \\ &= |a| \cdot |b| \text{ por Axioma (P2) (conmutativa del producto)} \end{aligned}$$

Asumamos que $a > 0$ y $b > 0$.

$$\begin{aligned} |a \cdot b| &= a \cdot b \text{ por Teorema 4.7-(k)} \\ &= |a| \cdot |b| \text{ por Definición 4.5} \end{aligned}$$

Asumamos que $a > 0$ y $b < 0$.

$$\begin{aligned} |a \cdot b| &= -a \cdot b \text{ por Teorema 4.7-(l)} \\ &= a \cdot (-b) \text{ por Teorema 4.5-(m)} \\ &= |a| \cdot |b| \text{ por Definición 4.5} \end{aligned}$$

Asumamos que $a < 0$ y $b > 0$.

$$\begin{aligned} |a \cdot b| &= |b \cdot a| \text{ por Axioma (P2) (conmutativa del producto)} \\ &= |b| \cdot |a| \text{ por el caso anterior pues } b > 0 \text{ y } a < 0 \\ &= |a| \cdot |b| \text{ por Axioma (P2) (conmutativa del producto)} \end{aligned}$$

Asumamos que $a < 0$ y $b < 0$.

$$\begin{aligned} |a \cdot b| &= a \cdot b \text{ por Teorema 4.7-(n)} \\ &= (-a) \cdot (-b) \text{ por Teorema 4.5-(n)} \\ &= |a| \cdot |b| \text{ por 4.5} \end{aligned}$$

(f) Probaremos que si $a \neq 0$ entonces $|a|^{-1} = |a^{-1}|$.
Como $a \neq 0$ entonces existe a^{-1} por el Axioma (P4) (elemento inverso del producto). Ahora:

$$\begin{aligned} |a| \cdot \left|a^{-1}\right| &= \left|a \cdot a^{-1}\right| \text{ por (e)} \\ &= |1| \text{ por Axioma (P4) (elemento inverso del producto)} \\ &= 1 \text{ por Teorema 4.7-(d) y Definición 4.5} \end{aligned}$$

Luego por Corolario 4.1-(b) se tiene que $|a|^{-1} = |a^{-1}|$.

(g) Vamos a demostrar que si $b \neq 0$ entonces $\left|\frac{a}{b}\right| = \frac{|a|}{|b|}$.
Como $b \neq 0$ entonces existe b^{-1} por el Axioma (P4). Ahora:

$$\begin{aligned} \left|\frac{a}{b}\right| &= \left|a \cdot b^{-1}\right| \text{ por Definicion 4.3} \\ &= |a| \cdot \left|b^{-1}\right| \text{ por (e)} \\ &= |a| \cdot |b|^{-1} \text{ por (f)} \\ &= \frac{|a|}{|b|} \text{ por Definicion 4.3} \end{aligned}$$

(h) Vamos a probar que $-|a| \leqslant a \leqslant |a|$.
Asumamos primero que $a = 0$.

$$\begin{aligned} -|0| &= -0 \text{ por (a)} \\ &= 0 \text{ por Teorema 4.5-(d)} \\ &= |0| \text{ por (a)} \end{aligned}$$

Luego, $-|0| = 0 = |0|$.
Asumamos ahora que $a > 0$.

$$\begin{aligned} -|a| &= -a \text{ por Definición 4.5} \\ &< 0 \text{ por Teorema 4.7-(b)} \\ &< a \text{ por hipótesis} \\ &= |a| \text{ por Definición 4.5} \end{aligned}$$

Luego, $-|a| < a = |a|$.

Asumamos ahora que $a < 0$.

$$\begin{aligned} -|a| &= -(-a) \text{ por Definición 4.5} \\ &= a \text{ por Teorema 4.5-(c)} \\ &< 0 \text{ por hipótesis} \\ &< -a \text{ por Teorema 4.7-(c)} \\ &= |a| \text{ por Definición 4.5} \end{aligned}$$

Luego, $-|a| = a < |a|$.

(i) Demostremos que $-|a| \leqslant b \leqslant |a| \Leftrightarrow |b| \leqslant |a|$. Vamos a probar las dos implicaciones por separado.
Demostremos primero que $-|a| \leqslant b \leqslant |a| \Rightarrow |b| \leqslant |a|$.
Supongamos que $b \geqslant 0$.

$$\begin{aligned} -|a| \leqslant b \leqslant |a| &\Rightarrow b \leqslant |a| \text{ pues es un caso particular de la hipótesis} \\ &\Rightarrow |b| \leqslant |a| \text{ por Definición 4.5} \end{aligned}$$

Supongamos que $b < 0$.

$$\begin{aligned} -|a| \leqslant b \leqslant |a| &\Rightarrow -|a| \leqslant b \text{ pues es un caso particular de la hipótesis} \\ &\Rightarrow -b \leqslant -(-|a|) \text{ por Teorema 4.7-(g)} \\ &\Rightarrow -b \leqslant |a| \text{ por Teorema 4.5-(c)} \\ &\Rightarrow |b| \leqslant |a| \text{ por Definición 4.5} \end{aligned}$$

Demostremos ahora que $|b| \leqslant |a| \Rightarrow -|a| \leqslant b \leqslant |a|$.
Supongamos que $b \geqslant 0$. Luego

$$\begin{aligned} -|a| &\leqslant 0 \text{ pues por Definición 4.5 tenemos que } |a| \geqslant 0 \text{ y Teorema 4.7-(g)} \\ &\leqslant b \text{ por hipótesis} \\ &= |b| \text{ por Definición 4.5} \\ &\leqslant |a| \text{ por hipótesis} \end{aligned}$$

Luego $-|a| \leqslant b \leqslant |a|$.
Supongamos que $b < 0$. Luego

$$\begin{aligned} -|a| &\leqslant b \text{ por hipótesis } -b \leqslant |a|\text{, Teorema 4.7-(g) y Teorema 4.5-(c)} \\ &< 0 \text{ por hipótesis} \\ &\leqslant |a| \text{ pues por Definición 4.5 tenemos que } |a| \geqslant 0 \end{aligned}$$

Luego $-|a| \leqslant b \leqslant |a|$.

(j) Vamos a demostrar que si $b \geqslant 0$, entonces $|a| \geqslant b \Leftrightarrow a \geqslant b$ o $a \leqslant -b$. Vamos a probar las dos implicaciones por separado.

Asumamos primero que $|a| \geqslant b$. Si consideramos el caso en que $a \geqslant 0$ se deduce que $|a| \geqslant b \Rightarrow a \geqslant b$ utilizando la Definición 4.5. Por otro lado, si consideramos el caso $a < 0$, se deduce que:

$$\begin{aligned} |a| \geqslant b &\Rightarrow -a \geqslant b \text{ por Definición 4.5 (valor absoluto)} \\ &\Rightarrow a \leqslant -b \text{ por Teoremas 4.7-(g) y 4.5-(c)} \end{aligned}$$

Ahora supongamos que ocurre que $a \geqslant b$ o $a \leqslant -b$. Si sucede el caso $a \geqslant b$, la hipótesis nos dice que $a \geqslant 0$ (pues $b \geqslant 0$). Luego, se deduce que: $a \geqslant b \Rightarrow |a| \geqslant b$ utilizando la Definición 4.5. Por otro lado, si sucede que $a \leqslant -b$ entonces $a \leqslant 0$ (pues $b \geqslant 0$). Luego se obtiene lo siguiente:

$$\begin{aligned} a \leqslant -b &\Rightarrow -a \geqslant b \text{ por Teoremas 4.7-(g) y 4.5-(c)} \\ &\Rightarrow |a| \geqslant b \text{ por Definición 4.5 (valor absoluto)} \end{aligned}$$

(k) Probemos que $|a+b| \leqslant |a| + |b|$.
Supongamos que $a + b \geqslant 0$, $a \geqslant 0$ y $b \geqslant 0$.

$$\begin{aligned} |a+b| &= a+b \text{ por Definición 4.5} \\ &= |a| + |b| \text{ por Definición 4.5} \end{aligned}$$

Supongamos que $a + b \geqslant 0$, $a \geqslant 0$ y $b < 0$.

$$\begin{aligned} |a+b| &= a+b \text{ por Definición 4.5} \\ &< a+0 \text{ por Axioma (SC) pues } b < 0 \\ &< a+(-b) \text{ por Axioma (SC) (pues } 0 < -b \text{ por Teorema 4.7-(c))} \\ &= |a| + |b| \text{ por Definición 4.5} \end{aligned}$$

Supongamos que $a + b \geqslant 0$, $a < 0$ y $b \geqslant 0$.

$$\begin{aligned} |a+b| &= |b+a| \text{ por Axioma (S2)} \\ &< |b| + |a| \text{ por caso anterior} \\ &= |a| + |b| \text{ por Axioma (S2)} \end{aligned}$$

Supongamos que $a + b \geqslant 0$, $a < 0$ y $b < 0$. Por Teorema 4.7-(f) y Teorema 4.1 se tiene que $a + b < 0 + 0 = 0$ lo cual contradice la hipótesis. Es decir, esta situación nunca ocurre.
Supongamos que $a + b < 0$, entonces $-(a+b) > 0$ por Teorema 4.7-(c). Ahora:

$$\begin{aligned} |a+b| &= |-(a+b)| \text{ por (b)} \\ &= |(-a)+(-b)| \text{ por Teorema 4.5-(j)} \\ &\leqslant |-a| + |-b| \text{ pues } (-a)+(-b) > 0 \text{ y los casos anteriores} \\ &\leqslant |a| + |b| \text{ por (b)} \end{aligned}$$

(l) Vamos a demostrar que $\Big|\, |a| - |b| \,\Big| \leqslant |a-b|$.
Notemos que:

$$\begin{aligned} |a| &= |a+0| \text{ por Axioma (S3) (elemento neutro de la suma)} \\ &= |a+b+(-b)| \text{ por Axiomas (S1) y (S4) (asoc. y elem. inverso de la suma)} \\ &= |a+(-b)+b| \text{ por Axioma (S2) (conmutativa de la suma)} \\ &\leqslant |a-b| + |b| \text{ por Axioma (S1) (asociativa de la suma) y (k)} \end{aligned}$$

Análogamente,

$$\begin{aligned} |b| &= |b+0| \text{ por Axioma (S3) (elemento neutro de la suma)} \\ &= |b+a+(-a)| \text{ por Axiomas (S1) y (S4) (asoc. y elem. inverso de la suma)} \\ &= |b+(-a)+a| \text{ por Axioma (S2) (conmutativa de la suma)} \end{aligned}$$

$$\begin{aligned} &\leqslant |b-a|+|a| \text{ por Axioma (S1) (asociativa de la suma) y (k)} \\ &= |a-b|+|a| \text{ por (c)} \end{aligned}$$

En el primer caso tenemos que:

$$\begin{aligned} |a| \leqslant |a-b|+|b| &\Rightarrow |a|+(-|b|) \leqslant |a-b|+|b|+(-|b|) \text{ por Axiomas (SC) y (S1)} \\ &\Rightarrow |a|-|b| \leqslant |a-b|+0 \text{ por Axiomas (S1) y (S4)} \\ &\Rightarrow |a|-|b| \leqslant |a-b| \text{ por Axiomas (S3)} \end{aligned}$$

En el segundo caso tenemos que:

$$\begin{aligned} |b| \leqslant |a-b|+|a| &\Rightarrow |b|+(-|a|) \leqslant |a-b|+|a|+(-|a|) \text{ por Axiomas (SC) y (S1)} \\ &\Rightarrow |b|-|a| \leqslant |a-b|+0 \text{ por Axiomas (S1) y (S4)} \\ &\Rightarrow |b|-|a| \leqslant |a-b| \text{ por Axiomas (S3)} \\ &\Rightarrow -(|a|-|b|) \leqslant |a-b| \text{ por Teorema 4.5-(k)} \\ &\Rightarrow -|a-b| \leqslant -[-(|a|-|b|)] \text{ por Teorema 4.7-(g)} \\ &\Rightarrow -|a-b| \leqslant |a|-|b| \text{ por Teorema 4.5-(c)} \end{aligned}$$

De las últimas dos desigualdades tenemos que $-|a-b| \leqslant |a|-|b| \leqslant |a-b|$. Por (i) se tiene que $\Big||a|-|b|\Big| \leqslant |a-b|$. ■

A partir de ahora usaremos las propiedades de los números reales libremente, tratando de ser claros en los pasos pero no justificando hasta el mínimo detalle.

4.7. Resolviendo desigualdades con valor absoluto

Vamos a resolver un ejercicio práctico de una desigualdad que involucra valores absolutos. Hay que hallar las soluciones en $\mathbb{R}$ de la desigualdad:

$$\frac{|x-1|}{|x+2|} < 1.$$

Lo primero que hay que hacer es eliminar aquellos x para los cuales la expresión no está definida. Debido a esto, el valor -2 no puede aparecer en el conjunto de soluciones pues hace que el denominador sea nulo. Por lo que de ahora en adelante deberemos considerar que $x \neq 2$.

Una forma extensa pero segura puede ser considerar dos casos posibles por cada valor absoluto. En nuestro caso tendríamos cuatro casos, a saber:

(a) $x-1 \geqslant 0$ y $x+2 > 0$ (el caso $x+2=0$ ya ha sido descartado).

(b) $x-1 \geqslant 0$ y $x+2 < 0$ (el caso $x+2=0$ ya ha sido descartado).

(c) $x-1 < 0$ y $x+2 > 0$.

(d) $x-1 < 0$ y $x+2 < 0$.

De cada uno de estos casos, obtendremos un posible conjunto de soluciones. Vamos a analizarlos uno por uno.

(a) Supongamos que $x-1 \geqslant 0$ y $x+2>0$. Esto significa que $x \geqslant 1$ y $x>-2$. El conjunto donde analizaremos la desigualdad está formado por la intersección de dos conjuntos: $\{x \in \mathbb{R} : x \geqslant 1\} \cap \{x \in \mathbb{R} : x > -2\} = \{x \in \mathbb{R} : x \geqslant 1\}$. Recién ahora veremos cómo queda expresada nuestra desigualdad para los x dentro de este último conjunto:

$$\begin{aligned}
\frac{|x-1|}{|x+2|} < 1 &\Leftrightarrow |x-1| < |x+2| \text{ pues } |x+2| > 0 \\
&\Leftrightarrow x-1 < x+2 \text{ pues estamos asumiendo que } x-1 \geqslant 0 \text{ y } x+2>0 \\
&\Leftrightarrow -1 < 2 \text{ utilizando el Axioma (SC) y el Teorema 4.7-(a)} \\
&\Leftrightarrow \boldsymbol{V}
\end{aligned}$$

lo cual significa que todos los elementos de $\{x \in \mathbb{R} : x \geqslant 1\}$ satisfacen la desigualdad.

(b) Supongamos que $x-1 \geqslant 0$ y $x+2<0$. Esto significa que $x \geqslant 1$ y $x<-2$. El conjunto donde analizaremos la desigualdad está formado por la intersección de dos conjuntos: $\{x \in \mathbb{R} : x \geqslant 1\} \cap \{x \in \mathbb{R} : x < -2\} = \varnothing$. Esto nos dice que esta situación nunca ocurre y por lo tanto no tiene sentido analizar la desigualdad para este caso. Dicho de otro modo, el conjunto de soluciones para este caso es $\varnothing$.

(c) Supongamos que $x-1<0$ y $x+2>0$. Esto significa que $x<1$ y $x>-2$. El conjunto donde analizaremos la desigualdad está formado por la intersección de dos conjuntos: $\{x \in \mathbb{R} : x < 1\} \cap \{x \in \mathbb{R} : x > -2\} = \{x \in \mathbb{R} : -2 < x < 1\}$. Recién ahora veremos cómo queda expresada nuestra desigualdad para los x dentro de este último conjunto:

$$\begin{aligned}
\frac{|x-1|}{|x+2|} < 1 &\Leftrightarrow |x-1| < |x+2| \text{ pues } |x+2| > 0 \\
&\Leftrightarrow -(x-1) < x+2 \text{ pues estamos asumiendo que } x-1<0 \text{ y } x+2>0 \\
&\Leftrightarrow -x+1 < x+2 \\
&\Leftrightarrow 1-2 < x+x \\
&\Leftrightarrow -1 < 2 \cdot x \\
&\Leftrightarrow -\frac{1}{2} < x
\end{aligned}$$

lo cual significa que aquellos elementos del conjunto $\{x \in \mathbb{R} : -2 < x < 1\}$ que satisfagan que $-\frac{1}{2} < x$ serán las soluciones para este caso. En otras palabras, el conjunto de soluciones para este caso se obtiene a través de la intersección de dos conjuntos: $\{x \in \mathbb{R} : -2 < x < 1\} \cap \left\{x \in \mathbb{R} : -\frac{1}{2} < x\right\}$ que es igual a $\left\{x \in \mathbb{R} : -\frac{1}{2} < x < 1\right\}$.

(d) Supongamos que $x-1<0$ y $x+2<0$. Esto significa que $x<1$ y $x<-2$. El conjunto donde analizaremos la desigualdad está formado por la intersección de dos conjuntos: $\{x \in \mathbb{R} : x < 1\} \cap \{x \in \mathbb{R} : x < -2\} = \{x \in \mathbb{R} : x < -2\}$. Recién ahora veremos cómo queda expresada nuestra desigualdad para los x dentro de este último conjunto:

$$\begin{aligned}
\frac{|x-1|}{|x+2|} < 1 &\Leftrightarrow |x-1| < |x+2| \text{ pues } |x+2| > 0 \\
&\Leftrightarrow -(x-1) < -(x+2) \text{ pues estamos asumiendo que } x-1<0 \text{ y } x+2<0 \\
&\Leftrightarrow -x+1 < -x-2 \\
&\Leftrightarrow 1 < -2
\end{aligned}$$

lo cual significa que ningún elemento del conjunto $\{x \in \mathbb{R} : x < -2\}$ puede ser solución de la desigualdad. En otras palabras, el conjunto de soluciones para este caso es igual a $\varnothing$.

Juntando toda la información, la solución del problema completo se obtiene realizando la unión de las soluciones parciales de cada caso. Es decir, la solución es:

$$\{x \in \mathbb{R} : x \geqslant 1\} \cup \varnothing \cup \left\{x \in \mathbb{R} : -\frac{1}{2} < x < 1\right\} \cup \varnothing = \left\{x \in \mathbb{R} : -\frac{1}{2} < x\right\}$$

Notemos que el valor -2 no está en el conjunto solución.

4.8. Ejemplos de utilización de las propiedades

En los siguientes ejercicios mostraremos la utilización de las propiedades de los números reales.

Ejemplo 4.2
Realizar los siguientes cálculos:

(a)

$$\begin{aligned}
3 - \left(-4 + \frac{5}{2}\right) &= 3 - \left(-\frac{8}{2} + \frac{5}{2}\right) \text{ escribiendo fracciones equivalentes} \\
&= 3 - \left(\frac{-8+5}{2}\right) \text{ por Teorema 4.6-(i)} \\
&= 3 - \left(\frac{-3}{2}\right) \\
&= 3 - \left(-\frac{3}{2}\right) \text{ por Teorema 4.6-(d)} \\
&= 3 + \frac{3}{2} \text{ por Teorema 4.5-(c)} \\
&= \frac{6}{2} + \frac{3}{2} \text{ escribiendo fracciones equivalentes} \\
&= \frac{6+3}{2} \text{ por Teorema 4.6-(i)} \\
&= \frac{9}{2} \text{ sumando las fracciones}
\end{aligned}$$

(b)

$$\begin{aligned}
\frac{-\frac{1}{5} + \frac{1}{3} \cdot \left(-\frac{2}{5}\right)}{-3} &= \frac{-\frac{1}{5} - \frac{1}{3} \cdot \frac{2}{5}}{-3} \text{ por Teorema 4.5-(m)} \\
&= \frac{-\frac{1}{5} - \frac{1 \cdot 2}{3 \cdot 5}}{-3} \text{ por Teorema 4.6-(f)}
\end{aligned}$$

$$= \frac{-\frac{1}{5}-\frac{2}{15}}{-3}$$

$$= \frac{-\frac{3}{15}-\frac{2}{15}}{-3} \text{ escribiendo fracciones equivalentes}$$

$$= \frac{-\left(\frac{3}{15}+\frac{2}{15}\right)}{-3} \text{ por Teorema 4.5-(j)}$$

$$= \frac{\frac{3}{15}+\frac{2}{15}}{3} \text{ por Teorema 4.6-(d)}$$

$$= \frac{\frac{3+2}{15}}{3} \text{ por Teorema 4.6-(i)}$$

$$= \frac{\frac{5}{15}}{3}$$

$$= \frac{\frac{1}{3}}{3} \text{ escribiendo fracciones equivalentes}$$

$$= \frac{\frac{1}{3}}{\frac{3}{1}} \text{ por Teorema 4.6-(c)}$$

$$= \frac{1 \cdot 1}{3 \cdot 3} \text{ por Teorema 4.6-(h)}$$

$$= \frac{1}{9}$$

(c)

$$\frac{-\frac{2}{3}+\frac{5}{2}}{-\frac{4}{3}\cdot\frac{1}{3}} = \frac{-\frac{4}{6}+\frac{15}{6}}{-\frac{4}{3}\cdot\frac{1}{3}} \text{ escribiendo fracciones equivalentes}$$

$$= \frac{\frac{-4+15}{6}}{-\frac{4}{3}\cdot\frac{1}{3}} \text{ por Teorema 4.6-(i)}$$

$$= \frac{\frac{11}{6}}{-\frac{4\cdot 1}{3\cdot 3}}$$

$$= \frac{\frac{11}{6}}{-\frac{4\cdot 1}{3\cdot 3}} \text{ por Teorema 4.6-(f)}$$

$$= \frac{\frac{11}{6}}{-\frac{4}{9}}$$

$$= -\frac{\frac{11}{6}}{\frac{4}{9}} \text{ por Teorema 4.6-(d)}$$

$$= -\frac{11\cdot 9}{6\cdot 4} \text{ por Teorema 4.6-(h)}$$

$$= -\frac{11\cdot 3}{2\cdot 4} \text{ escribiendo fracciones equivalentes}$$

$$= -\frac{33}{8}$$

(d)

$$-\frac{4}{5}\cdot\left(\frac{\frac{3}{4}\cdot\frac{2}{5}}{2-\frac{1}{2}}\right) = -\frac{4}{5}\cdot\left(\frac{\frac{3}{4}\cdot\frac{2}{5}}{\frac{4}{2}-\frac{1}{2}}\right) \text{ escribiendo fracciones equivalentes}$$

$$= -\frac{4}{5}\cdot\left(\frac{\frac{3}{4}\cdot\frac{2}{5}}{\frac{4-1}{2}}\right) \text{ por Teorema 4.6-(i)}$$

$$= -\frac{4}{5}\cdot\left(\frac{\frac{3}{4}\cdot\frac{2}{5}}{\frac{3}{2}}\right)$$

$$= -\frac{4}{5}\cdot\left(\frac{\frac{3\cdot 2}{4\cdot 5}}{\frac{3}{2}}\right) \text{ por Teorema 4.6-(f)}$$

$$= -\frac{4}{5}\cdot\left(\frac{\frac{3\cdot 1}{2\cdot 5}}{\frac{3}{2}}\right) \text{ escribiendo fracciones equivalentes}$$

$$= -\frac{4}{5}\cdot\left(\frac{\frac{3}{10}}{\frac{3}{2}}\right)$$

$$= -\frac{4}{5}\cdot\left(\frac{3\cdot 2}{10\cdot 3}\right) \text{ por Teorema 4.6-(h)}$$

$$= -\frac{4}{5}\cdot\left(\frac{1\cdot 1}{5\cdot 1}\right) \text{ escribiendo fracciones equivalentes}$$

$$= -\frac{4}{5}\cdot\frac{1}{5}$$

$$= -\frac{4\cdot 1}{5\cdot 5} \text{ por Teorema 4.6-(f)}$$

$$= -\frac{4}{25}$$

(e)

$$\frac{\frac{2}{7}+\frac{1}{13}\cdot\left(-\frac{1}{5}+\frac{3}{2}\right)}{(-2)\cdot\frac{1}{5}+\frac{3}{5}} = \frac{\frac{2}{7}+\frac{1}{13}\cdot\left(-\frac{2}{10}+\frac{15}{10}\right)}{(-2)\cdot\frac{1}{5}+\frac{3}{5}} \text{ escribiendo fracciones equivalentes}$$

$$= \frac{\frac{2}{7}+\frac{1}{13}\cdot\left(\frac{-2+15}{10}\right)}{(-2)\cdot\frac{1}{5}+\frac{3}{5}} \text{ por Teorema 4.6-(i)}$$

$$= \frac{\frac{2}{7}+\frac{1}{13}\cdot\frac{13}{10}}{(-2)\cdot\frac{1}{5}+\frac{3}{5}}$$

$$= \frac{\frac{2}{7}+\frac{1\cdot 13}{13\cdot 10}}{(-2)\cdot\frac{1}{5}+\frac{3}{5}} \text{ por Teorema 4.6-(f)}$$

$$= \frac{\frac{2}{7}+\frac{1\cdot 1}{1\cdot 10}}{(-2)\cdot\frac{1}{5}+\frac{3}{5}} \text{ escribiendo fracciones equivalentes}$$

$$= \frac{\frac{2}{7}+\frac{1}{10}}{(-2)\cdot\frac{1}{5}+\frac{3}{5}}$$

$$= \frac{\frac{2}{7}+\frac{1}{10}}{-2\cdot\frac{1}{5}+\frac{3}{5}} \text{ por Teorema 4.5-(m)}$$

$$= \frac{\frac{2}{7}+\frac{1}{10}}{-\frac{2}{1}\cdot\frac{1}{5}+\frac{3}{5}} \text{ por Teorema 4.6-(c)}$$

$$= \frac{\frac{2}{7}+\frac{1}{10}}{-\frac{2\cdot 1}{1\cdot 5}+\frac{3}{5}} \text{ por Teorema 4.6-(f)}$$

$$= \frac{\frac{2}{7}+\frac{1}{10}}{-\frac{2}{5}+\frac{3}{5}}$$

$$= \frac{\frac{20}{70}+\frac{7}{70}}{-\frac{2}{5}+\frac{3}{5}} \text{ escribiendo fracciones equivalentes}$$

$$= \frac{\frac{20+7}{70}}{\frac{-2+3}{5}} \text{ por Teorema 4.6-(i)}$$

$$= \frac{\frac{27}{70}}{\frac{1}{5}}$$

$$= \frac{27\cdot 5}{70\cdot 1} \text{ por Teorema 4.6-(h)}$$

$$= \frac{27\cdot 1}{14\cdot 1} \text{ escribiendo fracciones equivalentes}$$

$$= \frac{27}{14}$$

(f)

$$\frac{-2}{\frac{2}{3}-\frac{5}{2}\cdot\left(-\frac{1}{3}\right)} - \frac{\frac{1}{2}\cdot\frac{3}{2}\cdot\left(-3+\frac{4}{3}\right)}{-\frac{1}{6}} = \frac{-2}{\frac{2}{3}+\frac{5}{2}\cdot\frac{1}{3}} - \frac{\frac{1}{2}\cdot\frac{3}{2}\cdot\left(-3+\frac{4}{3}\right)}{-\frac{1}{6}} \text{ por Teorema 4.5-(c)}$$

$$= \frac{-2}{\frac{2}{3}+\frac{5\cdot 1}{2\cdot 3}} - \frac{\frac{1\cdot 3}{2\cdot 2}\cdot\left(-3+\frac{4}{3}\right)}{-\frac{1}{6}} \text{ por Teorema 4.6-(f)}$$

$$= \frac{-2}{\frac{2}{3}+\frac{5}{6}} - \frac{\frac{3}{4}\cdot\left(-3+\frac{4}{3}\right)}{-\frac{1}{6}}$$

$$= \frac{-2}{\frac{2}{3}+\frac{5}{6}} - \frac{\frac{3}{4}\cdot\left(-\frac{3}{1}+\frac{4}{3}\right)}{-\frac{1}{6}} \text{ por Teorema 4.6-(c)}$$

$$= \frac{-2}{\frac{4}{6}+\frac{5}{6}} - \frac{\frac{3}{4}\cdot\left(-\frac{9}{3}+\frac{4}{3}\right)}{-\frac{1}{6}} \text{ escribiendo fracciones equivalentes}$$

$$= \frac{-2}{\frac{4+5}{6}} - \frac{\frac{3}{4}\cdot\left(\frac{-9+4}{3}\right)}{-\frac{1}{6}} \text{ por Teorema 4.6-(i)}$$

$$= \frac{-2}{\frac{9}{6}} - \frac{\frac{3}{4}\cdot\left(\frac{-5}{3}\right)}{-\frac{1}{6}}$$

$$= \frac{-2}{\frac{9}{6}} - \frac{-\frac{3}{4}\cdot\frac{5}{3}}{-\frac{1}{6}} \text{ por Teorema 4.5-(m)}$$

$$= -\frac{2}{\frac{9}{6}} - \frac{\frac{3}{4}\cdot\frac{5}{3}}{\frac{1}{6}} \text{ por Teorema 4.6-(d)}$$

$$= -\frac{2}{\frac{9}{6}} - \frac{\frac{3\cdot 5}{4\cdot 3}}{\frac{1}{6}} \text{ por Teorema 4.6-(f)}$$

$$= -\frac{2}{\frac{9}{6}} - \frac{\frac{1\cdot 5}{4\cdot 1}}{\frac{1}{6}} \text{ escribiendo fracciones equivalentes}$$

$$= -\frac{2}{\frac{9}{6}} - \frac{\frac{5}{4}}{\frac{1}{6}}$$

$$
\begin{aligned}
&= -\frac{\frac{2}{1}}{\frac{9}{6}} - \frac{\frac{5}{4}}{\frac{1}{6}} \text{ por Teorema 4.6-(c)} \\
&= -\frac{2 \cdot 6}{1 \cdot 9} - \frac{5 \cdot 6}{4 \cdot 1} \text{ por Teorema 4.6-(h)} \\
&= -\frac{2 \cdot 2}{1 \cdot 3} - \frac{5 \cdot 3}{2 \cdot 1} \text{ escribiendo fracciones equivalentes} \\
&= -\frac{4}{3} - \frac{15}{2} \\
&= -\frac{8}{6} - \frac{45}{6} \text{ escribiendo fracciones equivalentes} \\
&= -\left(\frac{8}{6} + \frac{45}{6}\right) \text{ por Teorema 4.5-(j)} \\
&= -\frac{8 + 45}{6} \text{ por Teorema 4.6-(i)} \\
&= -\frac{53}{6}
\end{aligned}
$$

5. LOS NÚMEROS NATURALES

Hasta ahora hemos distinguido sólo dos números reales concretos: 0 y 1. Operando con el 0 no logramos nada nuevo, pues $0 + 0 = 0$. Sin embargo, sabemos que $1 > 0$ por Teorema 4.7-(d). Luego

$$\begin{aligned} 0 < 1 &\Rightarrow 0 + 1 < 1 + 1 \text{ por Axioma (SC)} \\ &\Rightarrow 1 < 1 + 1 \text{ por Axiomas (S1) y (S3)} \end{aligned}$$

Luego $1 + 1$ es un número diferente a 0 y a 1. En nuestro sistema de numeración decimal, se denota $1 + 1 = 2$. De esta manera, sumando 1 vamos obteniendo números diferentes, a saber:

$$\begin{aligned} 1+1 &= 2, \\ 2+1 &= 3, \\ 3+1 &= 4, \\ 4+1 &= 5, \\ 5+1 &= 6, \\ &\vdots \\ 9+1 &= 10, \\ 10+1 &= 11, \\ &\vdots \\ 19+1 &= 20, \\ 20+1 &= 21, \\ &\vdots \\ 99+1 &= 100, \\ &\vdots \end{aligned}$$

En la escuela primaria hemos aprendido a manipular el sistema decimal (que consta de diez dígitos).

5.1. Conjuntos inductivos

Definición 5.1
Diremos que un conjunto $K \subset \mathbb{R}$ es inductivo si verifica las siguientes propiedades:

(a) $1 \in K$.

(b) Si $r \in K$ *entonces* $r + 1 \in K$.

Ejemplo 5.1

- $\mathbb{R}$ es un conjunto inductivo.
- $\{x \in \mathbb{R} : x > 1\}$ no es un conjunto inductivo, pues no cumple la Definición 5.1-(a) (el 1 no está en el conjunto).
- $\{1\}$ no es un conjunto inductivo, pues no cumple la Definición 5.1-(b) (el 2 no está en el conjunto).
- $\{x \in \mathbb{R} : 1 < x \leqslant 2\}$ no es un conjunto inductivo pues no satisface las Definiciones 5.1-(a) (el 1 no está) y 5.1-(b) (notar que el 2 está pero no así el 3).

- $\varnothing$ no es un conjunto inductivo, pues no satisface la Definición 5.1-(a) (pero sí satisface la Definición 5.1-(b) pues el antecedente es F).

Notar que si K es un conjunto inductivo, entonces:

$$\begin{aligned} 1 &\in K, \\ 2 = 1 + 1 &\in K, \\ 3 = 2 + 1 &\in K, \\ 4 = 3 + 1 &\in K, \\ 5 = 4 + 1 &\in K, \\ &\vdots \end{aligned}$$

5.2. Definición y algunas propiedades de los números naturales

Definición 5.2
Llamaremos conjunto de números naturales al subconjunto denotado por $\mathbb{N}$ *que está caracterizado por las siguientes propiedades:*

(N1) $\mathbb{N}$ *es inductivo.*

(N2) Si $H \subset \mathbb{R}$ *es inductivo, entonces* $\mathbb{N} \subset H$.

En otras palabras, $a \in \mathbb{N}$ si y sólo si a pertenece a todo conjunto inductivo. También se podría decir que $\mathbb{N}$ es el conjunto inductivo más pequeño.

Ejemplo 5.2
(a) Si H es inductivo entonces:

$$\begin{aligned} 1 &\in H, \\ 2 &\in H, \\ 3 &\in H, \\ 4 &\in H, \\ 5 &\in H, \\ &\vdots \end{aligned}$$

El conjunto H podría eventualmente tener otros elementos.

(b) De la Definición 5.2 surge que

$$\mathbb{N} = \{1, 2, 3, \ldots\},$$

pues el mínimo requerimiento para que un conjunto sea inductivo es que estén los elementos $1, 2, 3, \ldots$. Ese mínimo requerimiento lo satisface el conjunto $\{1, 2, 3, \ldots\}$.

(c) $\frac{1}{2} \notin \mathbb{N}$.
Veamos que $H = \{x \in \mathbb{R} : x \geqslant 1\}$ es un conjunto inductivo. Es claro que $1 \in H$. Por otro lado:

$$\begin{aligned} x \in H \quad &\Rightarrow \quad x \geqslant 1 \\ &\Rightarrow \quad x + 1 \geqslant 1 + 1 \text{ por Axioma (SC)} \\ &\Rightarrow \quad x + 1 \geqslant 2 \text{ por definición de 2} \\ &\Rightarrow \quad x + 1 \geqslant 2 > 1 \text{ por definición de 2} \end{aligned}$$

$$\begin{aligned} &\Rightarrow \quad x+1>1 \\ &\Rightarrow \quad x+1 \in H. \end{aligned}$$

Como H es inductivo, entonces $\mathbb{N} \subset H$. Ahora:

$$\begin{aligned} 1<2 \wedge 2>0 \quad &\Rightarrow \quad 1 \cdot 2^{-1} < 2 \cdot 2^{-1} \text{ por Axioma (PC) y Teorema 4.7-(e)} \\ &\Rightarrow \quad \frac{1}{2} < 1 \text{ por Definición 4.3 y Axioma (P4)} \\ &\Rightarrow \quad \frac{1}{2} \notin H \\ &\Rightarrow \quad \frac{1}{2} \notin \mathbb{N} \text{ pues } \mathbb{N} \subset H \end{aligned}$$

Proposición 5.1
Todo $n \in \mathbb{N}$ satisface que $n \geqslant 1$.

Demostración.
El conjunto $H = \{x \in \mathbb{R} : x \geqslant 1\}$ es inductivo (ver Ejemplo 5.2-(c)). Por Definición (N2) se tiene que $\mathbb{N} \subset H$. Luego, si $n \in \mathbb{N}$ entonces $n \in H$, por lo que $n \geqslant 1$. ■

Debido al Teorema 4.7-(d) sabemos que $1 > 0$. Luego, del Axioma (O2) se deduce el corolario que sigue a continuación.

Corolario 5.1
Todo $n \in \mathbb{N}$ satisface que $n > 0$.

Proposición 5.2
No existe un número natural n tal que $1 < n < 2$.

Demostración.
Supongamos que existe $n \in \mathbb{N}$ tal que $1 < n < 2$. Definamos

$$H = \{x \in \mathbb{R} : x = 1 \vee x \geqslant 2\}.$$

Veamos que H es un conjunto inductivo. Es claro que $1 \in H$. Supongamos ahora que $x \in H$. Si $x = 1$ entonces $x + 1 = 2 \in H$. Si $x \neq 1$ entonces

$$\begin{aligned} x \geqslant 2 \quad &\Rightarrow \quad x+1 \geqslant 2+1 \text{ por Axioma (SC)} \\ &\Rightarrow \quad x+1 \geqslant 3 \text{ por definición de 3} \\ &\Rightarrow \quad x+1 \geqslant 3 > 2 \text{ por definición de 3} \\ &\Rightarrow \quad x+1 > 2 \\ &\Rightarrow \quad x+1 \in H. \end{aligned}$$

Luego, por Definición (N2) se tiene que $\mathbb{N} \subset H$. Esto implica que $n \in H$, lo cual es una contradicción. ■

Ejemplo 5.3
(a) Si m y n son números naturales tales que $m < n$, entonces $\frac{m}{n} \notin \mathbb{N}$.

Debido al Corolario 5.1 se tiene que $n > 0$. Luego

$$\begin{aligned} m<n \wedge n>0 \quad &\Rightarrow \quad m \cdot n^{-1} < n \cdot n^{-1} \text{ por Axioma (PC) y Teorema 4.7-(e)} \\ &\Rightarrow \quad \frac{m}{n} < 1 \text{ por Definición 4.3 y Axioma (P4)} \\ &\Rightarrow \quad \frac{m}{n} \notin \mathbb{N} \text{ por Proposición 5.1} \end{aligned}$$

(b) No existe $x \in \mathbb{N}$ tal que $x^2 = 2$.

Supongamos que exista $x \in \mathbb{N}$ tal que $x^2 = 2$.

Si $x = 1$ entonces $x^2 = 1^2 = 1 \neq 2$, lo cual es una contradicción. Por lo tanto $x > 1$ debido a la Proposición 5.1. Pero por la Proposición 5.2 se tiene que $x \geqslant 2$. Como $x > 0$ (por el Corolario 5.1) y $2 > 0$ se tiene que $x^2 \geqslant 2^2 = 4 > 2$ por Teorema 4.7-(q), lo cual es también una contradicción.

(c) Si x e y son números naturales tales que $x \cdot y = 1$, entonces $x = y = 1$.

Asumamos que $x \neq 1$.

Debido a las Proposiciones 5.1 y 5.2 se tiene que $x \geqslant 2$. Por otra parte, también por la Proposición 5.1 se tiene que $y \geqslant 1$. Ahora:

$$2 = 2 \cdot 1 \leqslant 2 \cdot y \leqslant x \cdot y = 1,$$

con lo que concluiríamos que $2 \leqslant 1$, lo cual es una contradicción. Esto nos dice que $x = 1$.

Luego, de la hipótesis se tiene que $1 = x \cdot y = 1 \cdot y = y$, lo cual implica que también $y = 1$.

5.3. Principio de inducción

Teorema 5.1 (Principio de inducción)
Sea $H \subset \mathbb{N}$ tal que H es inductivo, es decir, satisface

- $1 \in H$.
- *Si* $r \in H$ *entonces* $r + 1 \in H$.

Entonces $H = \mathbb{N}$.

Demostración.
Por hipótesis sabemos que $H \subset \mathbb{N}$. Por otro lado, como H es inductivo, la Definición 5.2-(N2) nos dice que $\mathbb{N} \subset H$. Luego $H = \mathbb{N}$. ■

El principio de inducción nos permite establecer el siguiente criterio de demostración por inducción.

Criterio 5.1
Sea $P(n)$ una función proposicional con $n \in \mathbb{N}$. Si

- $P(1)$ *es V,*
- *la proposición cuantificada* $\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1)$ *es V,*

entonces la siguiente proposición cuantificada es V:

$$\forall n \in \mathbb{N}, P(n).$$

Demostración.
Definimos el siguiente conjunto:

$$H = \{n \in \mathbb{N} : P(n) \text{ es } V\}.$$

De la definición de H se desprende que $H \subset \mathbb{N}$

Por las hipótesis se tiene que $1 \in H$ y que cada vez que $n \in H$ ocurre que $n + 1 \in H$, de lo que resulta que H es inductivo. Por Teorema 5.1 se tiene que $H = N$. Esto quiere decir que $P(n)$ es V para todo $n \in \mathbb{N}$. ■

Definición 5.3 (Sumatoria y productoria)
Dada una lista $a_1, a_2, a_3, \ldots, a_n$ $(n \in \mathbb{N})$ de números reales se denomina suma de la lista al número real denotado por

$$\sum_{i=1}^{n} a_i,$$

tal que

$$\begin{aligned} \sum_{i=1}^{1} a_i &= a_1, \\ \sum_{i=1}^{n+1} a_i &= \left(\sum_{i=1}^{n} a_i\right) + a_{n+1}, \end{aligned}$$

En el caso que quisiéramos sumar $a_k, a_{k+1}, a_{k+2}, \ldots, a_n$ la definición es análoga y se denota por:

$$\sum_{i=k}^{n} a_i,$$

Ejemplo 5.4
A continuación veremos ejemplos de la utilización del criterio de inducción y el uso de sumatorias:

(a) Mostrar que para todo $n \in \mathbb{N}$ se cumple que:

$$\sum_{i=1}^{n} a_i = \sum_{i=2}^{n+1} a_{i-1}.$$

Sea la siguiente función proposicional definida en $\mathbb{N}$:

$$P(n): \quad \sum_{i=1}^{n} a_i = \sum_{i=2}^{n+1} a_{i-1}.$$

Observemos que $P(1)$ es V, pues

$$\begin{aligned} \sum_{i=1}^{1} a_i &= a_1, \text{ por Definición 5.3} \\ \sum_{i=2}^{1+1} a_{i-1} &= \sum_{i=2}^{2} a_{i-1} = a_{2-1} = a_1 \text{ por Definición 5.3} \end{aligned}$$

Asumamos ahora que $P(n)$ es V. Veamos que $P(n+1)$ es V:

$$\begin{aligned} \sum_{i=1}^{n+1} a_i &= \left(\sum_{i=1}^{n} a_i\right) + a_{n+1} \text{ por Definición 5.3} \\ &= \sum_{i=2}^{n+1} a_{i-1} + a_{n+1} \text{ pues } P(n) \text{ es } V \\ &= \sum_{i=2}^{n+1} a_{i-1} + a_{(n+2)-1} \\ &= \sum_{i=2}^{n+2} a_{i-1} \text{ por Definición 5.3} \end{aligned}$$

Luego la proposición $\forall n \in \mathbb{N}, P(n)$ es V debido al Criterio 5.1.

(b) Mostrar que para todo $n \in \mathbb{N}$ se satisface:

$$\sum_{i=1}^{n} i = \frac{n \cdot (n+1)}{2}.$$

Sea la siguiente función proposicional definida en $\mathbb{N}$:

$$P(n): \quad \sum_{i=1}^{n} i = \frac{n \cdot (n+1)}{2}.$$

Observemos que $P(1)$ es V, pues

$$\frac{1 \cdot (1+1)}{2} = \frac{2}{2} = 1 = \sum_{i=1}^{1} i.$$

Asumamos ahora que $P(n)$ es V. Veamos que $P(n+1)$ es V:

$$\begin{aligned}
\sum_{i=1}^{n+1} i &= \sum_{i=1}^{n} i + (n+1) \text{ por Definición 5.3} \\
&= \frac{n \cdot (n+1)}{2} + (n+1) \text{ pues } P(n) \text{ es } V \\
&= \frac{n \cdot (n+1) + 2 \cdot (n+1)}{2} = \frac{(n+1) \cdot (n+2)}{2} \\
&= \frac{(n+1) \cdot [(n+1)+1]}{2}
\end{aligned}$$

Luego la proposición $\forall n \in \mathbb{N}, P(n)$ es V debido al Criterio 5.1.

(c) Mostrar que para todo $n \in \mathbb{N}$ se cumple que:

$$\sum_{i=1}^{n} (2 \cdot i - 1) = n^2.$$

Sea la siguiente función proposicional definida en $\mathbb{N}$:

$$P(n): \quad \sum_{i=1}^{n} (2 \cdot i - 1) = n^2.$$

Observemos que $P(1)$ es V, pues

$$\sum_{i=1}^{1} (2 \cdot i - 1) = 2 \cdot 1 - 1 = 1 = 1^2.$$

Asumamos ahora que $P(n)$ es V. Veamos que $P(n+1)$ es V:

$$\begin{aligned}
\sum_{i=1}^{n+1} (2 \cdot i - 1) &= \sum_{i=1}^{n} (2 \cdot i - 1) + [2 \cdot (n+1) - 1] \text{ por Definición 5.3} \\
&= n^2 + [2 \cdot (n+1) - 1] \text{ pues } P(n) \text{ es } V \\
&= n^2 + 2 \cdot n + 2 - 1 = n^2 + 2 \cdot n + 1 \\
&= (n+1)^2 \text{ por Teorema 4.5-(y)}
\end{aligned}$$

Luego la proposición $\forall n \in \mathbb{N}, P(n)$ es V debido al Criterio 5.1.

(d) Mostrar que para todo $n \in \mathbb{N}$ se cumple que:

$$\sum_{i=1}^{n} i^2 = \frac{n \cdot (n+1) \cdot (2 \cdot n + 1)}{6}.$$

Sea la siguiente función proposicional definida en $\mathbb{N}$:

$$P(n): \quad \sum_{i=1}^{n} i^2 = \frac{n \cdot (n+1) \cdot (2 \cdot n + 1)}{6}.$$

Observemos que $P(1)$ es V, pues

$$\frac{1 \cdot (1+1) \cdot (2 \cdot 1 + 1)}{6} = \frac{1 \cdot 2 \cdot 3}{6} = \frac{6}{6} = 1 = 1^2 = \sum_{i=1}^{1} i^2.$$

Asumamos ahora que $P(n)$ es V. Veamos que $P(n+1)$ es V:

$$\begin{aligned}
\sum_{i=1}^{n+1} i^2 &= \sum_{i=1}^{n} i^2 + (n+1)^2 \text{ por Definición 5.3} \\
&= \frac{n \cdot (n+1) \cdot (2 \cdot n + 1)}{6} + (n+1)^2 \text{ pues } P(n) \text{ es } V \\
&= \frac{n \cdot (n+1) \cdot (2 \cdot n + 1) + 6 \cdot (n+1)^2}{6} \\
&= \frac{(n+1) \cdot [n \cdot (2 \cdot n + 1) + 6 \cdot (n+1)]}{6} \\
&= \frac{(n+1) \cdot (2 \cdot n^2 + n + 6 \cdot n + 6)}{6} \\
&= \frac{(n+1) \cdot (2 \cdot n^2 + 7 \cdot n + 6)}{6} \\
&= \frac{2 \cdot n^3 + 7 \cdot n^2 + 6 \cdot n + 2 \cdot n^2 + 7 \cdot n + 6}{6} \\
&= \frac{2 \cdot n^3 + 9 \cdot n^2 + 13 \cdot n + 6}{6}
\end{aligned}$$

Luego

$$\begin{aligned}
\frac{(n+1) \cdot (n+2) \cdot [2 \cdot (n+1) + 1]}{6} &= \frac{(n+1) \cdot (n+2) \cdot (2 \cdot n + 2 + 1)}{6} \\
&= \frac{(n+1) \cdot (n+2) \cdot (2 \cdot n + 3)}{6} \\
&= \frac{(n^2 + 2 \cdot n + n + 2) \cdot (2 \cdot n + 3)}{6} \\
&= \frac{(n^2 + 3 \cdot n + 2) \cdot (2 \cdot n + 3)}{6} \\
&= \frac{2 \cdot n^3 + 3 \cdot n^2 + 6 \cdot n^2 + 9 \cdot n + 4 \cdot n + 6}{6} \\
&= \frac{2 \cdot n^3 + 9 \cdot n^2 + 13 \cdot n + 6}{6}
\end{aligned}$$

Por lo tanto la proposición $\forall n \in \mathbb{N}, P(n)$ es V debido al Criterio 5.1.

(e) Mostrar que para todo $n \in \mathbb{N}$ se cumple que:

$$\sum_{i=1}^{n} \frac{1}{i \cdot (i+1)} = \frac{n}{n+1}.$$

Sea la siguiente función proposicional definida en $\mathbb{N}$:

$$P(n): \quad \sum_{i=1}^{n} \frac{1}{i \cdot (i+1)} = \frac{n}{n+1}.$$

Observemos que $P(1)$ es V, pues

$$\sum_{i=1}^{1} \frac{1}{i \cdot (i+1)} = \frac{1}{1 \cdot (1+1)} = \frac{1}{(1+1)}.$$

Asumamos ahora que $P(n)$ es V. Veamos que $P(n+1)$ es V:

$$\begin{aligned}
\sum_{i=1}^{n+1} \frac{1}{i \cdot (i+1)} &= \sum_{i=1}^{n} \frac{1}{i \cdot (i+1)} + \frac{1}{(n+1) \cdot (n+2)} \text{ por Definición 5.3} \\
&= \frac{n}{n+1} + \frac{1}{(n+1) \cdot (n+2)} \text{ pues } P(n) \text{ es } V \\
&= \frac{n \cdot (n+2) + 1}{(n+1) \cdot (n+2)} \\
&= \frac{n^2 + 2 \cdot n + 1}{(n+1) \cdot (n+2)} \\
&= \frac{(n+1)^2}{(n+1) \cdot (n+2)} \\
&= \frac{n+1}{n+2} \\
&= \frac{n+1}{(n+1)+1}
\end{aligned}$$

Luego la proposición $\forall n \in \mathbb{N}, P(n)$ es V debido al Criterio 5.1.

5.4. Suma y resta en $\mathbb{N}$

Teorema 5.2 ($\mathbb{N}$ es cerrado para la suma y el producto en $\mathbb{R}$)
Sean a y b números naturales. Entonces:

(a) $a + b \in \mathbb{N}$.

(b) $a \cdot b \in \mathbb{N}$.

Demostración.
(a) Sea $a \in \mathbb{N}$ y definamos el siguiente conjunto:

$$H = \{b \in \mathbb{N} : a + b \in \mathbb{N}\}.$$

Veamos que H es un conjunto inductivo:

- Como el conjunto $\mathbb{N}$ es inductivo (ver Definición 5.2), ocurre que como $a \in \mathbb{N}$ entonces $a+1 \in \mathbb{N}$. Esto significa que $1 \in H$.
- Supongamos que $b \in H$. Esto significa que $a + b \in \mathbb{N}$. Entonces $a + (b + 1) = (a + b) + 1 \in \mathbb{N}$ pues $\mathbb{N}$ es inductivo. Esto implica que $b + 1 \in H$.

Como $H \subset \mathbb{N}$, el Teorema 5.1 nos dice que $H = \mathbb{N}$. Esto significa que $a + b \in \mathbb{N}$ para todo $b \in \mathbb{N}$. Como a era arbitrario, entonces vale lo que queríamos demostrar.

(b) Sea $a \in \mathbb{N}$ y definamos el siguiente conjunto:

$$H = \{b \in \mathbb{N} : a \cdot b \in \mathbb{N}\}.$$

Veamos que H es un conjunto inductivo:

- Como $a \in \mathbb{N}$, entonces $a \cdot 1 = a \in \mathbb{N}$. Esto significa que $1 \in H$.
- Supongamos que $b \in H$. Esto significa que $a \cdot b \in \mathbb{N}$. Entonces $a \cdot (b + 1) = a \cdot b + a \in \mathbb{N}$ debido a lo probado en (a), lo cual implica que $b + 1 \in H$.

Como $H \subset \mathbb{N}$, el Teorema 5.1 nos dice que $H = \mathbb{N}$. Esto significa que $a \cdot b \in \mathbb{N}$ para todo $b \in \mathbb{N}$. Como a era arbitrario, entonces vale lo que queríamos demostrar. ■

Observemos que si $a \in \mathbb{N}$ entonces $-a \notin \mathbb{N}$, pues si $-a \in \mathbb{N}$ entonces $0 = a + (-a) \in \mathbb{N}$, lo cual es una contradicción (ver Corolario 5.1).

Lema 5.1
Si $b \in \mathbb{N}$ tal que $b > 1$, entonces existe $c \in \mathbb{N}$ tal que $b = c + 1$.

Demostración.
Definamos el conjunto:

$$H = \{1\} \cup \{x + 1 : x \in \mathbb{N}\}.$$

Claramente se observa que $H \subset \mathbb{N}$ (pues $\mathbb{N}$ es un conjunto inductivo) y que H es un conjunto inductivo. El Teorema 5.1 nos asegura que $H = \mathbb{N}$.

Como $b \in \mathbb{N} = H$ y $b \neq 1$, entonces $b \in \{x + 1 : x \in \mathbb{N}\}$. Esto implica que existe $c \in \mathbb{N}$ tal que $b = c + 1$. ■

Teorema 5.3 (Posibilidad de la resta en $\mathbb{N}$)
Si a y b son números naturales tales que $a < b$, entonces $b - a \in \mathbb{N}$.

Demostración.
Definamos el siguiente conjunto:

$$H = \{a \in \mathbb{N} : b \in \mathbb{N} \wedge a < b \Rightarrow b - a \in \mathbb{N}\}.$$

Por definición se ve que $H \subset \mathbb{N}$.
Veamos que H es inductivo.

- Por Lema 5.1, si $b \in \mathbb{N}$ y $b > 1$ entonces existe $c \in \mathbb{N}$ tal que $c + 1 = b$. Luego, $b - 1 = c \in \mathbb{N}$. Esto nos dice que $1 \in H$.

- Asumamos que $a \in H$ y probemos que $a+1 \in H$. Tomemos $b \in \mathbb{N}$ tal que $a+1 < b$. Como $a \in H \subset \mathbb{N}$ entonces $a \geqslant 1$ por Proposición 5.1. Luego:

$$1 \leqslant a < a+1 < b.$$

Esto último implica que $1 < b$, y por el Lema 5.1 se deduce que existe $c \in \mathbb{N}$ tal que $c+1 = b$. Luego $a+1 < b = c+1$, o sea $a+1 < c+1$, lo que implica que $a < c$.

Como $c \in \mathbb{N}$ y $a < c$ entonces $c-a \in \mathbb{N}$ pues $a \in H$. Ahora:

$$\begin{aligned} b-(a+1) &= (c+1)-(a+1) \\ &= c-a \in \mathbb{N} \end{aligned}$$

Por el Teorema 5.1 se observa que $H = N$, lo cual dice que si a y b son números naturales tal que $a < b$, entonces $b-a \in \mathbb{N}$. ■

Corolario 5.2

(a) Si a y b son números naturales tal que $a < b$, entonces $a+1 \leqslant b$.

(b) Si $n \in \mathbb{N}$, entonces $\{x \in \mathbb{N} : n < x < n+1\} = \varnothing$.

Demostración.
(a)

$$\begin{aligned} a < b &\Rightarrow b-a \in \mathbb{N} \text{ por Teorema 5.3} \\ &\Rightarrow 1 \leqslant b-a \text{ por Proposición 5.1} \\ &\Rightarrow a+1 \leqslant b \end{aligned}$$

(b) Supongamos que existe $x \in \mathbb{N}$ tal que $n < x < n+1$. Luego:

$$\begin{aligned} n < x < n+1 &\Rightarrow n-(n-1) < x-(n-1) < n+1-(n-1) \text{ por Axioma (SC)} \\ &\Rightarrow n-n+1 < x-(n-1) < n+1-n+1 \\ &\Rightarrow 1 < x-(n-1) < 2 \end{aligned}$$

Por otro lado, notemos que:

$$\begin{aligned} n-1 < n < x &\Rightarrow n-1 < x \\ &\Rightarrow n < x+1 \\ &\Rightarrow x+1-n \in \mathbb{N} \text{ por Teorema 5.3} \\ &\Rightarrow x-(n-1) \in \mathbb{N}. \end{aligned}$$

Por lo tanto tenemos que $x-(n-1)$ es un número natural tal que $1 < x-(n-1) < 2$, lo cual es una contradicción debido a la Proposición 5.2. ■

5.5. Potenciación natural de números reales

Definición 5.4 (Potenciación natural)
Dados $x \in \mathbb{R}$ y $n \in \mathbb{N}$, definimos x^n inductivamente como se detalla a continuación:

$$\begin{aligned} x^1 &= x, \\ x^{n+1} &= (x^n) \cdot x. \end{aligned}$$

Si $x \neq 0$ se define

$$x^0 = 1.$$

La Definición 5.4 nos permite definir la potencia de un número real cuando el exponente es un número natural o cero. Notar que la expresión 0^0 carece de sentido por el momento.

Proposición 5.3
Sean $x, y \in \mathbb{R}$ y $m, n \in \mathbb{N} \cup \{0\}$. Entonces:

(a) $x^m \cdot x^n = x^{m+n}$.

(b) $(x^m)^n = x^{m \cdot n}$.

(c) $(x \cdot y)^m = x^m \cdot y^m$.

(d) Si $x > 0$, $y > 0$, $n \in \mathbb{N}$ *y* $x < y$ *entonces* $x^n < y^n$.

(e) Si $x > 1$ *y* $n \in \mathbb{N}$ *entonces* $x^n < x^{n+1}$.

(f) Si $x > 1$ *y* $n \in \mathbb{N}$ *entonces* $x^n > 1$.

(g) Si $x > 1$, $n, m \in \mathbb{N}$ *y* $n < m$ *entonces* $x^n < x^m$.

(h) Si $y \neq 0$ *entonces* $\left(\dfrac{x}{y}\right)^n = \dfrac{x^n}{y^n}$.

(i) Si $y \neq 0$ *entonces* $(y^{-1})^n = (y^n)^{-1}$.

Quedan excluídas todas las situaciones que den lugar a 0^0.

Demostración.
(a) Supongamos que $m = 0$. Para evitar cosas que no están definidas, debemos pedir que $x \neq 0$. Luego:

$$\begin{aligned} x^m \cdot x^n &= x^0 \cdot x^n \\ &= 1 \cdot x^n \text{ por Definición 5.4} \\ &= x^n \\ &= x^{0+n} \\ &= x^{m+n} \end{aligned}$$

Supongamos que $n = 0$. Como antes, debemos pedir que $x \neq 0$. Luego:

$$\begin{aligned} x^m \cdot x^n &= x^m \cdot x^0 \\ &= x^m \cdot 1 \text{ por Definición 5.4} \\ &= x^m \\ &= x^{m+0} \\ &= x^{m+n} \end{aligned}$$

Supongamos ahora que $m, n \in \mathbb{N}$. Aquí no hay restricciones para x. Vamos a hacer la demostración por inducción en n. Definimos la siguiente función proposicional definida en $\mathbb{N}$:

$$P(n): \quad x^m \cdot x^n = x^{m+n}.$$

Observemos que $P(1)$ es V, pues

$$\begin{aligned} x^m \cdot x^1 &= x^m \cdot x \text{ por Definición 5.4} \\ &= x^{m+1} \text{ por Definición 5.4} \end{aligned}$$

Asumamos ahora que $P(n)$ es V. Veamos que $P(n+1)$ es V:

$$\begin{aligned} x^m \cdot x^{n+1} &= x^m \cdot (x^n \cdot x) \text{ por Definición 5.4} \\ &= (x^m \cdot x^n) \cdot x \text{ por asociatividad} \\ &= x^{m+n} \cdot x \text{ pues } P(n) \text{ es } V \\ &= x^{(m+n)+1} \\ &= x^{m+(n+1)} \text{ por asociatividad} \end{aligned}$$

Luego la proposición $\forall n \in \mathbb{N}, P(n)$ es V debido al Criterio 5.1.

(b) Supongamos que $m = 0$. Para evitar cosas que no están definidas, debemos pedir que $x \neq 0$. Luego:

$$\begin{aligned} (x^m)^n &= \left(x^0\right)^n \text{ por hipótesis} \\ &= 1^n \text{ por Definición 5.4} \\ &= 1 \\ &= x^0 \text{ por Definición 5.4} \\ &= x^{0 \cdot n} \\ &= x^{m \cdot n} \end{aligned}$$

Supongamos que $n = 0$. Como antes, debemos pedir que $x \neq 0$:

$$\begin{aligned} (x^m)^n &= (x^m)^0 \text{ por hipótesis} \\ &= 1 \text{ por Definición 5.4} \\ &= x^0 \text{ por Definición 5.4} \\ &= x^{m \cdot 0} \\ &= x^{m \cdot n} \end{aligned}$$

Supongamos ahora que $m, n \in \mathbb{N}$. Aquí no hay restricciones para x. Vamos a hacer la demostración por inducción en n. Definimos la siguiente función proposicional definida en $\mathbb{N}$:

$$P(n): \quad (x^m)^n = x^{m \cdot n}.$$

Observemos que $P(1)$ es V, pues

$$\begin{aligned} (x^m)^1 &= x^m \text{ por Definición 5.4} \\ &= x^{m \cdot 1}. \end{aligned}$$

Asumamos ahora que $P(n)$ es V. Veamos que $P(n+1)$ es V:

$$\begin{aligned} (x^m)^{n+1} &= (x^m)^n \cdot x^m \text{ por Definición 5.4} \\ &= x^{m \cdot n} \cdot x^m \text{ pues } P(n) \text{ es } V \\ &= x^{m \cdot n + m} \text{ por (a)} \\ &= x^{m \cdot (n+1)} \end{aligned}$$

Luego la proposición $\forall n \in \mathbb{N}, P(n)$ es V debido al Criterio 5.1.

(c) Supongamos que $m = 0$. Para evitar cosas que no están definidas, debemos pedir que $x \neq 0$ y que $y \neq 0$. Luego:

$$(x \cdot y)^m = (x \cdot y)^0 \text{ por hipótesis}$$

$$\begin{aligned} &= 1 \text{ por Definición 5.4} \\ &= 1 \cdot 1 \\ &= x^0 \cdot y^0 \text{ por Definición 5.4} \\ &= x^m \cdot y^m \text{ por hipótesis} \end{aligned}$$

Supongamos ahora que $m \in \mathbb{N}$. Aquí no hay restricciones para x e y. Vamos a hacer la demostración por inducción en m. Definimos la siguiente función proposicional definida en $\mathbb{N}$:

$$P(m): \quad (x \cdot y)^m = x^m \cdot y^m.$$

Observemos que $P(1)$ es V, pues

$$\begin{aligned} (x \cdot y)^1 &= x \cdot y \text{ por Definición 5.4} \\ &= x^1 \cdot y^1 \text{ por Definición 5.4} \end{aligned}$$

Asumamos ahora que $P(m)$ es V. Veamos que $P(m+1)$ es V:

$$\begin{aligned} (x \cdot y)^{m+1} &= (x \cdot y)^m \cdot (x \cdot y) \text{ por Definición 5.4} \\ &= x^m \cdot y^m \cdot x \cdot y \text{ pues } P(n) \text{ es } V \\ &= x^m \cdot x \cdot y^m \cdot y \text{ por conmutatividad} \\ &= x^{m+1} \cdot y^{m+1} \text{ por Definición 5.4} \end{aligned}$$

Luego la proposición $\forall m \in \mathbb{N}, P(m)$ es V debido al Criterio 5.1.

(d) Vamos a hacer la demostración por inducción en n. Definimos la siguiente función proposicional definida en $\mathbb{N}$:

$$P(n): \quad x^n < y^n.$$

Observemos que $P(1)$ es V, pues $x < y$ por hipótesis.
Asumamos ahora que $P(n)$ es V. Veamos que $P(n+1)$ es V:

$$\begin{aligned} x^{n+1} &= x^n \cdot x \text{ por Definición 5.4} \\ &= x \cdot x^n \\ &< x \cdot y^n \text{ pues } P(n) \text{ es } V \text{ y porque } x > 0 \\ &< y \cdot y^n \text{ pues } x < y \text{ e } y > 0 \text{ (y por lo tanto } y^n > 0) \\ &< y^n \cdot y \\ &= y^{n+1} \text{ por Definición 5.4} \end{aligned}$$

Luego la proposición $\forall n \in \mathbb{N}, P(n)$ es V debido al Criterio 5.1.

(e) Vamos a hacer la demostración por inducción en n. Definimos la siguiente función proposicional definida en $\mathbb{N}$:

$$P(n): \quad x^n < x^{n+1}.$$

Observemos que $P(1)$ es V, pues como $x > 1$ entonces $x^2 > x$ por Axioma (PC).
Asumamos ahora que $P(n)$ es V. Veamos que $P(n+1)$ es V:

$$\begin{aligned} x^n < x^{n+1} &\Rightarrow x \cdot x^n < x \cdot x^{n+1} \text{ por Axioma (PC)} \\ &\Rightarrow x^{n+1} < x^{n+2} \text{ por Definición 5.4} \\ &\Rightarrow x^{n+1} < x^{(n+1)+1} \end{aligned}$$

Luego la proposición $\forall n \in \mathbb{N}, P(n)$ es V debido al Criterio 5.1.

(f) Vamos a hacer la demostración por inducción en n. Definimos la siguiente función proposicional definida en $\mathbb{N}$:

$$P(n): \quad x^n > 1.$$

Observemos que $P(1)$ es V, pues

$$\begin{aligned} x^1 &= x \text{ por Definición 5.4} \\ &> 1 \text{ por hipótesis} \end{aligned}$$

Asumamos ahora que $P(n)$ es V. Veamos que $P(n+1)$ es V:

$$\begin{aligned} x^n > 1 &\Rightarrow x^n \cdot x > 1 \cdot x \text{ pues } P(n) \text{ es } V \text{ y por Axioma (PC)} \\ &\Rightarrow x^{n+1} > x > 1 \text{ por Definición 5.4 e hipótesis} \end{aligned}$$

Luego la proposición $\forall n \in \mathbb{N}, P(n)$ es V debido al Criterio 5.1.

(g) Por Teorema 5.3 se tiene que $m - n \in \mathbb{N}$. Por (f) obtenemos que $x^{m-n} > 1$. Por otro lado $x^n > 1 > 0$ por (f). Ahora:

$$\begin{aligned} x^{m-n} > 1 &\Rightarrow x^{m-n} \cdot x^n > 1 \cdot x^n \text{ por Axioma (PC)} \\ &\Rightarrow x^{m-n} \cdot x^n > x^n \\ &\Rightarrow x^m > x^n \text{ por (a)} \end{aligned}$$

(h) Supongamos que $n = 0$. Para evitar cosas que no están definidas, debemos pedir que $x \neq 0$. Luego:

$$\begin{aligned} \left(\frac{x}{y}\right)^n &= \left(\frac{x}{y}\right)^0 \text{ por hipótesis} \\ &= 1 \text{ por Definición 5.4} \\ &= \frac{1}{1} \text{ por Teorema 4.6-(c)} \\ &= \frac{x^0}{y^0} \text{ por Definición 5.4} \\ &= \frac{x^n}{y^n} \text{ por hipótesis} \end{aligned}$$

Supongamos ahora que $n \in \mathbb{N}$. Aquí no hay restricciones para x. Vamos a hacer la demostración por inducción en n. Definimos la siguiente función proposicional definida en $\mathbb{N}$:

$$P(n): \quad \left(\frac{x}{y}\right)^n = \frac{x^n}{y^n}.$$

Observemos que $P(1)$ es V, pues

$$\begin{aligned} \left(\frac{x}{y}\right)^1 &= \frac{x}{y} \text{ por Definición 5.4} \\ &= \frac{x^1}{y^1} \text{ por Definición 5.4} \end{aligned}$$

Asumamos ahora que $P(n)$ es V. Veamos que $P(n+1)$ es V:

$$\begin{aligned}\left(\frac{x}{y}\right)^{n+1} &= \left(\frac{x}{y}\right)^{n} \cdot \frac{x}{y} \text{ por Definición 5.4}\\ &= \frac{x^n}{y^n} \cdot \frac{x}{y} \text{ pues } P(n) \text{ es } V\\ &= \frac{x^n \cdot x}{y^n \cdot y} \text{ por Teorema 4.6-(f)}\\ &= \frac{x^{n+1}}{y^{n+1}} \text{ por Definición 5.4}\end{aligned}$$

Luego la proposición $\forall n \in \mathbb{N}, P(n)$ es V debido al Criterio 5.1.

(i) Como $y \neq 0$ entonces existe y^{-1}. Ahora tenemos que:

$$\begin{aligned}y \cdot y^{-1} = 1 &\Rightarrow \left(y \cdot y^{-1}\right)^n = 1^n\\ &\Rightarrow y^n \cdot \left(y^{-1}\right)^n = 1 \text{ por (c)}\\ &\Rightarrow \left(y^n\right)^{-1} = \left(y^{-1}\right)^n \text{ por unicidad del inverso}\end{aligned}$$

■

5.6. Ejemplos de utilización de las propiedades

En los siguientes ejercicios mostraremos la utilización de las propiedades descriptas anteriormente.

Ejemplo 5.5
Realizar los siguientes cálculos:

(a)

$$\begin{aligned}\left(\frac{-3}{2}\right)^2 + \left(\frac{4}{5}\right)^2 &= \frac{(-3)^2}{2^2} + \frac{4^2}{5^2} \text{ por Proposición 5.3-(h)}\\ &= \frac{3^2}{2^2} + \frac{4^2}{5^2} \text{ por Teorema 4.5-(n)}\\ &= \frac{9}{4} + \frac{16}{25}\\ &= \frac{9 \cdot 25}{100} + \frac{4 \cdot 16}{100} \text{ escribiendo fracciones equivalentes}\\ &= \frac{225}{100} + \frac{64}{100}\\ &= \frac{225 + 64}{100} \text{ por Teorema 4.6-(i)}\\ &= \frac{289}{100} \text{ por Teorema 4.6-(i)}\end{aligned}$$

(b)

$$\left(\frac{3}{5} \cdot \frac{20}{16}\right)^2 = \left(\frac{3}{5} \cdot \frac{5}{4}\right)^2 \text{ escribiendo fracciones equivalentes}$$

$$= \left(\frac{3}{5}\right)^2 \cdot \left(\frac{5}{4}\right)^2 \text{ por Proposición 5.3-(c)}$$

$$= \frac{3^2}{5^2} \cdot \frac{5^2}{4^2} \text{ por Proposición 5.3-(h)}$$

$$= \frac{3^2 \cdot 5^2}{5^2 \cdot 4^2} \text{ por Teorema 4.6-(f)}$$

$$= \frac{3^2}{4^2} \text{ escribiendo fracciones equivalentes}$$

$$= \frac{9}{16}$$

(c)

$$\left(\frac{1}{2}\right)^3 \cdot \left(\frac{1}{2}\right)^2 = \left(\frac{1}{2}\right)^{3+2} \text{ por Proposición 5.3-(a)}$$

$$= \left(\frac{1}{2}\right)^5$$

$$= \frac{1^5}{2^5} \text{ por Proposición 5.3-(h)}$$

$$= \frac{1}{32}$$

(d)

$$\left[\left(\frac{2}{3}\right)^3\right]^2 = \left(\frac{2}{3}\right)^{3\cdot 2} \text{ por Proposición 5.3-(b)}$$

$$= \left(\frac{2}{3}\right)^6$$

$$= \frac{2^6}{3^6} \text{ por Proposición 5.3-(h)}$$

$$= \frac{64}{729}$$

5.7. Números combinatorios o coeficientes binomiales

Definición 5.5 (Factorial)
Dado $n \in \mathbb{N}$ definimos el factorial de n al número real denotado por $n!$ tal que:

$$1! = 1,$$
$$(n+1)! = (n+1) \cdot n!.$$

Definimos también:

$$0! = 1.$$

Ejemplo 5.6

$$\begin{aligned}
0! &= 1,\\
1! &= 1,\\
2! &= 2\cdot 1! = 2\cdot 1 = 2,\\
3! &= 3\cdot 2! = 3\cdot 2\cdot 1 = 6,\\
4! &= 4\cdot 3! = 4\cdot 3\cdot 2\cdot 1 = 24,\\
5! &= 5\cdot 4! = 5\cdot 4\cdot 3\cdot 2\cdot 1 = 120,\\
&\vdots
\end{aligned}$$

Definición 5.6 (Número combinatorio)
Dados $m, n \in \mathbb{N}\cup\{0\}$ tal que $m \geqslant n$, se define

$$\binom{m}{n} = \frac{m!}{(m-n)!\cdot n!},$$

y se denomina número combinatorio o coeficiente binomial.

Ejemplo 5.7
(a)

$$\begin{aligned}
\binom{5}{3} &= \frac{5!}{(5-3)!\cdot 3!} \text{ por Definición 5.6}\\
&= \frac{5!}{2!\cdot 3!}\\
&= \frac{5\cdot 4\cdot 3\cdot 2\cdot 1}{2\cdot 1\cdot 3\cdot 2\cdot 1}\\
&= \frac{5\cdot 4}{2\cdot 1}\\
&= \frac{20}{2}\\
&= 10
\end{aligned}$$

(b)

$$\begin{aligned}
\binom{5}{2} &= \frac{5!}{(5-2)!\cdot 2!} \text{ por Definición 5.6}\\
&= \frac{5!}{3!\cdot 2!}\\
&= \frac{5\cdot 4\cdot 3\cdot 2\cdot 1}{3\cdot 2\cdot 1\cdot 2\cdot 1}\\
&= \frac{5\cdot 4}{2\cdot 1}\\
&= \frac{20}{2}\\
&= 10
\end{aligned}$$

(c)

$$\begin{aligned}\binom{5}{1} &= \frac{5!}{(5-1)!\cdot 1!} \text{ por Definición 5.6}\\ &= \frac{5!}{4!\cdot 1!}\\ &= \frac{5\cdot 4!}{4!\cdot 1}\\ &= 5\end{aligned}$$

(d)

$$\begin{aligned}\binom{4}{0} &= \frac{4!}{(4-0)!\cdot 0!} \text{ por Definición 5.6}\\ &= \frac{4!}{4!\cdot 0!}\\ &= \frac{4!}{4!\cdot 1} \text{ por Definición 5.5}\\ &= \frac{4!}{4!}\\ &= 1\end{aligned}$$

(e)

$$\begin{aligned}\binom{3}{3} &= \frac{3!}{(3-3)!\cdot 3!} \text{ por Definición 5.6}\\ &= \frac{3!}{0!\cdot 3!}\\ &= \frac{3!}{1\cdot 3!} \text{ por Definición 5.5}\\ &= \frac{3!}{3!}\\ &= 1\end{aligned}$$

(f) $\binom{6}{3} = \binom{5}{2} + \binom{5}{3}$.

$$\begin{aligned}\binom{5}{2} + \binom{5}{3} &= 10 + 10 \text{ por los ejemplos anteriores}\\ &= 20\end{aligned}$$

$$\begin{aligned}\binom{6}{3} &= \frac{6!}{(6-3)!\cdot 3!} \text{ por Definición 5.6}\end{aligned}$$

$$
\begin{aligned}
&= \frac{6!}{3! \cdot 3!} \\
&= \frac{6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{3 \cdot 2 \cdot 1 \cdot 3 \cdot 2 \cdot 1} \\
&= \frac{6 \cdot 5 \cdot 4}{3 \cdot 2 \cdot 1} \\
&= \frac{120}{6} \\
&= 20
\end{aligned}
$$

Teorema 5.4 (Propiedades del número combinatorio)
Sean $m, n \in \mathbb{N} \cup \{0\}$ tal que $m \geqslant n$. Entonces

(a) $\binom{m}{0} = 1.$

(b) Si $m \geqslant 1$ entonces $\binom{m}{1} = m.$

(c) $\binom{m}{n} = \binom{m}{m-n}.$

(d) $\binom{m}{m} = 1.$

(e) Si $n \geqslant 1$ entonces $\binom{m+1}{n} = \binom{m}{n-1} + \binom{m}{n}.$

Demostración.
(a)

$$
\begin{aligned}
\binom{m}{0} &= \frac{m!}{(m-0)! \cdot 0!} \text{ por Definición 5.6} \\
&= \frac{m!}{m! \cdot 0!} \\
&= \frac{m!}{m! \cdot 1} \text{ por Definición 5.5} \\
&= \frac{m!}{m!} \\
&= 1
\end{aligned}
$$

(b)

$$
\begin{aligned}
\binom{m}{1} &= \frac{m!}{(m-1)! \cdot 1!} \text{ por Definición 5.6} \\
&= \frac{m!}{(m-1)! \cdot 1} \text{ por Definición 5.5}
\end{aligned}
$$

$$
\begin{aligned}
&= \frac{m!}{(m-1)!} \\
&= \frac{m \cdot (m-1)!}{(m-1)!} \text{ por Definición 5.5} \\
&= \frac{m}{1} \\
&= m
\end{aligned}
$$

(c)

$$
\begin{aligned}
\binom{m}{m-n} &= \frac{m!}{[m-(m-n)]! \cdot (m-n)!} \text{ por Definición 5.6} \\
&= \frac{m!}{(m-m+n)! \cdot (m-n)!} \\
&= \frac{m!}{n! \cdot (m-n)!} \\
&= \frac{m!}{(m-n)! \cdot n!} \\
&= \binom{m}{n} \text{ por Definición 5.6}
\end{aligned}
$$

(d)

$$
\begin{aligned}
\binom{m}{m} &= \binom{m}{m-m} \text{ por (c)} \\
&= \binom{m}{0} \\
&= 1 \text{ por (a)}
\end{aligned}
$$

(e)

$$
\begin{aligned}
\binom{m}{n-1} + \binom{m}{n} &= \frac{m!}{[m-(n-1)]! \cdot (n-1)!} + \frac{m!}{(m-n)! \cdot n!} \text{ por Definición 5.6} \\
&= \frac{m!}{(m-n+1)! \cdot (n-1)!} + \frac{m!}{(m-n)! \cdot n!} \\
&= \frac{m!}{(m-n+1) \cdot (m-n)! \cdot (n-1)!} + \frac{m!}{(m-n)! \cdot n \cdot (n-1)!} \text{ por Definición 5.5} \\
&= \frac{m! \cdot n + m! \cdot (m-n+1)}{(m-n+1) \cdot (m-n)! \cdot n \cdot (n-1)!} \text{ por Teorema 4.6-(i)} \\
&= \frac{m! \cdot (n+m-n+1)}{(m-n+1) \cdot (m-n)! \cdot n \cdot (n-1)!}
\end{aligned}
$$

$$= \frac{m! \cdot (m+1)}{(m-n+1)! \cdot n!} \text{ por Definición 5.5}$$

$$= \frac{(m+1)!}{[(m+1)-n]! \cdot n!} \text{ por Definición 5.5}$$

$$= \binom{m+1}{n}$$

■

Corolario 5.3
Si $m, n \in \mathbb{N} \cup \{0\}$ *tal que* $m \geqslant n$, *entonces* $\binom{m}{n} \in \mathbb{N}$.

Demostración.

Cuando $m = 0$ se tiene que $\binom{0}{0} = 1 \in \mathbb{N}$.

Ahora vamos a demostrar por inducción en m que

$$\binom{m}{n} \in \mathbb{N}, \quad m \geqslant n, \quad m \in \mathbb{N}, \quad n \in \mathbb{N} \cup \{0\}.$$

Definimos la siguiente función proposicional en $\mathbb{N}$:

$$P(m): \quad \forall n \in \mathbb{N} \cup \{0\} \text{ tal que } m \geqslant n, \quad \binom{m}{n} \in \mathbb{N}.$$

Observemos que $P(1)$ es V, pues

$$\binom{1}{0} = \binom{1}{1} = 1 \in \mathbb{N} \text{ por Teorema 5.4-(a) y 5.4-(b)}$$

Asumamos ahora que $P(m)$ es V. Veamos que $P(m+1)$ es V.

Primero notemos que $\binom{m+1}{0} = 1 \in \mathbb{N}$ por Teorema 5.4-(a). Consideremos ahora el caso cuando $m \geqslant n \geqslant 1$. Luego, por Teorema 5.4-(e), tenemos que $\binom{m+1}{n} = \binom{m}{n-1} + \binom{m}{n}$. Como estamos asumiendo que $P(m)$ es V, entonces $\binom{m}{n-1} \in \mathbb{N}$ y $\binom{m}{n} \in \mathbb{N}$. En virtud del Teorema 5.2-(a) se tiene que $\binom{m+1}{n} \in \mathbb{N}$. Finalmente se sabe también que $\binom{m+1}{m+1} \in \mathbb{N}$ por Teorema 5.4-(d).

Luego, la proposición $\forall m \in \mathbb{N}, P(m)$ es V debido al Criterio 5.1 y queda todo demostrado. ■

5.8. Combinatoria

5.8.1. Conceptos básicos

Definición 5.7 (Intervalo natural)
Dado $n \in \mathbb{N}$ *se define:*

$$[\![1, n]\!] = \{1, 2, \ldots, n\} = \{k \in \mathbb{N} : 1 \leqslant k \leqslant n\},$$
$$[\![1, n[\![= \{1, 2, \ldots, n-1\} = \{k \in \mathbb{N} : 1 \leqslant k < n\}.$$

Ejemplo 5.8
(a) $[\![1, 7]\!] = \{1, 2, 3, 4, 5, 6, 7\}$.

(b) $[\![1,7[\![= \{1,2,3,4,5,6\}$.

Vamos a formalizar el concepto de cantidad de elementos de un conjunto.

Definición 5.8 (Cardinalidad de un conjunto finito)
Sea $n \in \mathbb{N}$. Diremos que un conjunto A tiene n elementos si existe una biyección $f : [\![1,n]\!] \to A$. En tal caso, n se llama el cardinal de A y se denota por $|A|$. Un conjunto se dirá finito si $A = \varnothing$ o si existe $n \in \mathbb{N}$ tal que $|A| = n$. Diremos que $|\varnothing| = 0$.

Ejemplo 5.9
(a) El conjunto $A = \{a,b,c,d\}$ tiene cardinal 4.

En este caso podemos definir $f : [\![1,4]\!] \to A$ de la siguiente forma:

$$f(1) = a, \quad f(2) = b, \quad f(3) = c, \quad f(4) = d.$$

Claramente, f es una biyección, con lo que podemos afirmar que $|A| = 4$.

(b) El conjunto $A = \{1,3,a,z,\circ\}$ tiene cardinal 5.

Podemos definir $f : [\![1,5]\!] \to A$ de la siguiente forma:

$$f(1) = 1, \quad f(2) = 3, \quad f(3) = a, \quad f(4) = z, \quad f(5) = \circ.$$

Claramente, f es una biyección, con lo que podemos afirmar que $|A| = 5$.

5.8.2. Principio de adición

El principio de adición en términos de conjuntos se expresa en el siguiente teorema.

Teorema 5.5 (Principio de adición I)
Sean A y B conjuntos finitos disjuntos. Entonces $|A \cup B| = |A| + |B|$.

Demostración.
Si $A = \varnothing$ entonces

$$\begin{aligned} |A \cup B| &= |\varnothing \cup B| \\ &= |B| \text{ por Proposición 1.2-(b) y 1.2-(r)} \\ &= 0 + |B| \\ &= |\varnothing| + |B| \text{ por Definición 5.8} \\ &= |A| + |B| \end{aligned}$$

Si $B = \varnothing$ entonces

$$\begin{aligned} |A \cup B| &= |A \cup \varnothing| \\ &= |A| \text{ por Proposición 1.2-(r)} \\ &= |A| + 0 \\ &= |A| + |\varnothing| \text{ por Definición 5.8} \\ &= |A| + |B| \end{aligned}$$

Si $A \neq \varnothing$ y $B \neq \varnothing$ entonces existen $n, m \in \mathbb{N}$ y funciones biyectivas $f : [\![1,n]\!] \to A$ y $g : [\![1,m]\!] \to B$. Es decir,

$$f(i) = a_i, \quad 1 \leqslant i \leqslant n,$$

$$g(j) = b_j, \quad 1 \leqslant j \leqslant m,$$

donde $A = \{a_1, \ldots, a_n\}$ y $B = \{b_1, \ldots, b_m\}$.

Definimos la función $h : \{n+1, \ldots, n+m\} \to [\![1, m]\!]$ dada por:

$$h(x) = x - n.$$

Claramente h es una función biyectiva. Ahora sea $T : [\![1, n+m]\!] \to A \cup B$ definida por:

$$T(x) = \begin{cases} f(x), & x \in [\![1, n]\!], \\ g(h(x)), & x \in [\![n+1, n+m]\!]. \end{cases}$$

Esta función T es claramente biyectiva pues A y B son disjuntos:

$$\begin{aligned} T(1) &= f(1) = a_1, \\ &\vdots \\ T(n) &= f(n) = a_n, \\ T(n+1) &= g(h(n+1)) = g(1) = b_1, \\ &\vdots \\ T(n+m) &= g(h(n+m)) = g(m) = b_m. \end{aligned}$$

■

El principio de adición, aplicado a técnicas de conteo, puede expresarse de la siguiente manera:

Principio de adición II: Si una acción A se puede realizar de m formas distintas y otra acción B se puede realizar de n formas distintas, siendo A y B excluyentes (si se hace A no se hace B y vicecersa), entonces la cantidad de formas posibles de realizar la acción A o B es $m + n$.

Ejemplo 5.10

(a) Queremos comprar un helado de un solo gusto. La heladería ofrece 5 posibles gustos que incluyen chocolate (chocolate tentación, chocolate alpino, chocolate blanco, chocolate con dulce de leche, chocolate con maní) y 6 posibles gustos de fruta (banana, ananá, manzana, naranja, maracuyá, mandarina). ¿De cuántas formas podemos elegir nuestro helado?

La respuesta es 11. Podríamos definir el conjunto A cuyos elementos son los posibles gustos de chocolate, es decir,

$$\begin{aligned} A = \{&\text{chocolate tentación, chocolate alpino, chocolate blanco,} \\ &\text{chocolate con dulce de leche, chocolate con maní}\}. \end{aligned}$$

Asimismo, definimos el conjunto B cuyos elementos son los posibles gustos de fruta:

$$B = \{\text{banana, ananá, manzana, naranja, maracuyá, mandarina}\}.$$

Claramente los conjuntos A y B son disjuntos. De acuerdo al Teorema 5.5 se tiene que $|A \cup B| = |A| + |B| = 5 + 6 = 11$.

(b) Deseamos hacer un regalo de cumpleaños. Tenemos 4 diferentes prendas de vestir y 3 diferentes artefactos electrónicos. ¿Cuántos regalos posibles podemos hacer considerando que entregaremos solamente un objeto?

La respuesta es 7. En este caso la acción de regalar una prenda de vestir (acción A) puede realizarse de 4 formas diferentes, y la acción de regalar artefactos electrónicos (acción B) puede realizarse de 3 maneras distintas. Tales acciones son claramente excluyentes puesto que daremos un regalo que solamente contenga un objeto. Por ello la cantidad de formas posibles de regalar un objeto (acción A o B) es $4 + 3 = 7$.

El principio de la adición escrito en forma general puede ser expresado como:

Principio de adición I: Sean $A_1, \ldots, A_n$ conjuntos finitos disjuntos (dos a dos). Entonces:

$$|A_1 \cup \ldots \cup A_n| = \sum_{i=1}^{n} |A_i| .$$

Principio de adición II: Si acciones $A_1, \ldots, A_n$ se pueden realizar de $m_1, \ldots, m_n$ formas distintas respectivamente, siendo $A_1, \ldots A_n$ excluyentes, entonces la cantidad de formas posibles de realizar las acciones A_1 o A_2 o $\ldots$ o A_n es $m_1 + \ldots + m_n$.

5.8.3. Principio de multiplicación

El principio de multiplicación en términos de conjuntos se expresa en el siguiente teorema.

Teorema 5.6 (Principio de multiplicación I)
Sean A y B conjuntos finitos. Entonces $|A \times B| = |A| \cdot |B|$.

Demostración.
Si $A = \varnothing$ entonces $A \times B = \varnothing$. Luego

$$\begin{aligned} |A \times B| &= |\varnothing| \\ &= 0 \\ &= 0 \cdot |B| \\ &= |\varnothing| \cdot |B| \\ &= |A| \cdot |B| \end{aligned}$$

Si $B = \varnothing$ entonces $A \times B = \varnothing$. Luego

$$\begin{aligned} |A \times B| &= |\varnothing| \\ &= 0 \\ &= |A| \cdot 0 \\ &= |A| \cdot |\varnothing| \\ &= |A| \cdot |B| \end{aligned}$$

Si $A \neq \varnothing$ y $B \neq \varnothing$ entonces existen $n, m \in \mathbb{N}$ y funciones biyectivas $f : [\![1, n]\!] \to A$ y $g : [\![1, m]\!] \to B$. Es decir,

$$\begin{aligned} f(i) &= a_i, \quad 1 \leqslant i \leqslant n, \\ g(j) &= b_j, \quad 1 \leqslant j \leqslant m, \end{aligned}$$

donde $A = \{a_1, \ldots, a_n\}$ y $B = \{b_1, \ldots, b_m\}$. Luego se tiene que:

$$A \times B = (A \times \{b_1\}) \cup \ldots \cup (A \times \{b_m\}) ,$$

donde los participantes de esta unión son disjuntos dos a dos. Por el principio de la adición se tiene que:

$$|A \times B| = |A \times \{b_1\}| + \ldots + |A \times \{b_m\}| .$$

Notemos que dado j tal que $1 \leqslant j \leqslant m$:

$$A \times \{b_j\} = \{(a_1, b_j), \ldots, (a_n, b_j)\} ,$$

con lo cual es claro que $|A \times \{b_j\}| = n$. Luego,

$$|A \times B| = \sum_{j=1}^{m} |A \times \{b_j\}| = \sum_{j=1}^{m} n = n \cdot m = |A| \cdot |B|\,,$$

y esto concluye la prueba. ■

El principio de multiplicación, aplicado a técnicas de conteo, puede expresarse de la siguiente manera:

Principio de multiplicación II: Si una acción A se puede realizar de n formas distintas y una acción B se puede realizar de m formas distintas, siendo A y B acciones independientes, entonces la cantidad de formas de realizar la acción A y B es $n \cdot m$.

Ejemplo 5.11

(a) Estamos por levantarnos y pensamos qué vamos a desayunar. El desayuno incluye algo para tomar y algo para comer. Para tomar podemos elegir leche, chocolatada, té o café. Para comer podemos elegir tostadas, facturas o chipá. ¿De cuántas formas podemos armar nuestro desayuno?

La respuesta es 12. Podríamos definir el conjunto A cuyos elementos son las posibilidades para tomar, es decir,

$$A = \{\text{leche}, \text{chocolatada}, \text{té}, \text{café}\}\,.$$

Asimismo, definimos el conjunto B cuyos elementos son las posibilidades para comer:

$$B = \{\text{tostadas}, \text{facturas}, \text{chipá}\}\,.$$

Como el desayuno incluye algo para tomar y algo para comer, podríamos pensar a un desayuno como un par ordenado, cuya primer componente sea la bebida del desayuno, y la segunda componente sea lo que vamos a comer. Con este planteo, las posibilidades de desayuno son exactamente los elementos de $A \times B$. De acuerdo al Teorema 5.6 se tiene que $|A \times B| = |A| \cdot |B| = 4 \cdot 3 = 12$.

(b) Queremos comprarnos una computadora con ciertas características de espacio en disco y memoria RAM. Para las opciones de disco duro tenemos que elegir entre 1 TB, 2 TB y 4 TB. Para la memoria RAM podemos optar entre 4 GB, 8 GB, 16 GB, 32 GB y 64 GB. ¿De cuántas formas podemos armar nuestra computadora si nuestra placa madre soporta todas las opciones posibles?

La respuesta es 15. En este caso la acción de elegir la capacidad del disco duro (acción A) puede realizarse de 3 formas diferentes, y la acción de optar por la memoria RAM (acción B) puede realizarse de 5 maneras distintas. La acción de elegir el tamaño del disco duro es independiente de la acción de elegir la memoria RAM (estamos suponiendo que nuestra placa madre soporta todas las posibilidades). De acuerdo al principio de la multiplicación la cantidad de formas en que podemos armar nuestra computadora (acción A y B) es $3 \cdot 5 = 15$.

El principio de multiplicación escrito en forma general puede ser expresado como:

Principio de multiplicación I: Sean $A_1, \ldots, A_n$ conjuntos finitos. Entonces:

$$|A_1 \times \ldots \times A_n| = |A_1| \cdot \ldots \cdot |A_n|\,.$$

Principio de multiplicación II: Si acciones $A_1, \ldots, A_n$ se pueden realizar de $m_1, \ldots, m_n$ formas distintas respectivamente, siendo $A_1, \ldots A_n$ acciones independientes, entonces la cantidad de formas posibles de realizar las acciones A_1 y A_2 y $\ldots$ y A_n es $m_1 \cdot \ldots \cdot m_n$.

5.8.4. Principio del complemento

El principio del complemento en términos de conjuntos se expresa en el siguiente teorema.

Teorema 5.7 (Principio del complemento I)
Sea A un subconjunto de un universal $\mathcal{U}$ donde $|\mathcal{U}| = n$. Entonces $|A| = n - |A^c|$.

Demostración.
Recordemos que $A \cup A^c = \mathcal{U}$. Como A y A^c son conjuntos disjuntos, el principio de adición nos dice que:

$$\begin{aligned} n &= |\mathcal{U}| \\ &= |A \cup A^c| \\ &= |A| + |A^c| \end{aligned}$$

Por lo tanto, $|A| = n - |A^c|$. ■

El principio del complemento, aplicado a técnicas de conteo, puede expresarse de la siguiente manera:

> **Principio del complemento II:** Supongamos que hay n formas de realizar una determinada acción A y, de éstas, hay exactamente k que no cumplen con una propiedad P dada. Entonces, la cantidad de formas de realizar la acción A cumpliendo con la propiedad P es $n - k$.

Ejemplo 5.12

(a) Sean los conjuntos $A = \{1, 2, 3, 4, 5, 6\}$ y $B = \{1, 2, 3, 4, 5, 6\}$. ¿Cuántos elementos del conjunto $A \times B$ poseen componentes distintas?

La respuesta es 30. Podríamos definir el conjunto $C \subset A \times B$ cuyos elementos tienen componentes distintas. Luego C^c es un subconjunto de $A \times B$ cuyos elementos poseen componentes iguales. Es fácil deducir que C^c posee 6 elementos, pues:

$$C^c = \{(1,1), (2,2), (3,3), (4,4), (5,5), (6,6)\}.$$

Por otro lado, por el principio de la multiplicación se tiene que $|A \times B| = |A| \cdot |B| = 6 \cdot 6 = 36$. Por el principio del complemento obtenemos que: $|C| = |A \times B| - |C^c| = 36 - 6 = 30$.

(b) Queremos comprarnos una computadora con ciertas características de espacio en disco y memoria RAM. Para las opciones de disco duro tenemos que elegir entre 1 TB, 2 TB y 4 TB. Para la memoria RAM podemos optar entre 4 GB, 8 GB, 16 GB, 32 GB y 64 GB. ¿De cuántas formas podemos armar nuestra computadora si nuestra placa madre soporta todas las opciones posibles salvo que no soporta discos duros de 4 TB ni memoria RAM de 64 GB?

La respuesta es 8. La acción A de elegir una computadora puede realizarse de 15 formas diferentes (ver Ejemplo 5.11-(b)). Definimos la propiedad P como aquellas elecciones de disco duro y memoria RAM que satisfacen los requerimientos de nuestra placa madre. Aquellas posibles acciones que no cumplen la propiedad P son exactamente 7, a saber:

Disco duro (TB)	Memoria RAM (GB)
4	4
4	8
4	16
4	32
4	64
1	64
2	64

De acuerdo al principio del complemento, la cantidad de formas de elegir nuestra computadora adecuada a la placa madre es $15 - 7 = 8$.

5.8.5. Principio de inyección

Teorema 5.8 (Principio de inyección)
Sean A y B conjuntos finitos y $f : A \to B$ una función inyectiva. Entonces $|A| \leqslant |B|$.

Demostración.
Supongamos que A posee m elementos y B posee n elementos:

$$\begin{aligned} A &= \{a_1, a_2, \ldots, a_m\}, \\ B &= \{b_1, b_2, \ldots, b_n\}. \end{aligned}$$

Como f es inyectiva, entonces los elementos $f(a_1), \ldots, f(a_m)$ son todos distintos. Pero esto significa que B tiene al menos m elementos. Por lo tanto $m \leqslant n$, o sea, $|A| \leqslant |B|$. ■

El enunciado del principio de inyección utilizando la contrarrecíproca quedaría expresado de la siguiente manera:

> **Principio de inyección:** Sean A y B conjuntos finitos. Si $|A| > |B|$, entonces no existe ninguna función $f : A \to B$ que sea inyectiva.

5.8.6. Principio de biyección

Teorema 5.9 (Principio de biyección)
Sean A y B conjuntos finitos y $f : A \to B$ una función biyectiva. Entonces $|A| = |B|$.

Demostración.
Como f es biyectiva, en particular es inyectiva. Por el principio de inyección (Teorema 5.8) obtenemos que $|A| \leqslant |B|$.
Análogamente, como f^{-1} es biyectiva, en particular es inyectiva. Por el principio de inyección (Teorema 5.8) obtenemos que $|B| \leqslant |A|$.
Por lo tanto $|A| = |B|$. ■

El enunciado del principio de biyección utilizando la contrarrecíproca quedaría expresado de la siguiente manera:

> **Principio de biyección:** Sean A y B conjuntos finitos. Si $|A| \neq |B|$, entonces no existe ninguna función $f : A \to B$ que sea biyectiva.

Existe un resultado de caracterización de las funciones biyectivas cuando el dominio y el conjunto de llegada coinciden.

Corolario 5.4
Sea A un conjunto finito y $f : A \to A$. Entonces f es inyectiva si y sólo si f es sobreyectiva.

Demostración.
Como $\mathrm{Im}(f) \subset A$ se tiene que $|\mathrm{Im}(f)| \leqslant |A|$.
Definimos $\tilde{f} : A \to \mathrm{Im}(f)$ definida como $\tilde{f}(x) = f(x)$ para todo $x \in A$ (notar que lo único que hemos modificado de la función f ha sido el conjunto de llegada).
Si ocurriese que f es inyectiva, entonces $\tilde{f}$ también lo es. Por el principio de inyección tenemos que $|A| \leqslant |\mathrm{Im}(f)|$, lo cual significa que $|A| = |\mathrm{Im}(f)|$. En definitiva, $\mathrm{Im}(f) = A$. Por lo tanto que tenemos que f es sobreyectiva.

Por otro lado, ahora supongamos que f es sobreyectiva. Si $A = \{a_1, \ldots, a_n\}$, el hecho de que f sea sobreyectiva significa que

$$\forall k = 1, \ldots n, \exists b_k \in A : a_k = f(b_k).$$

Para ver que f es inyectiva, basta chequear que todos los $b_1, \ldots, b_n$ son distintos. Para ello supongamos que existen índices $k \neq l$ tales que $b_k = b_l$. Esto nos dice que

$$a_k = f(b_k) = f(b_l) = a_l,$$

lo cual es una contradicción. ■

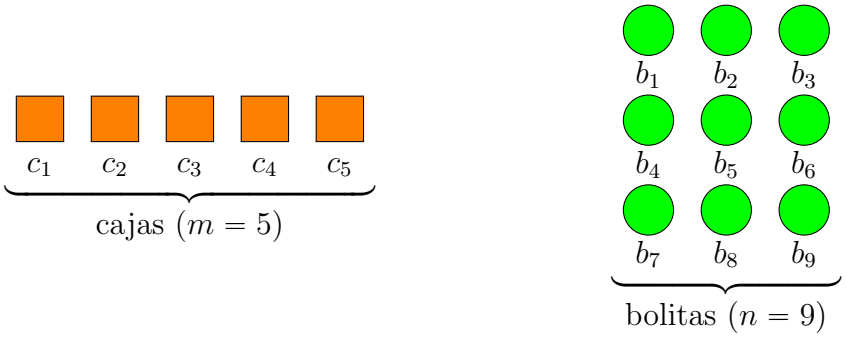
5.8.7. Variaciones simples

Imaginemos que tenemos n bolitas (enumeradas como $b_1, b_2, \ldots, b_n$) y m cajas (enumeradas como $c_1, c_2, \ldots, c_m$) donde deseamos guardar nuestras bolitas.

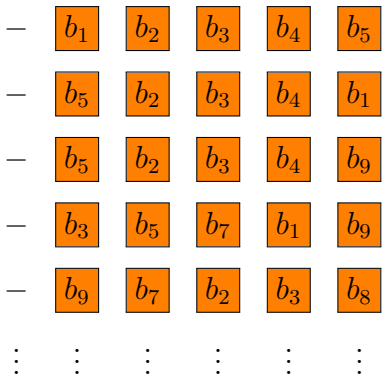
Supondremos que:

- la cantidad de cajas es menor o igual a la cantidad de bolitas: $m \leqslant n$.
- importa el orden de colocación.
- cada bolita debe ir ubicada en solamente una caja (o sea, no se puede repetir la elección de la bolita).
- debemos ocupar todas las cajas (esto siempre es posible pues $m \leqslant n$).

Gráficamente:



Algunas formas de ordenar podrían ser:



Definición 5.9 (Variación simple de n elementos de orden m)
Sean $m, n \in \mathbb{N}$ tal que $m \leqslant n$. Una variación simple de n elementos de orden m es una forma de ubicar n objetos en m lugares de modo que no haya repeticiones e importe el orden de colocación. La cantidad de variaciones simples de n elementos de orden m se denota por $V_{n,m}$.

Teorema 5.10
Sean $m, n \in \mathbb{N}$ tal que $m \leqslant n$. La cantidad de variaciones simples de n elementos de orden m es igual a:

$$V_{n,m} = \frac{n!}{(n-m)!}.$$

Demostración.

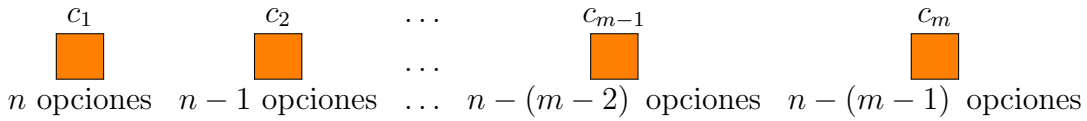
Notemos que ubicar la primera bolita en la primer caja nos da un total de n opciones (una por cada bolita).

Ubicar la segunda bolita en la segunda caja nos da un total de $n-1$ opciones (pues ya ubicamos la primer bolita y no hay repeticiones).

Ubicar la tercer bolita en la tercer caja nos da un total de $n-2$ opciones (pues ya ubicamos la primer y segunda bolita, y no hay repeticiones).

Siguiendo este procedimiento, nos encontramos que ubicar una bolita en la última caja desocupada nos da un total de $n-m+1$ opciones (pues ya ubicamos $m-1$ bolitas antes).

Gráficamente tendríamos:

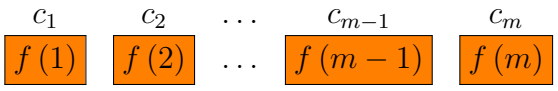


Por el principio de multiplicación tenemos que

$$\begin{aligned} V_{n,m} &= n \cdot (n-1) \cdot \ldots \cdot [n-(m-2)] \cdot [n-(m-1)] \\ &= n \cdot (n-1) \cdot \ldots \cdot (n-m+1) \\ &= \frac{n!}{(n-m)!}. \end{aligned}$$

■

Otra forma de ver las variaciones simples es mediante una función f que asigne a cada índice de cada caja el índice de la bolita a ubicar. Gráficamente:



donde $f : [\![1, m]\!] \to [\![1, n]\!]$.

Como no hay repeticiones, entonces la función f resulta inyectiva. Luego puede tenerse la siguiente definición equivalente.

> **Variación simple:** Una variación simple de n elementos de orden m (con $m, n \in \mathbb{N}$ y $m \leqslant n$) es una función inyectiva $f : [\![1, m]\!] \to [\![1, n]\!]$.

Notemos que si $m > n$, el principio de inyección afirma que no hay ninguna función inyectiva $f : [\![1, m]\!] \to [\![1, n]\!]$. De allí el requerimiento de que $m \leqslant n$.

A continuación podemos ver una demostración alternativa por inducción del Teorema 5.10.

Teorema 5.11
Sean $m, n \in \mathbb{N}$ tal que $m \leqslant n$. La cantidad de variaciones simples de n elementos de orden m, denotada por $V_{n,m}$, es igual a:

$$V_{n,m} = \frac{n!}{(n-m)!}.$$

Demostración.

Haremos la demostración por inducción en m. Sea la siguiente función proposicional definida en $\mathbb{N}$:

$$P(m): \quad V_{n,m} = \frac{n!}{(n-m)!}.$$

Observemos que $P(1)$ es V. Si consideramos una función inyectiva $f : \{1\} \to [\![1, n]\!]$, entonces $f(1)$ tiene n posibilidades, es decir, $V_{n,1} = n$. Además

$$\frac{n!}{(n-1)!} = n.$$

Asumamos ahora que $P(m)$ es V.

Veamos que $P(m+1)$ es V. Consideremos una función inyectiva $f : [\![1, m+1]\!] \to [\![1, n]\!]$ cualquiera. La función f mapea $[\![1, m]\!]$ a un conjunto de m elementos distintos de $[\![1, n]\!]$ (o sea f restringida a $[\![1, m]\!]$ es una variación simple de n elementos de orden m). De esta manera, $f(m+1)$ puede ser cualquiera de los $n - m$ elementos restantes de $[\![1, n]\!]$. Por lo tanto por cada función inyectiva de $[\![1, m]\!]$ en $[\![1, n]\!]$ hay $n - m$ funciones inyectivas de $[\![1, m+1]\!]$ en $[\![1, n]\!]$. Esto significa que:

$$V_{n,m+1} = V_{n,m} \cdot (n-m) = \frac{n!}{(n-m)!} \cdot (n-m) = \frac{n!}{(n-m-1)!} = \frac{n!}{[n-(m+1)]!}.$$

Luego la proposición $\forall n \in \mathbb{N}, P(n)$ es V debido al Criterio 5.1. ■

Ejemplo 5.13

(a) ¿Cuántos números de tres cifras distintas pueden formarse con 1, 2, 3 y 4?

Representemos un número de tres cifras:

$$\boxed{f(1)} \quad \boxed{f(2)} \quad \boxed{f(3)}$$

En el casillero de la izquierda pueden ir los números 1, 2, 3 o 4. En el casillero central, pueden ir nuevamente los cuatro números pero no se puede repetir, con lo cual nos quedan tres opciones. Análogamente, el casillero de la derecha puede contener a los cuatro números pero no se puede repetir ni con el del primer casillero ni con el del casillero central, con lo cual quedan dos opciones.

Esto indica que cada número de tres cifras distintas se corresponde con una función inyectiva $f : [\![1, 3]\!] \to [\![1, 4]\!]$. Luego la respuesta a nuestro problema es:

$$V_{4,3} = \frac{4!}{(4-3)!} = 4 \cdot 3 \cdot 2 = 24.$$

Para comprobar este cálculo, escribimos la lista completa de posibilidades

123	124	132	134	142	143	213	214	231	234	241	243
312	314	321	324	341	342	412	413	421	423	431	432

(b) ¿Cuántas banderas distintas se pueden hacer de 3 bandas verticales con los colores rojo, blanco, azul, verde y amarillo, si no puede haber dos bandas del mismo color?

Representemos una bandera de tres bandas verticales:

$$\boxed{f(1)} \quad \boxed{f(2)} \quad \boxed{f(3)}$$

donde f representa una función

$$f : \{1, 2, 3\} \to \{\text{rojo},\ \text{blanco},\ \text{azul},\ \text{verde},\ \text{amarillo}\}\,.$$

El dominio de f representa las posiciones de las bandas verticales, y el conjunto de llegada son los colores posibles de las bandas de la bandera.

Como se pide que no puede haber dos bandas del mismo color, entonces cada elección de bandera se corresponde con una función inyectiva $f : [\![1, 3]\!] \to [\![1, 5]\!]$ (pues hay 3 bandas disponibles y 5 opciones de colores). Luego la respuesta a nuestro problema es:

$$V_{5,3} = \frac{5!}{(5-3)!} = 5 \cdot 4 \cdot 3 = 60.$$

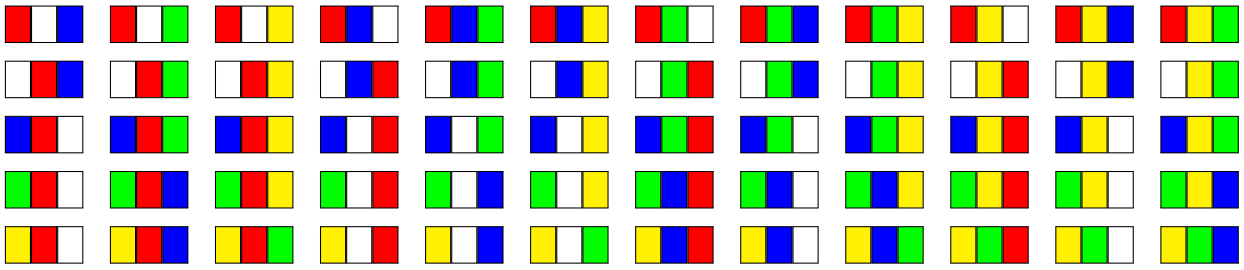
Para comprobar este cálculo, las posibilidades son:

123	124	125	132	134	135	142	143	145	152	153	154
213	214	215	231	234	235	241	243	245	251	253	254
312	314	315	321	324	325	341	342	345	351	352	354
412	413	415	421	423	425	431	432	435	451	452	453
512	513	514	521	523	524	531	532	534	541	542	543

Traduciendo a colores, es decir, identificando

- 1: rojo
- 2: blanco
- 3: azul
- 4: verde
- 5: amarillo

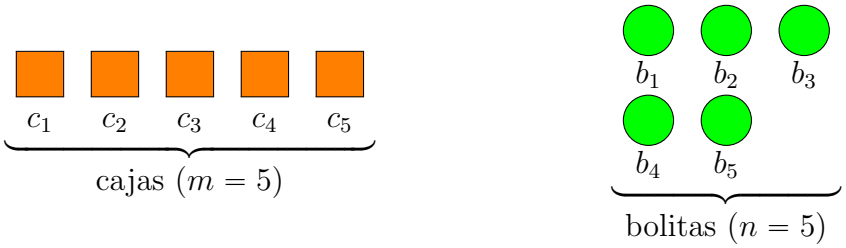
quedaría:



5.8.8. Permutaciones simples

Definición 5.10 (Permutación simple de m elementos)
Sean $m \in \mathbb{N}$. Una permutación simple de m elementos es una variación simple de m elementos de orden m. La cantidad de permutaciones simples de m elementos se denota por P_m.

Es decir, las permutaciones simples son un caso particular de variaciones simples, considerando que el número de cajas coincide con el número de bolitas a ubicar ($m = n$). Cabe recordar que al igual que en las variaciones simples, en una permutación simple importa el orden de colocación y no se puede repetir. Gráficamente:



Teorema 5.12
Sea $m \in \mathbb{N}$. La cantidad de permutaciones simples de m elementos, denotada por P_m, es igual a:

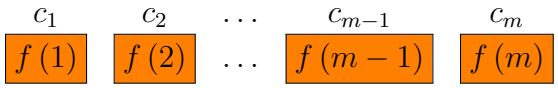
$$P_m = m!.$$

Demostración.
Por la definición de permutación simple tenemos que:

$$P_m = V_{m,m} = \frac{m!}{(m-m)!} = \frac{m!}{0!} = m!,$$

lo cual concluye la prueba. ■

Otra forma de ver las permutaciones simples es mediante una función f que asigne a cada índice de cada caja el índice de la bolita a ubicar. Gráficamente:



donde $f : [\![1, m]\!] \to [\![1, m]\!]$.

Como no hay repeticiones, entonces la función f resulta inyectiva. Por el Corolario 5.4 el hecho que f sea inyectiva equivale a que f sea biyectiva.

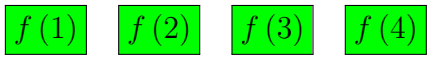
Luego puede tenerse la siguiente definición equivalente.

> **Permutación simple:** Una permutación simple de m elementos (con $m \in \mathbb{N}$) es una función biyectiva $f : [\![1, m]\!] \to [\![1, m]\!]$.

Ejemplo 5.14

(a) ¿Cuántos números de 4 cifras distintas pueden formarse con los números 6, 7, 8 y 9?

Representemos un número de cuatro cifras:



donde f representa una función

$$f : \{1, 2, 3, 4\} \to \{6, 7, 8, 9\}.$$

El dominio de f representa las posiciones de las cifras, y el conjunto de llegada son los números posibles con los que puedo formar el número de cuatro cifras.

Como se pide que las cifras sean distintas, entonces cada elección de número se corresponde con una función inyectiva $f : [\![1, 4]\!] \to [\![1, 4]\!]$ (pues hay 4 posiciones y 4 números disponibles). Luego la respuesta a nuestro problema es:

$$P_4 = 4! = 24.$$

Para comprobar este cálculo, las posibilidades son:

1234	1243	1324	1342	1423	1432
2134	2143	2314	2341	2413	2431
3124	3142	3214	3241	3412	3421
4123	4132	4213	4231	4312	4321

Traduciendo a los números, es decir, identificando

- 1: 6
- 2: 7
- 3: 8
- 4: 9

quedaría:

6789	6798	6879	6897	6978	6987
7689	7698	7869	7896	7968	7986
8679	8697	8769	8796	8967	8976
9678	9687	9768	9786	9867	9876

(b) Con las letras de la palabra "aro", ¿cuántas palabras de 3 letras distintas pueden formarse? (las palabras pueden tener sentido o no).

Representemos una palabra de tres letras:

$$\boxed{f\,(1)} \quad \boxed{f\,(2)} \quad \boxed{f\,(3)}$$

donde f representa una función

$$f : \{1, 2, 3\} \to \{\mathrm{a},\ \mathrm{r},\ \mathrm{o}\}\,.$$

El dominio de f representa las posiciones de las letras, y el conjunto de llegada son las letras posibles con las que puedo formar la palabra de tres letras.

Como se pide que las letras sean distintas, entonces cada elección de palabra se corresponde con una función inyectiva $f : [\![1, 3]\!] \to [\![1, 3]\!]$ (pues hay 3 posiciones y 3 letras disponibles). Luego la respuesta a nuestro problema es:

$$P_3 = 3! = 6.$$

Para comprobar este cálculo, las posibilidades son:

123	132	213	231	312	321

Traduciendo a palabras, es decir, identificando

- 1: a
- 2: r
- 3: o

quedaría:

aro	aor	rao	roa	oar	ora

(c) En un colectivo hay 8 butacas y suben 8 pasajeros. ¿De cuántas formas diferentes pueden sentarse tales pasajeros?

Como los pasajeros no pueden sentarse en dos lugares a la vez, la respuesta es el número de permutaciones de 8 elementos, es decir:

$$P_8 = 8! = 8 \cdot 7 \cdot \ldots \cdot 1 = 40320.$$

5.8.9. Combinaciones simples

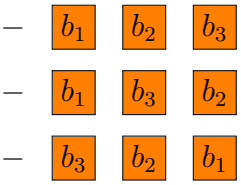
Imaginemos que tenemos n bolitas (enumeradas como $b_1, b_2, \ldots, b_n$) y m cajas (enumeradas como $c_1, c_2, \ldots, c_m$) donde deseamos guardar nuestras bolitas.

Supondremos que:

- la cantidad de cajas es menor o igual a la cantidad de bolitas: $m \leqslant n$.
- NO importa el orden de colocación.
- cada bolita debe ir ubicada en solamente una caja (o sea, no se puede repetir la elección de la bolita).
- debemos ocupar todas las cajas (esto siempre es posible pues $m \leqslant n$).

Gráficamente tendríamos una situación similar al caso de las variaciones simples

Sin embargo, algunas formas de ordenar podrían coincidir. Por ejemplo:

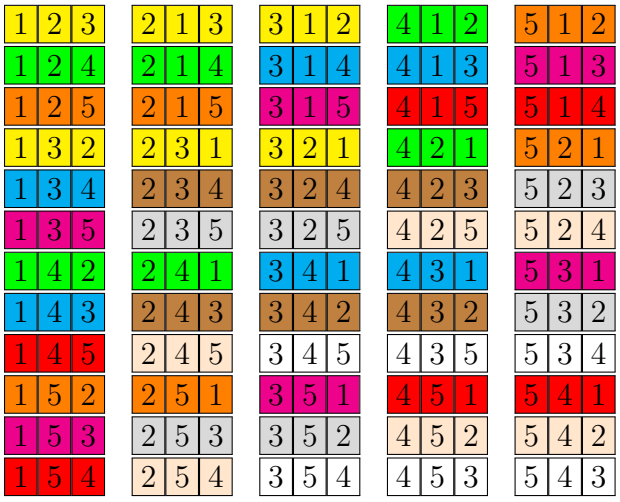


serían algunas elecciones equivalentes dado que NO importa el orden de colocación.

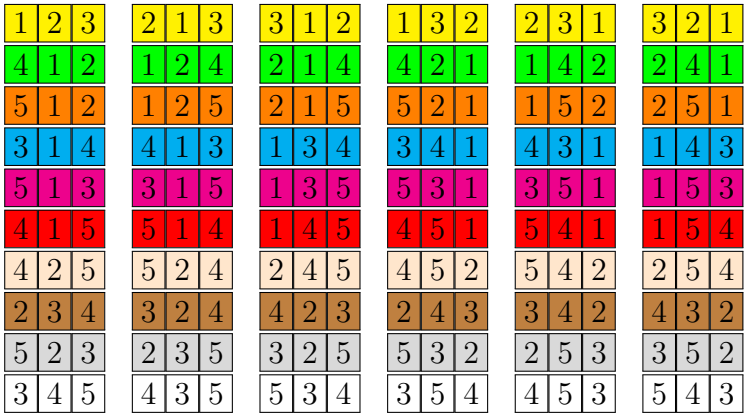
Definición 5.11 (Combinación simple de n elementos de orden m)
Sean $m, n \in \mathbb{N}$ tal que $m \leqslant n$. Una combinación simple de n elementos de orden m es una forma de ubicar n objetos en m lugares de modo que no haya repeticiones y no importe el orden de colocación. La cantidad de combinaciones simples de n elementos de orden m se denota por $C_{n,m}$.

De acuerdo a la definición de combinación simple, al no importar el orden, una combinación simple puede verse como un subconjunto de m elementos tomados de un conjunto de n elementos.

Continuemos con nuestro ejemplo inicial. Si asumiéramos por un momento que importa el orden de colocación, procederíamos como si fuera una variación simple de 5 elementos de orden 3. Si construyéramos la lista completa de posibilidades quedaría algo así (colocando sólo los índices de las bolitas para facilitar la lectura), coloreando aquellas elecciones equivalentes,



Clasificando por colores las mismas posibilidades reordenadas de otra manera serían:



Notemos que si tomáramos un representante de cada color estaríamos cumplimentando los requerimientos solicitados anteriormente, y entonces la cantidad de combinaciones simples sería 10.

Otra forma de ver a una combinación simple de n elementos de orden m es mediante funciones inyectivas $f : [\![1, m]\!] \to [\![1, n]\!]$ (como en el caso de las variaciones) pero que posean la misma imagen (que posean igual color como en el ejemplo). De acuerdo a esto, estamos frente a una relación de equivalencia.

Sean $m, n \in \mathbb{N}$ tales que $m \leqslant n$. Consideremos la siguiente relación en el conjunto de todas las funciones inyectivas de $[\![1, m]\!]$ en $[\![1, n]\!]$:

$$f \sim g \Leftrightarrow \operatorname{Im}(f) = \operatorname{Im}(g). \tag{9}$$

Claramente $\sim$ es relación de equivalencia.

Observación 5.1
La relación $\sim$ es de equivalencia.

Demostración.

Tenemos que comprobar que la relación es reflexiva, simétrica y transitiva.

(a) $\sim$ es reflexiva:

Como $\operatorname{Im}(f) = \operatorname{Im}(f)$ esto dice que $f \sim f$, por lo que $\sim$ resulta reflexiva.

(b) $\sim$ es simétrica:

$$f \sim g \Rightarrow \operatorname{Im}(f) = \operatorname{Im}(g) \Rightarrow \operatorname{Im}(g) = \operatorname{Im}(f) \Rightarrow g \sim f.$$

(c) $\sim$ es transitiva:

$$\left.\begin{array}{rcl} f \sim g & \Rightarrow & \mathrm{Im}\,(f) = \mathrm{Im}\,(g) \\ g \sim h & \Rightarrow & \mathrm{Im}\,(g) = \mathrm{Im}\,(h) \end{array}\right\} \Rightarrow \mathrm{Im}\,(f) = \mathrm{Im}\,(h) \Rightarrow f \sim h.$$

Esto concluye la prueba. ■

En la Proposición 2.2 se explicó que una relación de equivalencia sobre un conjunto define una partición sobre tal conjunto en clases de equivalencia. Cada una de estas clases de equivalencia está representada por una función inyectiva $f : [\![1, m]\!] \to [\![1, n]\!]$ y esta función está relacionada a todas aquellas funciones inyectivas con la misma imagen. Por lo tanto, la cantidad de elementos en cada clase de equivalencia es el número de permutaciones de m elementos (la cantidad de elementos de la imagen).

Pensando en funciones, podemos definir una combinación simple de la siguiente manera.

> **Combinación simple:** Una combinación simple de n elementos de orden m ($m, n \in \mathbb{N}$ con $m \leqslant n$) es un representante de la partición que induce la relación de equivalencia (9) sobre el conjunto de las funciones inyectivas $f : [\![1, m]\!] \to [\![1, n]\!]$.

La relación de equivalencia (9) manifiesta el hecho que no importa el orden en el cual están los elementos de la imagen. En otras palabras, la cantidad de clases de equivalencia corresponde a la cantidad de subconjuntos de m elementos que pueden extraerse de un conjunto de n elementos.

Teorema 5.13
Sean $m, n \in \mathbb{N}$ con $m \leqslant n$. La cantidad de clases de equivalencia de la relación (9) *definida sobre las funciones inyectivas de $[\![1, m]\!]$ en $[\![1, n]\!]$, denotada por $C_{n,m}$, es igual a:*

$$C_{n,m} = \binom{n}{m} = \frac{n!}{m! \cdot (n-m)!}.$$

Demostración.
Por lo explicado más arriba, se tiene que:

$$C_{n,m} = \frac{\text{cantidad de funciones inyectivas de } [\![1, m]\!] \text{ en } [\![1, n]\!]}{\text{cantidad de elementos en cada clase de equivalencia}} = \frac{V_{n,m}}{P_m} = \frac{n!}{m! \cdot (n-m)!},$$

lo cual concluye la prueba. ■

Ejemplo 5.15

(a) ¿Cuántos subconjuntos de 3 elementos del conjunto $\{1, 2, 3, 4, 5\}$ existen?

La respuesta a nuestro problema es:

$$C_{5,3} = \binom{5}{3} = \frac{5!}{3! \cdot (5-3)!} = \frac{5!}{6 \cdot 2} = \frac{120}{12} = 10.$$

Para chequear el resultado, hagamos la lista de los subconjuntos de 3 elementos:

$$\begin{array}{lllll} \{1,2,3\} & \{1,2,4\} & \{1,2,5\} & \{1,3,4\} & \{1,3,5\} \\ \{1,4,5\} & \{2,3,4\} & \{2,3,5\} & \{2,4,5\} & \{3,4,5\} \end{array}$$

(b) Considerando que para formar un equipo de fútbol se necesitan 11 jugadores, ¿cuántos equipos posibles se pueden formar con 18 jugadores?

La respuesta a nuestro problema es:

$$C_{18,11} = \binom{18}{11} = \frac{18!}{11! \cdot (18-11)!} = 31824.$$

5.8.10. Variaciones con repetición

Imaginemos que tenemos n bolitas (enumeradas como $b_1, b_2, \ldots, b_n$) y m cajas (enumeradas como $c_1, c_2, \ldots, c_m$) donde deseamos guardar nuestras bolitas.

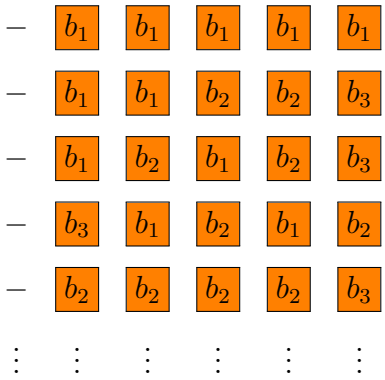
Supondremos que:

- importa el orden de colocación.
- en cada caja cabe solamente una bolita.
- una bolita podría estar asignada a más de una caja (es decir, ¡se puede repetir!).
- debemos ocupar todas las cajas (esto siempre es posible pues puedo repetir la elección de la bolita).

Notar que debido a la posibilidad de repetir, ya no es necesaria la restricción $m \leqslant n$.

Gráficamente:

Algunas formas de ordenar podrían ser:



Definición 5.12 (Variación con repetición de n elementos de orden m)
Sean $m, n \in \mathbb{N}$. Una variación con repetición de n elementos de orden m es una forma de ubicar n objetos en m lugares de modo que importe el orden de colocación. Es posible asignar un objeto a uno o más lugares. La cantidad de variaciones con repetición de n elementos de orden m se denota por $V'_{n,m}$.

Teorema 5.14
Sean $m, n \in \mathbb{N}$. La cantidad de variaciones con repetición de n elementos de orden m es igual a:

$$V'_{n,m} = n^m.$$

Demostración.

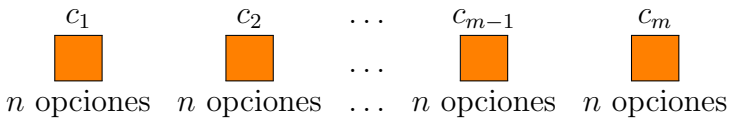
Notemos que ubicar la primera bolita en la primer caja nos da un total de n opciones (una por cada bolita).

Ubicar la segunda bolita en la segunda caja nos da un total de n opciones también (pues ya ubicamos la primer bolita y se puede repetir).

Ubicar la tercer bolita en la tercer caja nos da un total de n opciones (pues ya ubicamos la primer y segunda bolita, y se puede repeticiones).

Siguiendo este procedimiento, nos encontramos que ubicar una bolita en la última caja desocupada nos da también un total de n opciones.

Gráficamente tendríamos:

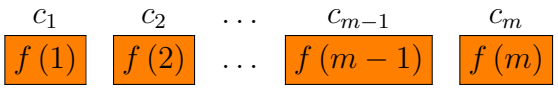


Por el principio de multiplicación tenemos que

$$\begin{aligned} V'_{n,m} &= n \cdot n \cdot \ldots \cdot n \cdot n \\ &= n^m. \end{aligned}$$

■

Otra forma de ver las variaciones con repetición es mediante una función f que asigne a cada índice de cada caja el índice de la bolita a ubicar. Gráficamente:



donde $f : [\![1, m]\!] \to [\![1, n]\!]$.

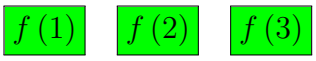
Como se puede repetir, entonces la función f no posee ninguna cualidad especial. Luego puede tenerse la siguiente definición equivalente.

Variación con repetición: Una variación con repetición de n elementos de orden m (con $m, n \in \mathbb{N}$) es una función $f : [\![1, m]\!] \to [\![1, n]\!]$.

Ejemplo 5.16

(a) ¿Cuántos números de 3 cifras pueden formarse con 1, 2, 3, 4?

Representemos un número de tres cifras:



Esto indica que cada número de tres cifras se corresponde con una función $f : [\![1, 3]\!] \to [\![1, 4]\!]$ (o bien a un elemento de $[\![1, 4]\!] \times [\![1, 4]\!] \times [\![1, 4]\!]$). Luego la respuesta a nuestro problema es:

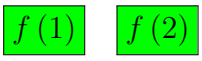
$$V'_{4,3} = 4^3 = 64.$$

Para corroborar este resultado, realicemos la lista de los posibles números que podemos formar:

111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144
211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244
311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344
411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444

(b) ¿Cuántas palabras de 2 letras pueden formarse con las letras a, b y c?

Representemos una palabra de dos letras:



Esto indica que cada palabra de dos letras se corresponde con una función $f : [\![1, 2]\!] \to [\![1, 3]\!]$ (o bien a un elemento de $[\![1, 3]\!] \times [\![1, 3]\!]$). Luego la respuesta a nuestro problema es:

$$V'_{3,2} = 3^2 = 9.$$

Para corroborar este resultado, realicemos la lista de las posibles palabras que podemos formar:

$$aa \quad ab \quad ac \quad ba \quad bb \quad bc \quad ca \quad cb \quad cc$$

5.8.11. Permutaciones con repetición

Definición 5.13
Supongamos que A es un conjunto de n elementos entre los cuales hay n_i elementos del tipo A_i, $i = 1, \dots m$, siendo $n = n_1 + \dots + n_m$. Los elementos del tipo A_i son distintos de los elementos del tipo A_j para $i \neq j$, sin embargo, los elementos del tipo A_i son indistinguibles entre sí. Una permutación con repetición del conjunto A es un posible reordenamiento de sus elementos (considerando los elementos de cada A_i como idénticos).

Teorema 5.15
Sean $n, n_1, \dots, n_m \in \mathbb{N}$ tales que $n = n_1 + \dots + n_m$. El número de permutaciones con repetición de n elementos entre $n_1, \dots, n_m$ tipos, denotado por $P_n^{n_1,\dots,n_m}$, es igual a:

$$P_n^{n_1,\dots,n_m} = \frac{n!}{n_1! \cdot \dots \cdot n_m!}.$$

Demostración.

Supongamos que tenemos formadas todas las permutaciones con repetición $P_n^{n_1,\dots,n_m}$. Si sustituimos los n_1 elementos iguales por otros distintos y luego los ordenamos de todos los modos posibles conservando en sus puestos los $n - n_1$ restantes, de cada grupo se deducirán $n_1!$ distintos y obtendremos un nuevo conjunto de posibilidades igual a $n_1! \cdot P_n^{n_1,\dots,n_m}$. Si a partir del último conjunto de posibilidades, reemplazamos los n_2 elementos iguales por otros distintos y procedemos de la misma forma, obtendremos un nuevo conjunto de opciones de $n_1! \cdot n_2! \cdot P_n^{n_1,\dots,n_m}$. Si continuamos con este proceso hasta llegar al último grupo de elementos iguales, resultará un total de

$$n_1! \cdot \dots \cdot n_m! \cdot P_n^{n_1,\dots,n_m}$$

opciones que constituyen las permutaciones de n elementos distintos, es decir,

$$n_1! \cdot \dots \cdot n_m! \cdot P_n^{n_1,\dots,n_m} = n!,$$

lo cual implica que

$$P_n^{n_1,\dots,n_m} = \frac{n!}{n_1! \cdot \dots \cdot n_m!},$$

lo cual concluye la prueba. ■

Ejemplo 5.17

(a) ¿Cuántas palabras distintas se pueden formar con las letras de la palabra *banana* alterando el orden de las letras?

Notemos que b aparece una vez, a aparece tres veces y n aparece dos veces.

$$P_6^{1,3,2} = \frac{6!}{1! \cdot 3! \cdot 2!} = 60.$$

Para comprobar este cálculo, las posibilidades son:

banana	banaan	bannaa	baanna	baanan	baaann
bnaana	bnaaan	bnanaa	bnnaaa	banana	abnaan
abnnaa	abanna	abanan	abaann	anbana	anbaan
anbnaa	anabna	anaban	ananba	ananab	anaabn
anaanb	annbaa	annaba	annaab	aabnna	aabnan
aabann	aanbna	aanban	aannba	aannab	aanabn
aananb	aaabnn	aaanbn	aaannb	nbaana	nbaaan
nbanaa	nbnaaa	nabana	nabaan	nabnaa	naabna
naaban	naanba	naanab	naaabn	naaanb	nanbaa
nanaba	nanaab	nnbaaa	nnabaa	nnaaba	nnaaab

(b) ¿Cuántos números distintos de 10 cifras se pueden formar con los dígitos de 1112233345?

Notemos que 1 aparece tres veces, 2 aparece dos veces, 3 aparece tres veces, y 4 y 5 aparecen sólo una vez. Luego la respuesta a nuestro problema es:

$$P_{10}^{3,2,3,1,1} = \frac{10!}{3! \cdot 2! \cdot 3! \cdot 1! \cdot 1!} = 50400.$$

5.8.12. Combinaciones con repetición

Definición 5.14
Sean $m, n \in \mathbb{N}$. Llamamos combinaciones con repetición de orden m definidas en un conjunto con n elementos a los diferentes grupos de m elementos (iguales o distintos) que se pueden construir de n elementos de modo que dos grupos se diferencian en algún elemento y no en el orden de colocación.

Teorema 5.16
Sean $m, n \in \mathbb{N}$. El número de combinaciones con repetición de orden m definidas en un conjunto con n elementos, denotado por $C'_{n,m}$, es igual a:

$$C'_{n,m} = \binom{n-1+m}{m}.$$

Demostración.

Enumeramos los elementos de 1 a n. Una combinación genérica se puede expresar con símbolos de dos clases: cero y uno. Para representar el elemento 1 se escribe un uno seguido de tantos ceros como veces se repita dicho elemento en la combinación considerada. A continuación se escribe otro uno que representa al 2 y se le hace seguir de tantos ceros como veces figure dicho elemento en la citada composición, y así sucesivamente. De esta manera, si faltase algún elemento se expresará dicha circunstancia escribiendo un uno por cada uno de ellos sin ir seguido de ningún cero.

Por ejemplo, la combinación 113 elegida entre los elementos 1, 2, 3 y 4 se escribirá:

1001101

De este modo cada combinación que estamos considerando viene representada por una expresión que comienza con uno y contiene de forma ordenada n veces uno y m veces cero. Recíprocamente toda expresión de este tipo representa una de tales combinaciones.

Consecuentemente, para determinar el número de estas combinaciones lo que haremos es calcular el número de expresiones del tipo $1\ldots$. El primer símbolo es un uno. Si lo dejamos fijo queda por disponer en cualquier orden los $n-1$ unos restantes y los m ceros, lo cual puede hacerse de $P_{n-1+m}^{n-1,m}$ formas distintas. Por lo tanto,

$$C'_{n,m} = \frac{(n-1+m)!}{(n-1)! \cdot m!} = \binom{n-1+m}{m},$$

lo cual concluye la prueba. ■

Ejemplo 5.18

(a) Se dispone de tres bolsas iguales con caramelos de fresa, de menta y de limón. Cada una de las bolsas contiene, al menos, diez caramelos. ¿De cuántas formas pueden seleccionarse diez caramelos sin ninguna restricción?

Una de las posibles distribuciones de los diez caramelos es

$$ffmflmmfll$$

donde f, m y l representan los sabores de fresa, menta y limón, respectivamente. Si en esta distribución elegida al azar intercambiamos entre sí uno o varios sabores, la misma no varía. Sin embargo, si cambiamos uno o varios caramelos por otros de distinto sabor, tendremos una distribución diferente. Por lo tanto, las distribuciones de los diez caramelos son combinaciones con repetición de orden 10 elegidas entre 3 tipos de caramelos distintos. Luego, la respuesta a nuestro problema es:

$$C'_{3,10} = \binom{3-1+10}{10} = \binom{12}{10} = 66.$$

(b) En una bodega hay cinco tipos diferentes de botellas. ¿De cuántas formas se pueden elegir cuatro botellas?

En este caso $n = 5$ y $m = 4$, con lo cual la respuesta es:

$$C'_{5,4} = \binom{5-1+4}{4} = \binom{8}{4} = 70.$$

5.8.13. Identificación de problemas y fórmulas

A manera de resumen, mostramos la siguiente tabla para identificar los tipos de problemas y recordar las fórmulas vistas anteriormente.

		TIPOS	SIN REPETICIÓN	CON REPETICIÓN
¿IMPORTA ORDEN?	SÍ	VARIACIONES	$V_{n,m} = \dfrac{n!}{(n-m)!}$	$V'_{n,m} = n^m$
		PERMUTACIONES	$P_m = m!$	$P_n^{a,b,c} = \dfrac{n!}{a! \cdot b! \cdot c!}$
	NO	COMBINACIONES	$C_{n,m} = \binom{n}{m}$	$C'_{n,m} = \binom{n-1+m}{m}$

5.9. Fórmula del binomio

Dados $a, b \in \mathbb{R}$, nos gustaría encontrar una expresión para $(a+b)^n$ donde $n \in \mathbb{N}$. Podríamos preguntarnos sobre la necesidad de encontrar tal expresión, puesto que podríamos calcular primero la suma, y luego la potencia. Por ejemplo:

$$\begin{aligned} (1+2)^5 &= 3^5 = 243 \\ (5-3)^4 &= 2^4 = 16 \\ (-5+1)^3 &= (-4)^3 = -64 \\ &\vdots \end{aligned}$$

Sin embargo, como se verá mas adelante, podemos utilizar la expresión de $(a+b)^n$ para demostrar otras propiedades.

Para introducirnos a la deducción de la expresión, vamos a intentar escribir las primeras potencias.

- Para $n = 1$ tenemos:

$$(a+b)^1 = a + b.$$

- Para $n = 2$ tenemos:

$$\begin{aligned}(a+b)^2 &= (a+b)\cdot(a+b)\\ &= a^2 + a\cdot b + b\cdot a + b^2\\ &= a^2 + 2\cdot a\cdot b + b^2\end{aligned}$$

- Para $n = 3$ tenemos:

$$\begin{aligned}(a+b)^3 &= (a+b)^2\cdot(a+b)\\ &= \left(a^2 + 2\cdot a\cdot b + b^2\right)\cdot(a+b)\\ &= a^3 + 2\cdot a^2\cdot b + b^2\cdot a + a^2\cdot b + 2\cdot a\cdot b^2 + b^3\\ &= a^3 + 3\cdot a^2\cdot b + 3\cdot a\cdot b^2 + b^3\end{aligned}$$

- Para $n = 4$ tenemos:

$$\begin{aligned}(a+b)^4 &= (a+b)^3\cdot(a+b)\\ &= \left(a^3 + 3\cdot a^2\cdot b + 3\cdot a\cdot b^2 + b^3\right)\cdot(a+b)\\ &= a^4 + 3\cdot a^3\cdot b + 3\cdot a^2\cdot b^2 + b^3\cdot a + a^3\cdot b + 3\cdot a^2\cdot b^2 + 3\cdot a\cdot b^3 + b^4\\ &= a^4 + 4\cdot a^3\cdot b + 6\cdot a^2\cdot b^2 + 4\cdot a\cdot b^3 + b^4\end{aligned}$$

- Para $n = 5$ tenemos:

$$\begin{aligned}(a+b)^5 &= (a+b)^4\cdot(a+b)\\ &= \left(a^4 + 4\cdot a^3\cdot b + 6\cdot a^2\cdot b^2 + 4\cdot a\cdot b^3 + b^4\right)\cdot(a+b)\\ &= a^5 + 4\cdot a^4\cdot b + 6\cdot a^3\cdot b^2 + 4\cdot a^2\cdot b^3 + b^4\cdot a\\ &+ a^4\cdot b + 4\cdot a^3\cdot b^2 + 6\cdot a^2\cdot b^3 + 4\cdot a\cdot b^4 + b^5\\ &= a^5 + 5\cdot a^4\cdot b + 10\cdot a^3\cdot b^2 + 10\cdot a^2\cdot b^3 + 5\cdot a\cdot b^4 + b^5\end{aligned}$$

La pregunta que nos hacemos ahora es cuál debería ser la fórmula para un n arbitrario. Veamos que podríamos deducir de las fórmulas obtenidas anteriormente:

- El primer término es a^n.
- El último término es b^n.
- Cada término intermedio es de la forma $coeficiente\cdot a^i\cdot b^j$ donde $i + j = n$.
- Hay $n + 1$ sumandos.
- Los exponentes de a van decreciendo desde n hasta 1 (de los primeros n términos).
- Los exponentes de b van creciendo desde 1 hasta n (de los últimos n términos).

Hasta aquí la fórmula general parece accesible, sin embargo nos está costando comprender los coeficientes de cada sumando. Pensemos que cada sumando se obtiene de elegir i elementos a y j elementos b (con $i + j = n$). Esto es un problema de permutaciones de n elementos con repetición. Los elementos están divididos en dos clases (los rotulados como a y los rotulados como b). Por lo tanto, cada coeficiente es igual a:

$$P_n^{i,j} = \frac{n!}{i!\cdot j!} = \frac{n!}{(n-j)!\cdot j!} = \binom{n}{j}.$$

Notar también que

$$\binom{n}{j} = \binom{n}{n-i} = \binom{n}{i}.$$

Por lo tanto, pareciera que la expresión que estamos buscando es:

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} \cdot a^{n-i} \cdot b^i,$$

considerando que a y b son no nulos (para que no haya inconsistencias con exponentes iguales a 0). El caso cuando $a = 0$ o $b = 0$ es fácilmente tratable. Para terminar de convencernos, vamos a demostrar la fórmula de arriba utilizando un procedimiento por inducción.

Teorema 5.17
Sean a y b números reales no nulos y $n \in \mathbb{N}$. Entonces:

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

Demostración.

Vamos a demostrar el teorema por inducción en n. Definimos la siguiente función proposicional sobre $\mathbb{N}$:

$$P(n): \quad (a+b)^n = \sum_{i=0}^{n} \binom{n}{i} \cdot a^{n-i} \cdot b^i.$$

Observemos que $P(1)$ es V, pues

$$\begin{aligned}
\sum_{i=0}^{1} \binom{1}{i} \cdot a^{1-i} \cdot b^i &= \binom{1}{0} \cdot a^{1-0} \cdot b^0 + \binom{1}{1} \cdot a^{1-1} \cdot b^1 \\
&= 1 \cdot a^{1-0} \cdot b^0 + 1 \cdot a^{1-1} \cdot b^1 \text{ por Teorema 5.4-(a) y 5.4-(b)} \\
&= a^1 \cdot b^0 + a^0 \cdot b^1 \\
&= a \cdot 1 + 1 \cdot b \text{ por Definición 5.4} \\
&= a + b
\end{aligned}$$

Asumamos ahora que $P(n)$ es V. Veamos que $P(n+1)$ es V.

$$\begin{aligned}
(a+b)^{n+1} &= (a+b) \cdot (a+b)^n \text{ por Definición 5.4} \\
&= (a+b) \cdot \sum_{i=0}^{n} \binom{n}{i} \cdot a^{n-i} \cdot b^i \text{ pues estamos asumiendo que } P(n) \text{ es } V \\
&= a \cdot \sum_{i=0}^{n} \binom{n}{i} \cdot a^{n-i} \cdot b^i + b \cdot \sum_{i=0}^{n} \binom{n}{i} \cdot a^{n-i} \cdot b^i \text{ por distributividad} \\
&= \sum_{i=0}^{n} \binom{n}{i} \cdot a^{n-i+1} \cdot b^i + \sum_{i=0}^{n} \binom{n}{i} \cdot a^{n-i} \cdot b^{i+1} \text{ por distributividad} \\
&= \binom{n}{0} \cdot a^{n-0+1} \cdot b^0 + \sum_{i=1}^{n} \binom{n}{i} \cdot a^{n-i+1} \cdot b^i + \text{ separando el primer término} \\
&+ \sum_{i=0}^{n-1} \binom{n}{i} \cdot a^{n-i} \cdot b^{i+1} + \binom{n}{n} \cdot a^{n-n} \cdot b^{n+1} \text{ separando el último término} \\
&= a^{n+1} + \sum_{i=1}^{n} \binom{n}{i} \cdot a^{n-i+1} \cdot b^i + \sum_{i=0}^{n-1} \binom{n}{i} \cdot a^{n-i} \cdot b^{i+1} + b^{n+1}
\end{aligned}$$

$$
\begin{aligned}
&= a^{n+1} + \sum_{i=1}^{n} \binom{n}{i} \cdot a^{n-i+1} \cdot b^i + \sum_{i=1}^{n} \binom{n}{i-1} \cdot a^{n-i+1} \cdot b^i + b^{n+1} \text{ corriendo índices} \\
&= a^{n+1} + \sum_{i=1}^{n} \left[\binom{n}{i} + \binom{n}{i-1} \right] \cdot a^{n-i+1} \cdot b^i + b^{n+1} \\
&= a^{n+1} + \sum_{i=1}^{n} \binom{n+1}{i} \cdot a^{n-i+1} \cdot b^i + b^{n+1} \text{ por Teorema 5.4-(e)} \\
&= a^{n+1} + \sum_{i=1}^{n} \binom{n+1}{i} \cdot a^{n+1-i} \cdot b^i + b^{n+1} \\
&= \binom{n+1}{0} \cdot a^{n+1-0} \cdot b^0 + \sum_{i=1}^{n} \binom{n+1}{i} \cdot a^{n+1-i} \cdot b^i \text{ por Teorema 5.4-(a)} \\
&+ \binom{n+1}{n+1} a^{n+1-n-1} b^{n+1} \text{ por Teorema 5.4-(d)} \\
&= \sum_{i=0}^{n+1} \binom{n+1}{i} \cdot a^{n+1-i} \cdot b^i
\end{aligned}
$$

Luego, la proposición $\forall n \in \mathbb{N}, P(n)$ es V debido al Criterio 5.1. ■

Nos podríamos preguntar cómo encontrar de manera eficiente los coeficientes que aparecen en el desarrollo del binomio (es decir, los números combinatorios). La respuesta a este interrogante la da el conocido Triángulo de Pascal. La primera representación explícita de un triángulo con coeficientes binomiales data del siglo X.

El triángulo de Pascal se construye como una pirámide (de arriba hacia abajo) de la siguiente manera:

- Nivel 0: se comienza con el número 1 centrado en la parte superior.
- Nivel 1: se coloca un número 1 a la izquierda y otro 1 a la derecha.
- Nivel $k+1$: se coloca un número 1 a la izquierda, y otro 1 a la derecha. Los números intermedios se obtienen sumando los dos de arriba del nivel k (ver Figura 5.1).

Nivel 0 →						1						
Nivel 1 →					1		1					
Nivel 2 →				1		2		1				
Nivel 3 →			1		3		3		1			
Nivel 4 →		1		4		6		4		1		
Nivel 5 →	1		5		10		10		5		1	
Nivel 6 →	1	6		15		20		15		6		1

Figura 5.1: Triángulo de Pascal (con números).

Notemos que de acuerdo al Teorema 5.4-(a), 5.4-(d) y 5.4-(e) el triángulo de la Figura 5.1 coincide con el triángulo de la Figura 5.2. Más precisamente el Teorema 5.4-(a) y 5.4-(d) hace referencia a la diagonal, y el Teorema 5.4-(e) hace referencia a cómo construir el nivel siguiente a partir del nivel anterior.

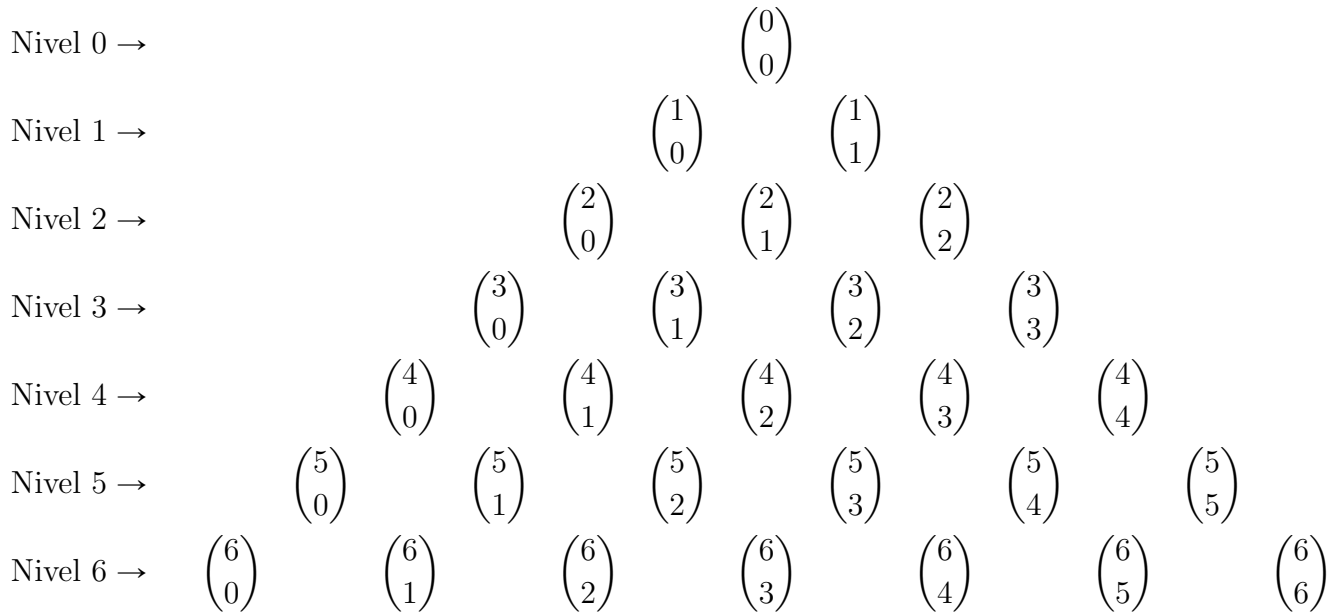


Figura 5.2: Triángulo de Pascal (con números combinatorios).

De esta manera el triángulo de Pascal nos da los coeficientes para construir el binomio de Newton, donde el número de nivel representa la potencia a la cual elevamos el binomio.

Corolario 5.5
Sean a y b números reales no nulos y $n \in \mathbb{N}$. Entonces:

(a)
$$(a-b)^n = \sum_{i=0}^{n} \binom{n}{i} \cdot (-1)^i \cdot a^{n-i} \cdot b^i.$$

(b)
$$2^n = \sum_{i=0}^{n} \binom{n}{i}.$$

(c)
$$0 = \sum_{i=0}^{n} (-1)^i \cdot \binom{n}{i} = \sum_{i=0}^{n} (-1)^{n-i} \cdot \binom{n}{i}.$$

Demostración.
(a)

$$\begin{aligned}
(a-b)^n &= [a+(-b)]^n \\
&= \sum_{i=0}^{n} \binom{n}{i} \cdot a^{n-i} \cdot (-b)^i \quad \text{por Teorema 5.17} \\
&= \sum_{i=0}^{n} \binom{n}{i} \cdot a^{n-i} \cdot (-1)^i \cdot b^i \\
&= \sum_{i=0}^{n} \binom{n}{i} \cdot (-1)^i \cdot a^{n-i} \cdot b^i
\end{aligned}$$

(b)

$$\begin{aligned} 2^n &= (1+1)^n \\ &= \sum_{i=0}^{n} \binom{n}{i} \cdot 1^{n-i} \cdot 1^i \text{ por Teorema 5.17} \\ &= \sum_{i=0}^{n} \binom{n}{i} \end{aligned}$$

(c)

$$\begin{aligned} 0 &= [1+(-1)]^n \\ &= \sum_{i=0}^{n} \binom{n}{i} \cdot 1^{n-i} \cdot (-1)^i \text{ por Teorema 5.17} \\ &= \sum_{i=0}^{n} (-1)^i \cdot \binom{n}{i} \end{aligned}$$

$$\begin{aligned} 0 &= [(-1)+1]^n \\ &= \sum_{i=0}^{n} \binom{n}{i} \cdot (-1)^{n-i} \cdot 1^i \text{ por Teorema 5.17} \\ &= \sum_{i=0}^{n} (-1)^{n-i} \cdot \binom{n}{i} \end{aligned}$$

■

Notar que el Corolario 5.5-(b) nos dice que si A es un conjunto finito de n elementos, entonces la cantidad de elementos del conjunto $\mathcal{P}(A)$ es 2^n.

5.10. Principio de buena ordenación

Definición 5.15 (Primer elemento)
Si $K \subset \mathbb{R}$, diremos que K posee primer elemento (o elemento minimal) si existe $r \in \mathbb{R}$ que satisface:

(a) $r \in K$.

(b) Si $x \in K$ *entonces* $r \leqslant x$.

Ejemplo 5.19

(a) Si $A = \{1, 2, 3, 4, 5\}$ entonces el elemento 1 es minimal.

Esto se debe a que $1 \in A$ y es el más pequeño de todos.

(b) Si $A = \left\{ \dfrac{1}{n} : n \in \mathbb{N} \right\} \cup \{0\}$ entonces el elemento 0 es minimal.

Esto se debe a que $0 \in A$ y además

$$\begin{aligned} 0 &\leqslant 0, \\ 0 &\leqslant \frac{1}{n}, \quad \forall n \in \mathbb{N}. \end{aligned}$$

(c) Si $A = \left\{ \dfrac{1}{n} : n \in \mathbb{N} \right\}$ entonces el conjunto A no posee elemento minimal.

Si existiese elemento minimal, entonces existiría $m \in \mathbb{N}$ tal que

$$\frac{1}{m} \leqslant \frac{1}{n}, \quad \forall n \in \mathbb{N}.$$

Sin embargo

$$\frac{1}{m+1} < \frac{1}{m},$$

y $\dfrac{1}{m+1} \in A$, lo cual es una contradicción.

Definición 5.16 (Conjunto bien ordenado)
Un conjunto $L \subset \mathbb{R}$ se dice bien ordenado (BO) si todo subconjunto no vacío de L posee primer elemento.

Ejemplo 5.20

(a) El conjunto $A = \{1, 2, 3\}$ es bien ordenado.

Analicemos los subconjuntos no vacíos de A:

$$\begin{aligned}
\{1\}, &\quad 1 \text{ es primer elemento} \\
\{2\}, &\quad 2 \text{ es primer elemento} \\
\{3\}, &\quad 3 \text{ es primer elemento} \\
\{1,2\}, &\quad 1 \text{ es primer elemento} \\
\{1,3\}, &\quad 1 \text{ es primer elemento} \\
\{2,3\}, &\quad 2 \text{ es primer elemento} \\
\{1,2,3\}, &\quad 1 \text{ es primer elemento}
\end{aligned}$$

Luego A es bien ordenado.

(b) El conjunto vacío es bien ordenado.

Supongamos que no es bien ordenado. Por definición, debe haber algún subconjunto no vacío de $\varnothing$ que no posea primer elemento. Como tal cosa no sucede nunca, entonces $\varnothing$ es bien ordenado.

(c) El conjunto

$$A = \left\{ \frac{1}{n} : n \in \mathbb{N} \right\} \cup \{0\},$$

no es bien ordenado.

El subconjunto $\{1/n : n \in \mathbb{N}\}$ es no vacío y no tiene primer elemento (ver Ejemplo 5.19-(c)).

Lema 5.2
Todo subconjunto de un conjunto bien ordenado es bien ordenado.

Demostración.
Sea A un conjunto bien ordenado y $B \subset A$. Veamos que B es bien ordenado. Si $B = \varnothing$ entonces B es bien ordenado debido al Ejemplo 5.20-(b). Si $B \neq \varnothing$, tomemos $C \subset B$ con $C \neq \varnothing$. Como $B \subset A$ sabemos que $C \subset A$. Como A es bien ordenado y $C \neq \varnothing$ se tiene que C tiene primer elemento. Luego B es bien ordenado. ■

Teorema 5.18
Todo subconjunto finito de $\mathbb{R}$ *es bien ordenado.*

Demostración.
Sea $A \subset \mathbb{R}$ finito. Si A es finito de cardinal 0 (es decir, $A = \varnothing$) ya hemos visto que A es bien ordenado (ver Ejemplo 5.20-(b)). Supongamos entonces que $A \neq \varnothing$ de cardinal $n \in \mathbb{N}$. Vamos a probar el teorema por inducción en n. Consideremos la siguiente función proposicional en $\mathbb{N}$:

$$P(n): \quad \text{si } A \text{ es finito de cardinal } n, \text{ entonces } A \text{ es bien ordenado.}$$

Observemos que $P(1)$ es V, pues en este caso $A = \{a\}$ con $a \in \mathbb{R}$. El único subconjunto no vacío de A es el mismo A, y tal conjunto posee primer elemento.

Asumamos ahora que $P(n)$ es V. Veamos que $P(n+1)$ es V. Para ver esto consideremos un conjunto A finito de cardinal $n+1$, es decir, existe una función biyectiva

$$\theta : [\![1, n+1]\!] \to A.$$

Llamemos $t = \theta(n+1)$. Es claro que $t \in A$. Restringiendo θ, queda definida una nueva biyección de $[\![1, n]\!]$ en $A - \{t\}$ (o sea $A - \{t\}$ es finito de cardinal n).

Ahora tomemos un subconjunto no vacío $U \subset A$. Vamos a distinguir dos casos:

(a) Si $t \notin U$ entonces $U \subset A - \{t\}$. Como $A - \{t\}$ es finito de cardinal n sucede que U tiene primer elemento (pues $P(n)$ es V).

(b) Si $t \in U$ podemos considerar dos subcasos:

(I) Si $U = \{t\}$ entonces U tiene a t como primer elemento.

(II) Si $U \neq \{t\}$, entonces hay otros elementos en U distintos de t. Esto dice que $U - \{t\} \neq \varnothing$ y además $U - \{t\} \subset A - \{t\}$. De esta manera $U - \{t\}$ posee primer elemento, que llamaremos p (esto se debe a que $A - \{t\}$ es finito de cardinal n).
Por lo tanto p o t es el primer elemento de U.

En cada caso vimos que siempre podemos encontrar un primer elemento para U. Luego A es un conjunto bien ordenado.

Luego la proposición $\forall n \in \mathbb{N}, P(n)$ es V debido al Criterio 5.1. ■

Teorema 5.19
El conjunto $\mathbb{N}$ *es bien ordenado.*

Demostración.
Definamos el siguiente conjunto

$$H = \{h \in \mathbb{N} : \text{ todo subconjunto no vacío de } \mathbb{N} \text{ que contiene a } h \text{ posee primer elemento}\}.$$

Es claro que $H \subset \mathbb{N}$. Vamos a ver que H es un conjunto inductivo.

Observemos que $1 \in H$. Sea $U \subset \mathbb{N}$ no vacío tal que $1 \in U$. Por Proposición 5.1 sabemos que $n \geqslant 1$ para cada $n \in \mathbb{N}$. En particular, $x \geqslant 1$ para cada $x \in U$. Por Definición 5.15 se tiene que 1 es primer elemento de U.

Asumamos ahora que $k \in H$. Esto significa que todo subconjunto de $\mathbb{N}$ que contenga a k posee primer elemento.

Veamos que $k+1 \in H$. Tomemos $L \subset \mathbb{N}$ no vacío tal que $k+1 \in L$. Debemos probar que L posee primer elemento. Se pueden presentar dos casos:

(a) Si $k \in L$, entonces por nuestra hipótesis se tiene que L posee primer elemento.

(b) Si $k \notin L$ definimos

$$L' = L \cup \{k\}.$$

Como $k \in L'$, nuestra hipótesis nos dice que L' posee primer elemento que llamaremos p. Esto significa que

$$\begin{aligned} p &\leqslant k, \\ p &\leqslant x, \quad \forall x \in L. \end{aligned}$$

Se pueden presentar dos casos:

(I) Si $p = k$, entonces $k \leqslant x$ para cada $x \in L$. Como $k \notin L$ se sigue que $k < x$ para cada $x \in L$. Pero por Corolario 5.2-(a) se tiene que $k + 1 \leqslant x$ para cada $x \in L$. Como $k + 1 \in L$ se sigue que $k + 1$ es primer elemento de L.

(II) Si $p \neq k$ entonces $p \in L$. Luego p es primer elemento de L.

De esta manera H es un conjunto inductivo y por Teorema 5.1 se ve que $H = \mathbb{N}$.

Sea ahora $T \subset \mathbb{N}$ no vacío. Como T es no vacío existe $m \in \mathbb{N}$ tal que $m \in T$. Como $H = \mathbb{N}$ entonces $m \in H$. Como T es un subconjunto no vacío de los números naturales que contiene a m se sigue que T tiene primer elemento. Esto ha demostrado que $\mathbb{N}$ es bien ordenado. ■

5.11. Cotas superiores y máximos

Definición 5.17

(a) Sean $X \subset Y \subset \mathbb{R}$ e $y \in Y$ Diremos que y es una cota superior de X en Y si $x \leqslant y$ para cada $x \in X$.

(b) Un subconjunto $Y \subset \mathbb{R}$ se dice acotado superiormente en $\mathbb{R}$ si posee una cota superior en $\mathbb{R}$.

(c) Sea $X \subset \mathbb{R}$. Diremos que un elemento $m \in \mathbb{R}$ es máximo de X si $m \in X$ y m es cota superior de X en $\mathbb{R}$, es decir:

- *$m \in X$.*
- *$x \leqslant m$ para todo $x \in X$.*

Proposición 5.4

Todo subconjunto de $\mathbb{N}$ no vacío y acotado superiormente en $\mathbb{N}$ posee máximo.

Demostración.

Sea $K \subset \mathbb{N}$, $K \neq \varnothing$, acotado superiormente en $\mathbb{N}$. Definimos el siguiente conjunto:

$$L = \{n \in \mathbb{N} : n \text{ es cota superior de } K \text{ en } \mathbb{N}\}.$$

Por definición se tiene que $L \subset \mathbb{N}$. Además, como K está acotado superiormente en $\mathbb{N}$, entonces $L \neq \varnothing$. Por Teorema 5.19 se tiene que existe $m \in L$ que es el elemento minimal de L, es decir:

$$x \leqslant m, \quad \forall x \in K.$$

Vamos a ver que m debe estar en K. Supongamos por el absurdo que $x < m$ para todo $x \in K$. Como $K \neq \varnothing$ se tiene que $1 < m$. Por otro lado, el Corolario 5.2-(a) nos dice que $x + 1 \leqslant m$ para todo $x \in K$, o lo que es lo mismo,

$$x \leqslant m - 1, \quad \forall x \in K.$$

Esto dice que $m-1$ es una cota superior de K en $\mathbb{N}$ (o sea $m-1 \in L$). Pero m era el primer elemento de L y tenemos que $m - 1 < m$, lo cual nos lleva a una contradicción.

Por lo tanto debe existir algún $x \in K$ tal que $x = m$. Esto nos dice que m es un elemento máximo de K. ■

5.12. Variante del principio de inducción

Teorema 5.20 (Variante del principio de inducción)
Sea $H \subset \mathbb{N}$ tal que

- $1 \in H$.
- *Si $n \in \mathbb{N}$ tal que $[\![1, n[\![\subset H$ entonces se cumple que $n \in H$.*

Entonces $H = \mathbb{N}$.

Demostración.
Si $H = \mathbb{N}$ ya está.

Supongamos entonces que $H \subsetneq \mathbb{N}$. Esto dice que $\mathbb{N} - H \neq \varnothing$. Por Teorema 5.19 se sigue que existe $j \in \mathbb{N} - H$ que es elemento minimal. Notemos que $j > 1$, pues si $j = 1$ entonces $j \in H$ que sería una contradicción (pues a su vez $j \in \mathbb{N} - H$). Ahora, como j es el elemento minimal de $\mathbb{N} - H$:

$$\begin{aligned} 1 \notin \mathbb{N} - H, &\qquad (\Rightarrow 1 \in H), \\ 2 \notin \mathbb{N} - H, &\qquad (\Rightarrow 2 \in H), \\ \vdots &\qquad \vdots \\ j - 1 \notin \mathbb{N} - H, &\qquad (\Rightarrow j - 1 \in H), \end{aligned}$$

es decir, $[\![1, j[\![\subset H$. Por hipótesis del teorema se tiene que $j \in H$, o sea que $j \notin \mathbb{N} - H$, lo cual es una contradicción. ■

El Teorema 5.20 nos da el siguiente criterio de inducción.

Criterio 5.2
Sea P una función proposicional sobre $\mathbb{N}$. Si

- *$P(1)$ es V.*
- *La siguiente proposición cuantificada es V:*

$$\forall n \in \mathbb{N}, n > 1, \quad P(k) \text{ es } V \text{ para todo } k < n \Rightarrow P(n) \text{ es } V$$

entonces $P(n)$ es V para todo $n \in \mathbb{N}$.

Demostración.
Definimos el siguiente conjunto:

$$H = \{n \in \mathbb{N} : P(n) \text{ es } V\}.$$

De la definición de H se desprende que $H \subset \mathbb{N}$

Por las hipótesis se tiene que H satisface las hipótesis del Teorema 5.20, por lo que resulta que $H = \mathbb{N}$. Esto quiere decir que $P(n)$ es V para todo $n \in \mathbb{N}$. ■

Ejemplo 5.21
Consideremos la sucesión de Fibonacci definida recursivamente de la siguiente manera:

$$\begin{aligned} a_1 &= 1, \\ a_2 &= 1, \\ a_{n+1} &= a_n + a_{n-1}, \quad n \geqslant 2. \end{aligned}$$

(a) Mostrar que $a_n < 2^n$ para todo $n \in \mathbb{N}$.

Vamos a considerar la función proposicional P definida sobre $\mathbb{N}$:

$$P(n) : a_n < 2^n$$

Observamos que $P(1)$ es V, pues:

$$a_1 = 1 < 2 = 2^1.$$

Supongamos que $n > 1$ y que $P(1), P(2), \ldots, P(n-1)$ son V.

Vamos a probar que $P(n)$ es V. Si $n = 2$ entonces

$$a_2 = 1 < 4 = 2^2,$$

lo cual significa que $P(2)$ es V. Veamos qué sucede si $n \geqslant 3$:

$$\begin{aligned} a_n &= a_{n-1} + a_{n-2} \text{ por definición de la sucesión de Fibonacci} \\ &< 2^{n-1} + 2^{n-2} \text{ por hipótesis inductiva} \\ &< 2^{n-1} + 2^{n-1} \\ &= 2 \cdot 2^{n-1} \\ &= 2^n \end{aligned}$$

Luego la proposición $\forall n \in \mathbb{N}, P(n)$ es V debido al Criterio 5.2.

(b) Mostrar que para todo $n \in \mathbb{N}$

$$a_n = \frac{\alpha^n - \beta^n}{\alpha - \beta},$$

donde $\alpha = \dfrac{1+\sqrt{5}}{2}$ y $\beta = \dfrac{1-\sqrt{5}}{2}$ que son las soluciones de la ecuación $x^2 = x + 1$. El número α es conocido como el número de oro.

Vamos a considerar la función proposicional P definida sobre $\mathbb{N}$:

$$P(n) : a_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

Observamos que $P(1)$ es V, pues:

$$\frac{\alpha^1 - \beta^1}{\alpha - \beta} = \frac{\alpha - \beta}{\alpha - \beta} = 1 = a_1.$$

Supongamos que $n > 1$ y que $P(1), P(2), \ldots, P(n-1)$ son V.

Vamos a probar que $P(n)$ es V. Si $n = 2$ entonces

$$\begin{aligned} \frac{\alpha^2 - \beta^2}{\alpha - \beta} &= \frac{\alpha + 1 - \beta - 1}{\alpha - \beta} \text{ pues } \alpha \text{ y } \beta \text{ satisfacen la ecuación } x^2 = x + 1 \\ &= \frac{\alpha - \beta}{\alpha - \beta} \\ &= 1 \\ &= a_2. \end{aligned}$$

lo cual significa que $P(2)$ es V. Veamos qué sucede si $n \geqslant 3$:

$$\begin{aligned} a_n &= a_{n-1} + a_{n-2} \text{ por definición de la sucesión de Fibonacci} \\ &= \frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta} + \frac{\alpha^{n-2} - \beta^{n-2}}{\alpha - \beta} \text{ por hipótesis inductiva} \\ &= \frac{(\alpha^{n-1} + \alpha^{n-2}) - (\beta^{n-1} + \beta^{n-2})}{\alpha - \beta} \text{ agrupando} \\ &= \frac{\alpha^n - \beta^n}{\alpha - \beta}. \end{aligned}$$

La última igualdad surge multiplicando la ecuación $x^2 = x + 1$ por x^{n-2}, quedando $x^n = x^{n-1} + x^{n-2}$.

Luego la proposición $\forall n \in \mathbb{N}, P(n)$ es V debido al Criterio 5.2.

6. LOS NÚMEROS ENTEROS

6.1. Concepto

Definición 6.1 (Enteros negativos)
Definimos el conjunto de los enteros negativos de la siguiente manera:

$$\mathbb{N}^- = \{-a : a \in \mathbb{N}\}.$$

Es claro que

$$\mathbb{N}^- = \{-1, -2, -3, \ldots\}.$$

Observación 6.1

(a) $x \in \mathbb{N}$ *si y sólo si* $-x \in \mathbb{N}^-$.

(b) $\mathbb{N} \cap \mathbb{N}^- = \varnothing$.

(c) Si a *y* b *son números naturales, entonces*

(I) Si $a > b$ *entonces* $a - b \in \mathbb{N}$.

(II) Si $a = b$ *entonces* $a - b = 0$.

(III) Si $a < b$ *entonces* $a - b \in \mathbb{N}^-$.

Demostración.
(a) Por definición.

(b) Debido a que los elementos de $\mathbb{N}$ son positivos y los elementos de $\mathbb{N}^-$ son negativos.

(c)-(I) Esto se debe al Teorema 5.3.

(c)-(II) Esto se debe al Teorema 4.5-(a).

(c)-(III)

$$\begin{aligned} a < b &\Rightarrow b - a \in \mathbb{N} \text{ por Teorema 5.3} \\ &\Rightarrow -(b - a) \in \mathbb{N}^- \text{ por Definición 6.1} \\ &\Rightarrow a - b \in \mathbb{N}^- \end{aligned}$$

■

Definición 6.2 (Números enteros)
Llamamos conjunto de números enteros al conjunto

$$\mathbb{Z} = \mathbb{N} \cup \{0\} \cup \mathbb{N}^-.$$

6.2. Propiedades

Proposición 6.1
No existe $z \in \mathbb{Z}$ *tal que* $0 < z < 1$.

Demostración.
La condición $z > 0$ implica que $z \in \mathbb{N}$. La Proposición 5.1 nos dice que $z \geqslant 1$, lo cual contradice la hipótesis. Luego no puede existir tal z. ■

Proposición 6.2
Dado $n \in \mathbb{Z}$, no existe $z \in \mathbb{Z}$ tal que $n < z < n+1$.

Demostración.
Si $n > 0$ entonces $n \in \mathbb{N}$. Luego el Corolario 5.2-(b) nos dice que no existe ningún natural z tal que $n < z < n+1$.
Si $n = 0$ el resultado se reduce a la Proposición 6.1 que ya ha sido demostrada.
Supongamos que $n < 0$ y que existe $z \in \mathbb{Z}$ tal que $n < z < n+1$. Luego se tiene que

$$-(n+1) < -z < -n.$$

Como $n < 0$, entonces $-n > 0$, lo que nos dice que $-n \in \mathbb{N}$. Por Proposición 5.1 se tiene que $-n \geqslant 1$, lo que implica que $-n - 1 \geqslant 0$. Es decir,

$$0 \leqslant -(n+1) < -z < -n.$$

Luego estamos en alguno de los dos casos anteriores, por lo que llegamos a una contradicción sobre la existencia de tal z. ■

Teorema 6.1 ($\mathbb{Z}$ es cerrado para la suma y el producto en $\mathbb{R}$)
Sean x e y dos números enteros. Entonces:

(a) $-x \in \mathbb{Z}$.

(b) $x + y \in \mathbb{Z}$.

(c) $x \cdot y \in \mathbb{Z}$.

Demostración.
(a) Si $x = 0$ entonces $-x = -0 = 0 \in \mathbb{Z}$.
Si $x \in \mathbb{N}$, entonces $-x \in \mathbb{N}^- \subset \mathbb{Z}$.
Si $x \in \mathbb{N}^-$, entonces existe $a \in \mathbb{N}$ tal que $x = -a$. Luego $-x = -(-a) = a \in \mathbb{N} \subset \mathbb{Z}$.

(b) Si $x = 0$ entonces $x + y = 0 + y = y \in \mathbb{Z}$.
Si $y = 0$ entonces $x + y = x + 0 = x \in \mathbb{Z}$.
Si $x > 0$ e $y > 0$ entonces $x \in \mathbb{N}$ e $y \in \mathbb{N}$. Luego $x + y \in \mathbb{N}$ por Teorema 5.2-(a). Esto significa que $x + y \in \mathbb{Z}$.
Si $x < 0$ e $y < 0$ entonces existen $a, b \in \mathbb{N}$ tal que $x = -a$ e $y = -b$. Por lo tanto:

$$\begin{aligned} x + y &= -a + (-b) \\ &= -(a + b) \\ &\in \mathbb{N}^- \text{ por el caso anterior} \\ &\subset \mathbb{Z}. \end{aligned}$$

Si $x < 0$ e $y > 0$, entonces existe $a \in \mathbb{N}$ tal que $x = -a$. Entonces podemos distinguir dos casos:

- Si $a < y$ entonces

$$\begin{aligned} x + y &= -a + y \\ &= y - a \\ &\in \mathbb{N} \text{ por Teorema 5.3} \\ &\subset \mathbb{Z}. \end{aligned}$$

- Si $a \geqslant y$ entonces

$$\begin{aligned} -(x+y) &= -x+(-y) \\ &= a-y \\ &\in \mathbb{N}\cup\{0\} \text{ por Teorema 5.3 y Teorema 4.5-(a)} \\ &\subset \mathbb{Z}. \end{aligned}$$

  Luego $x+y=-[-(x+y)] \in \mathbb{Z}$ por (a).

Si $x>0$ e $y<0$, entonces $x+y=y+x \in \mathbb{Z}$ por el caso anterior.

(c) Si $x=0$ entonces $x\cdot y=0\cdot y=0\in\mathbb{Z}$.
Si $y=0$ entonces $x\cdot y=x\cdot 0=0\in\mathbb{Z}$.
Si $x>0$ e $y>0$ entonces $x\in\mathbb{N}$ e $y\in\mathbb{N}$. Luego $x\cdot y\in\mathbb{N}$ por Teorema 5.2-(b). Esto significa que $x\cdot y\in\mathbb{Z}$.
Si $x<0$ e $y<0$ entonces existen $a,b\in\mathbb{N}$ tal que $x=-a$ e $y=-b$. Por lo tanto:

$$\begin{aligned} x\cdot y &= (-a)\cdot(-b) \\ &= a\cdot b \\ &\in \mathbb{N} \text{ por Teorema 5.2-(b)} \\ &\subset \mathbb{Z}. \end{aligned}$$

Si $x<0$ e $y>0$, entonces existe $a\in\mathbb{N}$ tal que $x=-a$, y además $y\in\mathbb{N}$. Por lo tanto:

$$\begin{aligned} x\cdot y &= (-a)\cdot y \\ &= -a\cdot y \\ &\in \mathbb{N}^{-} \text{ pues } a\cdot y\in\mathbb{N} \text{ debido al Teorema 5.2-(b)} \\ &\subset \mathbb{Z}. \end{aligned}$$

Si $x>0$ e $y<0$, entonces $x\cdot y=y\cdot x\in\mathbb{Z}$ por el caso anterior. ■

Observación 6.2
Los únicos elementos inversibles en $\mathbb{Z}$ (es decir, cuyo inverso también es un número entero) son 1 y -1.

Demostración.
Debido al Teorema 4.5-(s) y 4.5-(t) los elementos 1 y -1 son inversibles en $\mathbb{Z}$.
Veamos que son los únicos. Para ello asumamos que tenemos $a\in\mathbb{Z}$ inversible en $\mathbb{Z}$, es decir,

$$a\neq 0 \text{ y } \exists c\in\mathbb{Z} : a\cdot c=1.$$

Si $a>0$ entonces $c>0$ debido a la regla de los signos. Luego a y c son números naturales. Debido al Ejemplo 5.3-(c) tenemos que $a=c=1$.
Asumamos ahora que $a<0$. Esto nos dice que $c<0$. Por otro lado sabemos que $(-a)\cdot(-c)=1$ donde $-a>0$ y $-c>0$. Por ello estamos en el caso anterior, y debe ocurrir que $-a=1$, o sea, $a=-1$. ■

Observación 6.3
$\mathbb{Z}$ no es bien ordenado.

Demostración.

Veamos que $\mathbb{N}^-$ no tiene primer elemento. Supongamos que lo tiene, entonces existe $x \in \mathbb{N}^-$ tal que $x \leqslant y$ para todo $y \in \mathbb{N}^-$. Sabemos que existe $a \in \mathbb{N}$ tal que $x = -a$. Por otro lado sabemos que $a < a + 1$, lo cual implica que $-(a+1) < -a = x$. Pero resulta que $-(a+1) \in \mathbb{N}^-$ y es menor que x. Esto es una contradicción. Como tenemos un subconjunto no vacío de $\mathbb{Z}$ que no tiene primer elemento, se deduce que $\mathbb{Z}$ no es bien ordenado. ■

Proposición 6.3

Sea $z \in \mathbb{Z}$. Entonces

$$S_z = \{m \in \mathbb{Z} : z \leqslant m\},$$

es bien ordenado. El conjunto S_z se denomina la sección o semirrecta cerrada a derecha de z.

Demostración.

Sea $K \subset S_z$ no vacío. Definimos:

$$K' = \{k + |z| + 1 : k \in K\},$$

la traslación de K a la derecha en $|z| + 1$ unidades. Observemos los siguientes hechos:

- K' es no vacío.
- $z \leqslant k$ para cada $k \in K$.
- $-z \leqslant |z|$ por Teorema 4.8-(h). Luego se tiene que $0 \leqslant z + |z|$, y también que $1 \leqslant z + |z| + 1$.

Se deduce entonces que:

$$1 \leqslant z + |z| + 1 \leqslant k + |z| + 1, \quad \forall k \in K.$$

Como $K' \subset \mathbb{Z}$ y todos sus elementos son positivos se tiene que $K' \subset \mathbb{N}$. Como $\mathbb{N}$ es bien ordenado, se sigue que K' tiene primer elemento que llamaremos $a = k_0 + |z| + 1$ con $k_0 \in K$. Luego

$$\begin{aligned} a &\leqslant k + |z| + 1, \quad \forall k \in K, \\ k_0 + |z| + 1 &\leqslant k + |z| + 1, \quad \forall k \in K, \\ k_0 &\leqslant k, \quad \forall k \in K. \end{aligned}$$

Luego, $k_0 \in K$ es primer elemento de K. ■

6.3. Divisibilidad

Definición 6.3

Sean $a, b \in \mathbb{Z}$ con $a \neq 0$. Diremos que a divide a b (o que b es múltiplo de a) en $\mathbb{Z}$ si existe $c \in \mathbb{Z}$ tal que

$$b = a \cdot c.$$

Lo denotamos con el símbolo $a \mid b$. Con $a \nmid b$ denotamos la negación de $a \mid b$.

Observación 6.4

(a) Remarcamos que el símbolo $a \mid b$ no es una división entre números enteros. En realidad es una proposición que dice que a divide a b, o que b es un múltiplo de a.

(b) Si en la Definición 6.3 permitiéramos que $a = 0$, entonces la proposición $a \mid b$ diría que existe $c \in \mathbb{Z}$ tal que $b = 0 \cdot c$. O sea, debe ocurrir que $b = 0$. Por lo tanto considerar la definición de divisibilidad permitiendo $a = 0$ sólo nos estaría aportando el caso $0 \mid 0$ que ya sabemos que es válido, y por esta razón este caso particular no lo consideramos.

Ejemplo 6.1

(a) Como $8 = 2 \cdot 4$ se tiene que $2 \mid 8$ y $4 \mid 8$.

(b) Como $33 = 3 \cdot 11$ se tiene que $3 \mid 33$ y $11 \mid 33$.

(c) Como $-50 = 2 \cdot (-25) = (-2) \cdot 25$ se tiene que $2 \mid -50$, $-25 \mid -50$, $-2 \mid -50$ y $25 \mid -50$.

Proposición 6.4 (Propiedades básicas de divisibilidad)
Sean a, b y c números enteros donde $a \neq 0$. Entonces

(a) $a \mid a$, $a \mid a \cdot c$, $a \mid -a$, $-a \mid a$, $a \mid |a|$ *y* $|a| \mid a$.

(b) $1 \mid c$ *y* $-1 \mid c$.

(c) Sea $b \neq 0$*:* $a \mid b$ *y* $b \mid c \Rightarrow a \mid c$.

(d) Sea $b \neq 0$*:* $a \mid b$ *y* $b \mid a \Rightarrow a = b$ *o* $a = -b$.

(e) $a \mid 1 \Rightarrow a = 1$ *o* $a = -1$.

(f) $a \mid b$ *y* $a \mid c \Rightarrow a \mid b + c$ *y* $a \mid b - c$.

(g) $a \mid b + c$ *y* $a \mid b \Rightarrow a \mid c$.

(h) $a \mid b \Rightarrow a \mid b \cdot c$.

(i) $a \mid b \Leftrightarrow a \mid |b|$.

(j) $a \mid b \Leftrightarrow |a| \mid b$.

(k) $a \mid b \Leftrightarrow |a| \mid |b|$.

Demostración.
(a) Como $a = a \cdot 1$ entonces $a \mid a$.
Como $(a \cdot c) = a \cdot c$ entonces $a \mid a \cdot c$.
Como $-a = a \cdot (-1)$ entonces $a \mid -a$.
Como $a = (-a) \cdot (-1)$ entonces $-a \mid a$.
Como $a \mid a$ y $a \mid -a$ entonces $a \mid |a|$.
Como $a \mid a$ y $-a \mid a$ entonces $|a| \mid a$.

(b) Como $c = 1 \cdot c$, entonces $1 \mid c$. Además, como $c = (-1) \cdot (-c)$ entonces $-1 \mid c$.

(c)
$$\left.\begin{array}{rcl} a \mid b & \Rightarrow & \exists u \in \mathbb{Z} \text{ tal que } b = a \cdot u \\ b \mid c & \Rightarrow & \exists v \in \mathbb{Z} \text{ tal que } c = b \cdot v \end{array}\right\} \Rightarrow c = b \cdot v = (a \cdot u) \cdot v = a \cdot (u \cdot v)\,,$$
luego $a \mid c$.

(d)
$$\left.\begin{array}{rcl} a \mid b & \Rightarrow & \exists u \in \mathbb{Z} \text{ tal que } b = a \cdot u \\ b \mid a & \Rightarrow & \exists v \in \mathbb{Z} \text{ tal que } a = b \cdot v \end{array}\right\} \Rightarrow b = a \cdot u = b \cdot v \cdot u.$$
Por Teorema 4.4-(b) se tiene que $v \cdot u = 1$ y por Teorema 4.5-(i) tenemos que $v \neq 0$. Luego v es un elemento inversible en $\mathbb{Z}$, y por la Observación 6.2 se tiene que $v = 1$ o $v = -1$.

Para el caso $v = 1$ se tiene que $a = b$. Para el caso que $v = -1$ tenemos que $a = -b$.

(e) Supongamos que $a \mid 1$. Como sabemos que $1 \mid a$ por (b), entonces (d) nos dice que $a = 1$ o $a = -1$.

(f)

$$\left.\begin{array}{rcl} a \mid b & \Rightarrow & \exists u \in \mathbb{Z} \text{ tal que } b = a \cdot u \\ a \mid c & \Rightarrow & \exists v \in \mathbb{Z} \text{ tal que } c = a \cdot v \end{array}\right\} \Rightarrow \left\{\begin{array}{l} b + c = a \cdot u + a \cdot v = a \cdot (u + v) \\ b - c = a \cdot u - a \cdot v = a \cdot (u - v) \end{array}\right.$$

Luego $a \mid b + c$ y $a \mid b - c$.

(g) Usando (f)

$$\left.\begin{array}{l} a \mid b + c \\ a \mid b \end{array}\right\} \Rightarrow a \mid b + c - b \Rightarrow a \mid c.$$

(h)

$$\begin{array}{rcl} a \mid b & \Rightarrow & \exists u \in \mathbb{Z} \text{ tal que } b = a \cdot u \\ & \Rightarrow & b \cdot c = a \cdot u \cdot c \\ & \Rightarrow & a \mid b \cdot c \end{array}$$

(i) Asumamos primero que $a \mid b$. Si $b \geqslant 0$ entonces $|b| = b$, lo que dice que $a \mid |b|$. Por el contrario, si $b < 0$ entonces $|b| = -b$. Como sabemos que $a \mid b$, esto implica que $a \mid -b$ por (h), es decir $a \mid |b|$.

Asumamos ahora que $a \mid |b|$. Esto significa que existe $u \in \mathbb{Z}$ tal que $|b| = a \cdot u$. Si $b \geqslant 0$ entonces $|b| = b$ por lo que $b = a \cdot u$, lo que nos dice que $a \mid b$. Si $b < 0$ entonces $|b| = -b$. Luego $-b = a \cdot u$, lo que implica que $b = a \cdot (-u)$. Esto nos dice que $a \mid b$. En ambos casos resulta que $a \mid b$.

(j) Asumamos primero que $a \mid b$. Si $a \geqslant 0$ entonces $|a| = a$, lo que dice que $|a| \mid b$. Por el contrario, si $a < 0$ entonces $|a| = -a$. Como sabemos que $a \mid b$, esto significa que existe $u \in \mathbb{Z}$ tal que $b = a \cdot u$. Luego tenemos que $b = (-a) \cdot (-u)$, por lo que deducimos que $-a \mid b$, es decir $|a| \mid b$.

Asumamos ahora que $|a| \mid b$. Esto significa que existe $u \in \mathbb{Z}$ tal que $b = |a| \cdot u$. Si $a \geqslant 0$ entonces $|a| = a$ por lo que $b = a \cdot u$, lo que nos dice que $a \mid b$. Si $a < 0$ entonces $|a| = -a$. Luego $b = (-a) \cdot u$, lo que implica que $b = a \cdot (-u)$. Esto nos dice que $a \mid b$. En ambos casos resulta que $a \mid b$.

(k)

$$\begin{array}{rcl} a \mid b & \Leftrightarrow & a \mid |b| \text{ por (i)} \\ & \Leftrightarrow & |a| \mid |b| \text{ por (j)} \end{array}$$

■

Notemos que del Teorema 6.4-(a) y 6.4-(b) todo número $a \neq 0$ tiene al menos los siguientes divisores, a saber: 1, -1, a y $-a$.

6.4. Números primos

Definición 6.4 (Número primo)
Llamaremos número primo a todo número entero que posea exactamente 4 divisores.

Ejemplo 6.2
(a) 0 no es primo.

Como $0 = a \cdot 0$ para cualquier $a \in \mathbb{Z}$ no nulo, se tiene que 0 tiene infinitos divisores.

(b) 1 y -1 no son números primos.

Sea $a \in \mathbb{Z}$ no nulo tal que $a \mid 1$. Esto significa que existe $b \in \mathbb{Z}$ tal que $1 = a \cdot b$. Luego a es un elemento inversible en $\mathbb{Z}$. Por Observación 6.2 se tiene que $a = 1$ o $a = -1$, por lo que 1 tiene exactamente dos divisores.

Análogamente, sea $a \in \mathbb{Z}$ no nulo tal que $a \mid -1$. Por Proposición 6.4-(h) deducimos que $a \mid 1$. Por el caso anterior obtenemos que $a = 1$ o $a = -1$, por lo que -1 tiene exactamente dos divisores.

(c) 2 es número primo.

Sea $a \in \mathbb{Z}$ no nulo tal que $a \mid 2$. Esto significa que existe $b \in \mathbb{Z}$ tal que $2 = a \cdot b$. Naturalmente, $b \neq 0$ debido al Teorema 4.5-(i).

Si $a > 0$ entonces resulta que $b > 0$ por Teorema 4.7-(k) a 4.7-(l) ya que $2 > 0$. Luego se tiene que a y b son números naturales, lo que implica que $1 \leqslant a$ y $1 \leqslant b$ por Proposición 5.1. Un posible valor para a es 1, con lo cual $2 = a \cdot b = 1 \cdot b = b$. Por el contrario, suponiendo que $a \neq 1$ se tiene que $1 < a$. Ahora:

$$\begin{aligned} 1 < a &\Rightarrow 1 \cdot b < a \cdot b \text{ por Axioma (PC)} \\ &\Rightarrow b < 2 \text{ pues } 2 = a \cdot b \end{aligned}$$

por lo que $b = 1$ por Proposición 5.2. Luego $2 = a \cdot b = a \cdot 1 = a$, por lo que $a = 2$. Resumiendo, $a = 1$ o $a = 2$.

Si $a < 0$ entonces escribimos $2 = a \cdot b = (-a) \cdot (-b)$ donde $-a > 0$ por Teorema 4.7-(c). Luego estamos en el caso anterior, con lo cual $-a = 1$ o $-a = 2$ lo que implica que $a = -1$ o $a = -2$.

Concluimos entonces que 2 tiene exactamente cuatro divisores: -2, -1, 1 y 2. Esto significa que 2 es primo.

(d) 4 no es primo.

Como $4 = 2 \cdot 2$, se ve que 4 tiene a 2 como divisor, aparte de los 4 divisores 1, 4, -1 y -4. Luego 4 no es primo.

(e) 3 es número primo.

Sea $a \in \mathbb{Z}$ no nulo tal que $a \mid 3$. Esto significa que existe $b \in \mathbb{Z}$ tal que $3 = a \cdot b$. Naturalmente, $b \neq 0$ debido al Teorema 4.5-(i).

Si $a > 0$ entonces resulta que $b > 0$ por Teorema 4.7-(k) a 4.7-(l) ya que $3 > 0$. Luego se tiene que a y b son números naturales, lo que implica que $1 \leqslant a$ y $1 \leqslant b$ por Proposición 5.1. Un posible valor para a es 1, con lo cual $3 = a \cdot b = 1 \cdot b = b$. Por el contrario, suponiendo que $a \neq 1$ se tiene que $1 < a$ (lo que implica también que $2 \leqslant a$ por Proposición 5.2-(b)). Ahora:

$$\begin{aligned} 1 < a &\Rightarrow 1 \cdot b < a \cdot b \text{ por Axioma (PC)} \\ &\Rightarrow b < 3 \text{ pues } 3 = a \cdot b \end{aligned}$$

por lo que $b = 1$ o $b = 2$ por Proposición 5.2-(b) y Proposición 5.1. Pero si $b = 2$ entonces $3 = a \cdot b \geqslant 2 \cdot 2 = 4$ lo cual es una contradicción. Por esto se tiene que $b = 1$ y por lo tanto $3 = a \cdot b = a \cdot 1 = a$. Resumiendo, $a = 1$ o $a = 3$.

Si $a < 0$ entonces escribimos $3 = a \cdot b = (-a) \cdot (-b)$ donde $-a > 0$ por Teorema 4.7-(c). Luego estamos en el caso anterior, con lo cual $-a = 1$ o $-a = 3$ lo que implica que $a = -1$ o $a = -3$.

Concluimos entonces que 3 tiene exactamente cuatro divisores: -3, -1, 1 y 3. Esto significa que 3 es primo.

Observación 6.5
Sea $p \in \mathbb{Z}$. Luego, p es primo si y sólo si $|p|$ es primo.

Demostración.
El resultado es una consecuencia directa del hecho que p y $|p|$ tienen los mismos divisores debido a la Proposición 6.4-(i). ■

Definición 6.5
Un número $m \in \mathbb{Z}$ se dice par (impar) si $2 \mid m$ ($2 \nmid m$).

Proposición 6.5
Sean $a, b, c \in \mathbb{N}$. Luego

$$a = b \cdot c \Rightarrow b \leqslant a \text{ y } c \leqslant a.$$

En particular, esto significa que si $b \mid a$ entonces $b \leqslant a$.

Demostración.
Por Proposición 5.1 tenemos que $1 \leqslant b$, $1 \leqslant c$ y, en particular, $b > 0$ y $c > 0$. Por lo que tenemos:

$$\begin{aligned} 1 \leqslant b &\Rightarrow 1 \cdot c \leqslant b \cdot c \Rightarrow c \leqslant b \cdot c \Rightarrow c \leqslant a \\ 1 \leqslant c &\Rightarrow b \cdot 1 \leqslant b \cdot c \Rightarrow b \leqslant b \cdot c \Rightarrow b \leqslant a. \end{aligned}$$ ■

Proposición 6.6
Sea $a \in \mathbb{Z}$ tal que $a \neq 1$, $a \neq -1$, $a \neq 0$ y a no es un número primo. Entonces existe $t \in \mathbb{N}$ tal que $1 < t < |a|$ y $t \mid |a|$.

Demostración.
Como a no es un número primo y además es distinto de 1, -1 y 0, existe $r \in \mathbb{Z}$ distinto de 0, 1, -1, a y $-a$ tal que $a = r \cdot s$ para algún $s \in \mathbb{Z}$. Tomando valor absoluto tenemos que $|a| = |r| \cdot |s|$ donde $|r|$ es un número natural. Por Proposición 5.1 y Proposición 6.5 se tiene que $1 \leqslant |r| \leqslant |a|$. Pero como $r \neq 1$, $r \neq -1$, $r \neq a$ y $r \neq -a$ se cumple que $1 < |r| < |a|$. Finalmente, observemos que como $r \mid a$ entonces $|r| \mid |a|$ por Proposición 6.4-(k). Luego $t = |r|$ es el número que buscamos. ■

Teorema 6.2
Todo entero distinto de 1, -1 y 0 es divisible por un número primo.

Demostración.
Vamos a razonar por el absurdo. Supongamos que existe $t \in \mathbb{Z}$ tal que $t \neq 1, -1, 0$ que no es divisible por ningún primo. Luego $|t|$ tampoco es divisible por ningún primo (pues t y $|t|$ tiene los mismos divisores debido a la Proposición 6.4-(i)). Esto dice que hay al menos un natural (distinto de 1) no divisible por ningún primo.

Llamemos

$$H = \{x \in \mathbb{N} : x \neq 1 \text{ y } x \text{ no es divisible por ningún primo}\}.$$

Como $|t| \in H$ se tiene que $H \neq \varnothing$. Como $H \subset \mathbb{N}$, el Teorema 5.19 nos dice que H tiene primer elemento que llamaremos g. Como $g \in H$ entonces g no es primo, pues de otro modo, como $g \mid g$ entonces g sería divisible por un primo. Por definición de H tenemos que $g \neq 1$ y como $H \subset \mathbb{N}$ tenemos que $g \neq -1$ y $g \neq 0$. Por Proposición 6.6 existe $k \in \mathbb{N}$, $1 < k < g$ tal que $k \mid g$.

Como $k < g$ entonces $k \notin H$, con lo cual $k = 1$ o k es divisible por algún primo. Como $k > 1$ se tiene que existe p primo tal que $p \mid k$. Debido a que $p \mid k$ y $k \mid g$, se tiene que $p \mid g$ por el Teorema 6.4-(c). Por lo tanto g es divisible por un primo, lo cual es una contradicción. De este modo, todo entero $t \neq 1, -1, 0$ es divisible por algún primo. ■

Teorema 6.3
Existen infinitos primos en $\mathbb{Z}$.

Demostración.
Razonemos por al absurdo. Supongamos que hay a lo sumo un número finito de números primos:

$$p_1, \ldots, p_k.$$

Definamos $x \in \mathbb{Z}$ dado por

$$x = \prod_{i=1}^{k} p_i + 1.$$

Observemos que $x \neq 1$, $x \neq -1$ y $x \neq 0$. Si $x = 1$ se tiene que

$$\begin{aligned} x = 1 &\Rightarrow \prod_{i=1}^{k} p_i + 1 = 1 \\ &\Rightarrow \prod_{i=1}^{k} p_i = 0 \\ &\Rightarrow \exists i \in \{1, \ldots, k\} : p_i = 0 \text{ por Teorema 4.5-(i)} \end{aligned}$$

lo cual es una contradicción pues 0 no es primo por el Ejemplo 6.2-(a). Por otro lado, si $x = -1$ se tiene que

$$\begin{aligned} x = -1 &\Rightarrow \prod_{i=1}^{k} p_i + 1 = -1 \\ &\Rightarrow \prod_{i=1}^{k} p_i = -2 \\ &\Rightarrow \prod_{i=1}^{k} |p_i| = 2 \\ &\Rightarrow \forall i \in \{1, \ldots, k\}, |p_i| \leqslant 2 \text{ por Proposición 6.5} \end{aligned}$$

lo cual es una contradicción pues 3 es un número primo y $3 > 2$. Finalmente, si $x = 0$ se tiene que:

$$\begin{aligned} x = 0 &\Rightarrow \prod_{i=1}^{k} p_i + 1 = 0 \\ &\Rightarrow \prod_{i=1}^{k} p_i = -1 \\ &\Rightarrow \prod_{i=1}^{k} |p_i| = 1 \\ &\Rightarrow \forall i \in \{1, \ldots, k\}, |p_i| \leqslant 1 \text{ por Proposición 6.5} \end{aligned}$$

lo cual es una contradicción pues 2 es un número primo y $2 > 1$.

Por lo tanto, el Teorema 6.2 nos dice que x es divisible por algún primo q, es decir,

$$q \mid \prod_{i=1}^{k} p_i + 1,$$

pero como q es alguno de los $p_1, \ldots, p_k$ se tiene que

$$q \mid \prod_{i=1}^{k} p_i$$

debido a la Proposición 6.4-(h). Por Proposición 6.4-(f) se tiene que

$$q \mid \prod_{i=1}^{k} p_i + 1 - \prod_{i=1}^{k} p_i,$$

lo que dice que $q \mid 1$. Por Proposición 6.4-(e) se tiene que $q = 1$ o $q = -1$, pero esto contradice el hecho que q es primo (ver Ejemplo 6.2-(b)). Por lo tanto, existen infinitos primos en $\mathbb{Z}$. ■

6.5. Criterio para detectar números primos

Sea $a \in \mathbb{N}$. Llamemos

$$H_a = \left\{ y \in \mathbb{N} : y^2 \leqslant a \right\}.$$

El conjunto H_a es no vacío pues $1 \in H_a$. Ahora, si $y \in H_a$ se tiene que $1 \leqslant y$ por Proposición 5.1. Luego se deduce por el Axioma (PC) que $y \leqslant y^2$. Pero como $y \in H_a$ se tiene que $y \leqslant y^2 \leqslant a$. Esto nos dice que H_a es un conjunto acotado superiormente en $\mathbb{N}$. Por Proposición 5.4 el conjunto H_a tiene máximo. Esto motiva la siguiente definición.

Definición 6.6 (Raíz cuadrada entera)
Dado $a \in \mathbb{N}$, llamamos raíz cuadrada entera de a, denotada por $\lfloor \sqrt{a} \rfloor$, al máximo del siguiente conjunto:

$$H_a = \left\{ y \in \mathbb{N} : y^2 \leqslant a \right\}.$$

Notemos que el máximo del conjunto H_a existe por la Proposición 5.4.

Ejemplo 6.3

(a) $a = 1$.

$$H_1 = \{1\} \Rightarrow \left\lfloor \sqrt{1} \right\rfloor = 1.$$

(b) $a = 2$.

$$H_2 = \{1\} \Rightarrow \left\lfloor \sqrt{2} \right\rfloor = 1.$$

(c) $a = 3$.

$$H_3 = \{1\} \Rightarrow \left\lfloor \sqrt{3} \right\rfloor = 1.$$

(d) $a = 4$.

$$H_4 = \{1, 2\} \Rightarrow \left\lfloor \sqrt{4} \right\rfloor = 2.$$

(e) $a = 15$.

$$H_{15} = \{1, 2, 3\} \Rightarrow \left\lfloor \sqrt{15} \right\rfloor = 3.$$

(f) $a = 17$.

$$H_{17} = \{1, 2, 3, 4\} \Rightarrow \left\lfloor \sqrt{17} \right\rfloor = 4.$$

(g) $a = 99$.

$$H_{99} = \{1, 2, 3, 4, 5, 6, 7, 8, 9\} \Rightarrow \left\lfloor \sqrt{99} \right\rfloor = 9.$$

Criterio 6.1 (Criba de Eratóstenes)
Sea $a \in \mathbb{N}$ con $a \neq 1$. Si a no es divisible por ningún primo p tal que $p \leqslant \lfloor \sqrt{a} \rfloor$ entonces a es primo.

Demostración.

Como $a \neq 1$ tenemos que a es divisible por un primo positivo q debido al Teorema 6.2 y a la Proposición 6.4-(j). Llamemos

$$H = \{h \in \mathbb{N} : h \text{ es primo y } h \mid a\}.$$

Notemos que $H \subset \mathbb{N}$ y que H es no vacío pues $q \in H$. El Teorema 5.19 afirma que H tiene un elemento minimal que llamaremos p.

Como $p \mid a$ existe $x \in \mathbb{N}$ tal que $a = p \cdot x$ (notar que también $x \neq 0$). Además esto dice que $x \mid a$.

De ahora en adelante razonemos por el absurdo y asumamos que a no es primo.

Se observa que $x > 1$, pues si $x = 1$ entonces $a = p$ y a sería primo.

Por el Teorema 6.2 y la Proposición 6.4-(j) se tiene que existe un primo $r \in \mathbb{N}$ tal que $r \mid x$. Por Proposición 6.5 tenemos que $r \leqslant x$.

Como $r \mid x$ y $x \mid a$ se cumple que $r \mid a$ por Teorema 6.4-(c).

Si ocurriera que $p > x$ entonces $p > r$, pero esto es una contradicción pues p es un elemento minimal de H. Por lo tanto $p \leqslant x$, lo cual implica que $p^2 \leqslant p \cdot x = a$, es decir, $p \in H_a$. Esto significa que p es un número primo tal que $p \mid a$ y $p \leqslant \lfloor \sqrt{a} \rfloor$, lo cual es una contradicción. Por lo tanto a es primo. ■

Ejemplo 6.4

(a) Determinar los números primos hasta 35.

Procedemos de la siguiente manera:

- Calculamos primero la raíz cuadrada entera: $\lfloor \sqrt{35} \rfloor = 5$. Los primos p tales que $p \leqslant \lfloor \sqrt{35} \rfloor$ son: 2, 3 y 5.
- Confeccionamos una lista de números hasta 35.
- Eliminamos el 1 pues no es primo.
- "Cribamos" los múltiplos de 2 (sin contar el 2 pues es primo) marcando con $\boxed{\cdot}$.
- "Cribamos" los múltiplos de 3 (sin contar el 3 pues es primo) marcando con $\boxed{\cdot}$.
- "Cribamos" los múltiplos de 5 (sin contar el 5 pues es primo) marcando con $\boxed{\cdot}$.
- Los elementos sin recuadro son los números primos hasta 35, a saber, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29 y 31.

~~1~~	2	3	$\boxed{4}$	5	$\boxed{6}$	7	$\boxed{8}$	$\boxed{9}$	$\boxed{10}$
11	$\boxed{12}$	13	$\boxed{14}$	$\boxed{15}$	$\boxed{16}$	17	$\boxed{18}$	19	$\boxed{20}$
$\boxed{21}$	$\boxed{22}$	23	$\boxed{24}$	$\boxed{25}$	$\boxed{26}$	$\boxed{27}$	$\boxed{28}$	29	$\boxed{30}$
31	$\boxed{32}$	$\boxed{33}$	$\boxed{34}$	$\boxed{35}$					

6.6. Algoritmo de la división

Teorema 6.4 (Existencia del algoritmo de división en $\mathbb{Z}$)
Sean $a, b \in \mathbb{Z}$ con $b > 0$. Entonces existen únicos $q, r \in \mathbb{Z}$ tales que:

$$a = b \cdot q + r, \quad 0 \leqslant r < b.$$

Los números q y r se denominan respectivamente el cociente y el resto de la división de a por b.

Demostración.
Analicemos primero la existencia.
Llamemos $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. Por la Proposición 6.3 el conjunto $\mathbb{N}_0$ es bien ordenado (pues $\mathbb{N}_0 = S_0$ es la semirrecta cerrada a derecha de 0).
Sea

$$L = \{a - b \cdot k : k \in \mathbb{Z}\}.$$

Vamos a ver ahora que $L \cap \mathbb{N}_0 \neq \varnothing$:

- Si $a \geqslant 0$ entonces $a \in \mathbb{N}_0$. Además $a = a - b \cdot 0 \in L$. Por lo tanto deducimos que $a \in L \cap \mathbb{N}_0$.
- Por otro lado, si $a < 0$ tenemos que $-a > 0$. Además, como $b > 0$ tenemos que $b \geqslant 1$, es decir, $b - 1 \geqslant 0$. Por lo tanto,

$$0 \leqslant (-a) \cdot (b-1) = (-a) \cdot b - (-a) = a - a \cdot b = a - b \cdot a \in L \cap \mathbb{N}_0.$$

Como $L \cap \mathbb{N}_0 \subset \mathbb{N}_0$, $L \cap \mathbb{N}_0 \neq \varnothing$ y $\mathbb{N}_0$ es bien ordenado, entonces $L \cap \mathbb{N}_0$ posee elemento minimal que llamaremos r. Veamos las propiedades de r:

- Como $r \in L$, existe $q \in \mathbb{Z}$ tal que $r = a - b \cdot q$.
- Como $r \in \mathbb{N}_0$ entonces $r \geqslant 0$.
- r es un elemento minimal de $L \cap \mathbb{N}_0$.

Luego $a = b \cdot q + r$ donde $r \geqslant 0$. Veamos que $r < b$, para lo cual razonemos por el absurdo suponiendo que $r \geqslant b$. Entonces

$$a = b \cdot q + r = b \cdot q + b - b + r = b \cdot (q+1) + (r - b).$$

Por lo tanto tenemos que:

$$\begin{aligned} a = b \cdot (q+1) + (r-b) &\Rightarrow r - b = a - b \cdot (q+1) \in L, \\ r \geqslant b &\Rightarrow r - b \geqslant 0 \Rightarrow r - b \in \mathbb{N}_0. \end{aligned}$$

Esto significa que $r - b \in L \cap \mathbb{N}_0$ y $r - b < r$, lo cual es una contradicción pues r era el elemento minimal.
Resumiendo, existe $q, r \in \mathbb{Z}$ tal que $a = b \cdot q + r$ donde $0 \leqslant r < b$.
Analicemos ahora la unicidad.
Sean $q, q', r, r' \in \mathbb{Z}$ tal que

$$\begin{aligned} a &= b \cdot q + r, \quad 0 \leqslant r < b, \\ a &= b \cdot q' + r', \quad 0 \leqslant r' < b. \end{aligned}$$

Restando:

$$b \cdot (q - q') = r' - r.$$

Tomando valor absoluto:

$$b \cdot |q - q'| = |r' - r| .$$

Supongamos que $|q - q'| > 0$. Entonces $|q - q'| \geqslant 1$, lo cual dice que

$$|r' - r| = b \cdot |q - q'| \geqslant b.$$

Por otra parte, sabemos que $0 \leqslant r < b$ y $0 \leqslant r' < b$, lo cual implica que:

$$\begin{aligned} r' < b \leqslant b + r &\Rightarrow r' - r < b, \\ r < b \leqslant b + r' &\Rightarrow r - r' < b \Rightarrow -b < r' - r. \end{aligned}$$

Luego, tenemos que $-b < r' - r < b$ lo cual dice que $|r' - r| < b$. Pero esto es una contradicción. Por lo tanto $|q - q'| = 0$ y como consecuencia obtenemos que $|r' - r| = 0$. Esto significa que $q = q'$ y $r = r'$. ■

Corolario 6.1
Sean $a, b \in \mathbb{Z}$ con $b \neq 0$. Entonces existen únicos $q, r \in \mathbb{Z}$ tales que:

$$a = b \cdot q + r, \quad 0 \leqslant r < |b| .$$

Demostración.

Si $b > 0$, la existencia y unicidad surge de manera inmediata del Teorema 6.4.

Si $b < 0$ entonces $-b > 0$. Luego el Teorema 6.4 dice que existen $q, r \in \mathbb{Z}$ tales que $a = (-b) \cdot q + r$ con $0 \leqslant r < -b$. Pero

$$a = (-b) \cdot q + r = b \cdot (-q) + r.$$

Esto nos da la existencia. Para probar la unicidad, sean $q, q', r, r' \in \mathbb{Z}$ tal que

$$\begin{aligned} a &= b \cdot q + r, \quad 0 \leqslant r < |b| , \\ a &= b \cdot q' + r', \quad 0 \leqslant r' < |b| . \end{aligned}$$

Luego

$$\begin{aligned} a &= b \cdot q + r = (-b) \cdot (-q) + r, \quad 0 \leqslant r < -b, \\ a &= b \cdot q' + r' = (-b) \cdot (-q') + r', \quad 0 \leqslant r' < -b. \end{aligned}$$

Por unicidad surge que $r = r'$ y también que $-q = -q'$, es decir, $q = q'$. ■

6.7. Máximo común divisor

Teorema 6.5 (Máximo común divisor)
Sean $a, b \in \mathbb{Z}$ con $b \neq 0$. Entonces existe un único $d \in \mathbb{N}$ con las siguientes propiedades:

(a) $d \mid a$ y $d \mid b$.

(b) Existen $u, v \in \mathbb{Z}$ tales que $d = u \cdot a + v \cdot b$.

El número d se denomina máximo común divisor (m.c.d.) de a y b y se denota (a, b). La forma de escribir a d como en (b) se denomina una combinación lineal entera de a y b.

Demostración.

Analizaremos primero la existencia.

Supongamos primero que $b > 0$, o sea $b \in \mathbb{N}$. Haremos la prueba por inducción en b. Sea la siguiente función proposicional definida en $\mathbb{N}$:

$$P(b): \quad \forall a \in \mathbb{Z}, \exists d \in \mathbb{N}: \begin{cases} d \mid a \text{ y } d \mid b, \\ \exists u, v \in \mathbb{Z}: d = u \cdot a + v \cdot b. \end{cases}$$

Observemos que $P(1)$ es V, pues dado $a \in \mathbb{Z}$ elegimos $d = 1 \in \mathbb{N}$. Luego

$$\begin{aligned} &1 \mid a \text{ y } 1 \mid 1 \text{ por Proposición 6.4-(b)} \\ &\text{Sean } u = 0 \in \mathbb{Z} \text{ y } v = 1 \in \mathbb{Z}. \text{ Luego } u \cdot a + v \cdot 1 = 0 \cdot a + 1 \cdot 1 = 1. \end{aligned}$$

Asumamos ahora que

$$\forall b \in \mathbb{N}, b > 1, \quad P(k) \text{ es } V \text{ para todo } k < b.$$

Veamos que $P(b)$ es V. Dado $a \in \mathbb{Z}$, existen únicos $b', r \in \mathbb{Z}$ tales que

$$a = b' \cdot b + r, \quad 0 \leqslant r < b.$$

debido al algoritmo de la división (Teorema 6.4).

Ahora tenemos dos opciones.

- Si $r = 0$:

  $$\begin{aligned} &b \mid a \text{ pues } a = b' \cdot b \\ &b \mid b \text{ por Proposición 6.4-(a)} \\ &\text{Sean } u = 0 \in \mathbb{Z}, v = 1 \in \mathbb{Z}. \text{ Luego } u \cdot a + v \cdot b = 0 \cdot a + 1 \cdot b = b. \end{aligned}$$

  Por lo tanto basta tomar $d = b$.

- Si $r \neq 0$, entonces $1 \leqslant r < b$. Como $P(r)$ es V por hipótesis, existe $d \in \mathbb{N}$ tal que

  $$\begin{aligned} &d \mid b \text{ y } d \mid r, \\ &\exists x, y \in \mathbb{Z}: d = x \cdot b + y \cdot r. \end{aligned}$$

  Además,

  $$\left.\begin{array}{l} d \mid b \Rightarrow d \mid b' \cdot b \\ d \mid r \end{array}\right\} \Rightarrow \quad d \mid b' \cdot b + r \Rightarrow d \mid a$$

  Finalmente

  $$\begin{aligned} d &= x \cdot b + y \cdot r = x \cdot b + y \cdot (a - b' \cdot b) \\ &= x \cdot b - y \cdot b' \cdot b + y \cdot a \\ &= y \cdot a + (x - y \cdot b') \cdot b. \end{aligned}$$

  Juntando todo tenemos que:

  $$\begin{aligned} &d \mid a \text{ y } d \mid b, \\ &\text{Sean } u = y \in \mathbb{Z}, v = x - y \cdot b' \in \mathbb{Z} \text{ donde } d = u \cdot a + v \cdot b. \end{aligned}$$

Esto nos dice que $P(b)$ es V. Luego la proposición $\forall b \in \mathbb{N}, P(b)$ es V debido al Criterio 5.2.

Supongamos que $b < 0$, entonces $-b > 0$. Por lo demostrado anteriormente se tiene que existe $d \in \mathbb{N}$ tal que

$$\begin{aligned} &d \mid a \text{ y } d \mid -b, \\ &\exists u, v \in \mathbb{Z} : d = u \cdot a + v \cdot (-b), \end{aligned}$$

de donde se deduce que

$$\begin{aligned} &d \mid a \text{ y } d \mid b \text{ por Proposición 6.4-(i)} \\ &\exists u, v \in \mathbb{Z} : d = u \cdot a + (-v) \cdot b. \end{aligned}$$

Analizaremos ahora la unicidad.

Supongamos que existe $d' \in \mathbb{N}$ tal que

$$\begin{aligned} &d' \mid a \text{ y } d' \mid b, \\ &\exists u', v' \in \mathbb{Z} : d' = u' \cdot a + v' \cdot b. \end{aligned}$$

Ahora

$$\left.\begin{array}{lll} d \mid a & \Rightarrow & d \mid u' \cdot a \\ d \mid b & \Rightarrow & d \mid v' \cdot b \end{array}\right\} \begin{array}{ll} \Rightarrow & d \mid u' \cdot a + v' \cdot b \text{ por Proposición 6.4-(f)} \\ \Rightarrow & d \mid d' \\ \Rightarrow & d \leqslant d' \text{ por Proposición 6.5} \end{array}$$

Análogamente

$$\left.\begin{array}{lll} d' \mid a & \Rightarrow & d' \mid u \cdot a \\ d' \mid b & \Rightarrow & d' \mid v \cdot b \end{array}\right\} \begin{array}{ll} \Rightarrow & d' \mid u \cdot a + v \cdot b \text{ por Proposición 6.4-(f)} \\ \Rightarrow & d' \mid d \\ \Rightarrow & d' \leqslant d \text{ por Proposición 6.5} \end{array}$$

Por lo tanto $d = d'$. ■

La demostración del Teorema 6.5 nos sugiere una forma de encontrar el máximo común divisor, llamada el algoritmo de Euclides. A continuación veremos algunos ejemplos prácticos.

Ejemplo 6.5

(a) Hallar $(84, 45)$.

Primero usamos el algoritmo de la división:

$$84 = 45 \cdot 1 + 39.$$

Aquí el resto es 39 y es no nulo. De acuerdo a la demostración, $(84, 45) = (45, 39)$. Usamos de nuevo el algoritmo de la división pero ahora entre 45 y 39:

$$45 = 39 \cdot 1 + 6.$$

Aquí el resto es 6 y es no nulo. De acuerdo a la demostración, $(45, 39) = (39, 6)$. Usamos de nuevo el algoritmo de la división pero ahora entre 39 y 6:

$$39 = 6 \cdot 6 + 3.$$

Aquí el resto es 3 y es no nulo. De acuerdo a la demostración, $(39, 6) = (6, 3)$. Usamos de nuevo el algoritmo de la división pero ahora entre 6 y 3:

$$6 = 3 \cdot 2 + 0.$$

Como el resto es 0, de acuerdo a la demostración tenemos que $(6, 3) = 3$. Por lo tanto:

$$(84, 45) = (45, 39) = (39, 6) = (6, 3) = 3.$$

Si queremos encontrar los números $u, v \in \mathbb{Z}$ asociados al máximo común divisor, hacemos la siguiente cuenta:

$$\begin{aligned} 3 &= 39 - 6 \cdot 6 \text{ pues } 39 = 6 \cdot 6 + 3 \\ &= 39 - 6 \cdot (45 - 39 \cdot 1) = 7 \cdot 39 - 6 \cdot 45 \text{ pues } 45 = 39 \cdot 1 + 6 \\ &= 7 \cdot (84 - 45 \cdot 1) - 6 \cdot 45 = 7 \cdot 84 - 13 \cdot 45 \text{ pues } 84 = 45 \cdot 1 + 39 \\ &= 7 \cdot 84 + (-13) \cdot 45. \end{aligned}$$

(b) Hallar $(84, 78)$.

Usamos el algoritmo de la división hasta que el resto de cero:

$$\begin{aligned} 84 &= 78 \cdot 1 + 6 \\ 78 &= 6 \cdot 13 + 0 \end{aligned}$$

Por lo tanto $(84, 78) = 6$. Ahora:

$$\begin{aligned} 6 &= 84 - 78 \cdot 1 \\ &= 1 \cdot 84 + (-1) \cdot 78. \end{aligned}$$

(c) Hallar $(234, 129)$.

Usamos el algoritmo de la división hasta que el resto de cero:

$$\begin{aligned} 234 &= 129 \cdot 1 + 105 \\ 129 &= 105 \cdot 1 + 24 \\ 105 &= 24 \cdot 4 + 9 \\ 24 &= 9 \cdot 2 + 6 \\ 9 &= 6 \cdot 1 + 3 \\ 6 &= 3 \cdot 2 + 0 \end{aligned}$$

Por lo tanto $(234, 129) = 3$. Ahora:

$$\begin{aligned} 3 &= 9 - 6 \cdot 1 \text{ pues } 9 = 6 \cdot 1 + 3 \\ &= 9 - (24 - 9 \cdot 2) \cdot 1 = (-1) \cdot 24 + 9 \cdot 3 \text{ pues } 24 = 9 \cdot 2 + 6 \\ &= (-1) \cdot 24 + (105 - 24 \cdot 4) \cdot 3 = 3 \cdot 105 + 24 \cdot (-13) \text{ pues } 105 = 24 \cdot 4 + 9 \\ &= 3 \cdot 105 + (129 - 105 \cdot 1) \cdot (-13) = (-13) \cdot 129 + 105 \cdot 16 \text{ pues } 129 = 105 \cdot 1 + 24 \\ &= (-13) \cdot 129 + (234 - 129 \cdot 1) \cdot 16 \text{ pues } 234 = 129 \cdot 1 + 105 \\ &= 16 \cdot 234 + (-29) \cdot 129. \end{aligned}$$

Proposición 6.7
Sean $a, b \in \mathbb{Z}$ tales que $a \neq 0$ y $b \neq 0$. Entonces $(a, b) = (b, a)$.

Demostración.

Como $b \neq 0$ entonces (a, b) está bien definido. Análogamente, como $a \neq 0$ entonces (b, a) también está bien definido.

Si $d = (a, b)$, entonces

$$d \mid a \text{ y } d \mid b,$$
$$\exists u, v \in \mathbb{Z} : d = u \cdot a + v \cdot b.$$

Pero esto significa que

$$d \mid b \text{ y } d \mid a,$$
$$\exists u, v \in \mathbb{Z} : d = v \cdot b + u \cdot a.$$

Por unicidad del máximo común divisor tenemos que $d = (b, a)$. ■

Observación 6.6

La definición de máximo común divisor entre dos enteros a y b sólo está permitida cuando $b \neq 0$. Supongamos que ambos a y b son no simultáneamente nulos:

- *Si $b \neq 0$ el máximo común divisor entre a y b está bien definido.*
- *Si $b = 0$ (y por lo tanto $a \neq 0$) el máximo común divisor entre a y b se define como (b, a).*

El máximo común divisor entre 0 y 0 no está definido.

La denominación de máximo común divisor es debido a la siguiente proposición.

Proposición 6.8

Sean $a, b \in \mathbb{N}$. Si $k \in \mathbb{N}$ tal que $k \mid a$ y $k \mid b$ entonces $k \leqslant (a, b)$.

Demostración.

Por Teorema 6.5 se sigue que existen $u, v \in \mathbb{Z}$ tal que $(a, b) = u \cdot a + v \cdot b$. Ahora:

$$\left.\begin{array}{lll} k \mid a & \Rightarrow & k \mid u \cdot a \\ k \mid b & \Rightarrow & k \mid v \cdot b \end{array}\right\} \Rightarrow k \mid u \cdot a + v \cdot b \text{ por Proposición 6.4-(f)}$$
$$\Rightarrow k \mid (a, b)$$
$$\Rightarrow k \leqslant (a, b) \text{ por Proposición 6.5}$$

■

Como consecuencia de la Proposición 6.8, el máximo común divisor puede obtenerse realizando la descomposición de los dos números en factores primos y tomando los factores comunes elevados al menor exponente. Lamentablemente esta metodología no nos sirve para encontrar la combinación lineal entera y podría requerir más operaciones. Veamos nuevamente el ejemplo anterior.

Ejemplo 6.6

(a) Hallar $(84, 45)$.

84	2	45	3
42	2	15	3
21	3	5	5
7	7	1	
1			

Luego $84 = 2^2 \cdot 3 \cdot 7$ y $45 = 3^2 \cdot 5$, lo que implica que $(84, 45) = 3$.

(b) Hallar $(84, 78)$.

$$\begin{array}{r|l\quad r|l} 84 & 2 & 78 & 2 \\ 42 & 2 & 39 & 3 \\ 21 & 3 & 13 & 13 \\ 7 & 7 & 1 & \\ 1 & & & \end{array}$$

Luego $84 = 2^2 \cdot 3 \cdot 7$ y $78 = 2 \cdot 3 \cdot 13$, lo que implica que $(84, 78) = 2 \cdot 3 = 6$.

(c) Hallar $(234, 129)$.

$$\begin{array}{r|l\quad r|l} 234 & 2 & 129 & 3 \\ 117 & 3 & 43 & 43 \\ 39 & 3 & 1 & \\ 13 & 13 & & \\ 1 & & & \end{array}$$

Luego $234 = 2 \cdot 3^2 \cdot 13$ y $129 = 3 \cdot 43$, lo que implica que $(234, 129) = 3$.

Observación 6.7
Sean $a, b \in \mathbb{Z}$ no simultáneamente nulos y $d \in \mathbb{N}$ tal que $d = (a, b)$. Entonces la forma de escribir a d como combinación lineal entera de a y b no es única.

Demostración.
Sabemos por el Teorema 6.5 que existen $u, v \in \mathbb{Z}$ tal que

$$d = u \cdot a + v \cdot b.$$

Tomemos t un múltiplo de a y de b, es decir, $t = a \cdot h$ y $t = b \cdot r$ con $h, r \in \mathbb{Z}$ (una opción sería tomar $h = b$ y $r = a$). Luego

$$\begin{aligned} (u + h) \cdot a + (v - r) \cdot b &= u \cdot a + h \cdot a + v \cdot b - r \cdot b \\ &= u \cdot a + t + v \cdot b - t \\ &= u \cdot a + v \cdot b \\ &= d \end{aligned}$$

Por lo tanto la forma de escribir al máximo común divisor como combinación lineal entera de a y b no es única, cuando $h \neq 0$ o $r \neq 0$. ■

Ejemplo 6.7
(a) Recordemos el Ejemplo 6.5-(a). Se tenía que $(84, 45) = 3$ y que

$$3 = 7 \cdot 84 + (-13) \cdot 45.$$

Notemos que $t = 1260$ es un múltiplo de 84 y de 45 puesto que $1260 = 84 \cdot 15 = 45 \cdot 28$. En la nomenclatura de la Observación 6.7 tenemos que: $a = 84$, $b = 45$, $d = 3$, $u = 7$, $v = -13$, $h = 15$ y $r = 28$. Siguiendo los pasos de la Observación 6.7 se observa que:

$$(u + h) \cdot a + (v - r) \cdot b = u \cdot a + v \cdot b = d,$$

es decir,

$$22 \cdot 84 + (-41) \cdot 45 = 7 \cdot 84 + (-13) \cdot 45 = 3.$$

(b) Recordemos el Ejemplo 6.5-(b). Se tenía que $(84, 78) = 6$ y que

$$6 = 1 \cdot 84 + (-1) \cdot 78.$$

Notemos que $t = 1092$ es un múltiplo de 84 y de 78 puesto que $1092 = 84 \cdot 13 = 78 \cdot 14$. En la nomenclatura de la Observación 6.7 tenemos que: $a = 84$, $b = 78$, $d = 6$, $u = 1$, $v = -1$, $h = 13$ y $r = 14$. Siguiendo los pasos de la Observación 6.7 se observa que:

$$(u + h) \cdot a + (v - r) \cdot b = u \cdot a + v \cdot b = d,$$

es decir,

$$14 \cdot 84 + (-15) \cdot 78 = 1 \cdot 84 + (-1) \cdot 78 = 6.$$

(c) Recordemos el Ejemplo 6.5-(c). Se tenía que $(234, 129) = 3$ y que

$$3 = 16 \cdot 234 + (-29) \cdot 129.$$

Notemos que $t = 10062$ es un múltiplo de 234 y de 129 puesto que $10062 = 234 \cdot 43 = 129 \cdot 78$. En la nomenclatura de la Observación 6.7 tenemos que: $a = 234$, $b = 129$, $d = 3$, $u = 16$, $v = -29$, $h = 43$ y $r = 78$. Siguiendo los pasos de la Observación 6.7 se observa que:

$$(u + h) \cdot a + (v - r) \cdot b = u \cdot a + v \cdot b = d,$$

es decir,

$$59 \cdot 234 + (-107) \cdot 129 = 16 \cdot 234 + (-29) \cdot 129 = 3.$$

Definición 6.7
Sean $a, b \in \mathbb{Z}$ no simultáneamente nulos. Diremos que a y b son coprimos si $(a, b) = 1$.

Proposición 6.9
Sean $a, b \in \mathbb{Z}$ no simultáneamente nulos.

(a) Si existen $r, s \in \mathbb{Z}$ tales que $1 = r \cdot a + s \cdot b$ entonces $(a, b) = 1$.

(b) Si $d = (a, b)$ entonces $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Demostración.
(a) Supongamos que $d = (a, b)$. Luego,

$$\left.\begin{array}{rcl} d \mid a & \Rightarrow & d \mid r \cdot a \\ d \mid b & \Rightarrow & d \mid s \cdot b \end{array}\right\} \Rightarrow d \mid r \cdot a + s \cdot b \text{ por Proposición 6.4-(f)}$$
$$\Rightarrow d \mid 1$$
$$\Rightarrow d = 1 \text{ por Proposición 6.4-(e) y el hecho que } d \in \mathbb{N}$$

(b) Por Teorema 6.5 existen $r, s \in \mathbb{Z}$ tal que $d = r \cdot a + s \cdot b$. Dividiendo por d queda:

$$1 = r \cdot \frac{a}{d} + s \cdot \frac{b}{d},$$

donde $\frac{a}{d}, \frac{b}{d} \in \mathbb{Z}$. Por (a) se tiene que $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. ■

Proposición 6.10
Sean a y b coprimos. Si $t \in \mathbb{Z}$ satisface que $t \mid a$ y $t \mid b$, entonces $t = 1$ o $t = -1$.

Demostración.
Como a y b son coprimos, existen $u, v \in \mathbb{Z}$ tales que $u \cdot a + v \cdot b = 1$. Luego,

$$\left.\begin{array}{rcl} t \mid a & \Rightarrow & t \mid u \cdot a \\ t \mid b & \Rightarrow & t \mid v \cdot b \end{array}\right\} \Rightarrow t \mid u \cdot a + v \cdot b \text{ por Proposición 6.4-(f)}$$
$$\Rightarrow t \mid (a, b)$$
$$\Rightarrow t \mid 1$$
$$\Rightarrow t = 1 \text{ o } t = -1 \text{ por Proposición 6.4-(e)}$$ ■

Lo que dice la proposición anterior es que cuando dos números son coprimos, entonces no comparten divisores distintos a 1 y -1.

Lema 6.1
Sean $a, b, p, q \in \mathbb{Z}$ con $a \neq 0$, p y q primos.

(a) $(a, b) = |a|$ si y sólo si $a \mid b$.

(b) $(p, q) = 1$ si y sólo si $|p| \neq |q|$.

(c) $(a, p) = 1$ si y sólo si $p \nmid a$.

Demostración.
(a) Asumamos primero que $(a, b) = |a|$. Luego $|a| \mid b$ por definición de máximo común divisor. Por Proposición 6.4-(j) se tiene que $a \mid b$.

Asumamos ahora que $a \mid b$. Por Proposición 6.4-(a) se tiene que $|a| \mid a$. Además, como $a \mid b$ entonces $|a| \mid b$ por Proposición 6.4-(j). Por lo tanto, $|a| \leqslant (a, b)$ por Proposición 6.8. Por otro lado, como $(a, b) \mid a$ entonces $(a, b) \mid |a|$ por Proposición 6.4-(i). Esto dice que $(a, b) \leqslant |a|$ por Proposición 6.5. Por lo tanto, $(a, b) = |a|$.

(b) Los divisores de p son: 1, -1, p, $-p$.
Los divisores de q son: 1, -1, q, $-q$.
Ahora

$$\begin{aligned} (p, q) = 1 &\Leftrightarrow \{1, -1, p, -p\} \cap \{1, -1, q, -q\} = \{1, -1\} \\ &\Leftrightarrow |p| \neq |q| \,. \end{aligned}$$

(c) Como $(a, p) \mid p$ entonces $(a, p) = |p|$ o $(a, p) = 1$ (pues p es primo). Ahora:

$$\begin{aligned} a \text{ y } p \text{ no son coprimos} &\Leftrightarrow (a, p) = |p| \\ &\Leftrightarrow (p, a) = |p| \\ &\Leftrightarrow p \mid a \text{ por (a)} \end{aligned}$$ ■

Teorema 6.6
Sea $p \in \mathbb{Z}$, $p \neq 1$ y $p \neq -1$. Entonces p es primo si y sólo si toda vez que $p \mid a \cdot b$ con $a, b \in \mathbb{Z}$ ocurre que $p \mid a$ o $p \mid b$.

Demostración.

En virtud de la Observation 6.5 podemos pensar que $p > 0$.

Asumamos primero que p es primo. Sean $a, b \in \mathbb{Z}$ tales que $p \mid a \cdot b$. Si $p \mid a$ listo, de otro modo asumamos que $p \nmid a$. Por Lema 6.1-(c) tenemos que $(a, p) = 1$. Podemos afirmar entonces que existen $r, s \in \mathbb{Z}$ tales que:

$$1 = r \cdot a + s \cdot p,$$

y multiplicando ambos miembros por b se tiene que:

$$b = r \cdot a \cdot b + s \cdot p \cdot b.$$

Ahora:

$$\left.\begin{array}{rcl} p \mid a \cdot b & \Rightarrow & p \mid r \cdot a \cdot b \\ p \mid p & \Rightarrow & p \mid s \cdot p \cdot b \end{array}\right\} \Rightarrow p \mid r \cdot a \cdot b + s \cdot p \cdot b \text{ por Proposición 6.4-(f)}$$
$$\Rightarrow p \mid b$$

Asumamos ahora que toda vez que $p \mid a \cdot b$ con $a, b \in \mathbb{Z}$ ocurre que $p \mid a$ o $p \mid b$. Supongamos que p no es primo. Entonces existen $a, b \in \mathbb{N}$ tales que:

$$p = a \cdot b, \quad 1 < a < p, \quad 1 < b < p.$$

Luego se ve que $p \mid a \cdot b$, pero $p \nmid a$ y $p \nmid b$ por Proposición 6.5. Esto contradice la hipótesis, por lo que p debe ser primo. ■

Teorema 6.7

Sean $a, b, c \in \mathbb{Z}$. Entonces:

(a) Si $(a, b) = 1$, $a \mid c$ y $b \mid c$, entonces $a \cdot b \mid c$.

(b) Si $(a, c) = 1$ y $a \mid b \cdot c$, entonces $a \mid b$.

Demostración.

(a) Como $(a, b) = 1$ tenemos que existen $r, s \in \mathbb{Z}$ tales que:

$$1 = r \cdot a + s \cdot b.$$

Multiplicando por c ambos miembros tenemos que:

$$c = r \cdot c \cdot a + s \cdot c \cdot b.$$

Como $a \mid c$ entonces existe $a' \in \mathbb{Z}$ tal que $c = a' \cdot a$.

Como $b \mid c$ entonces existe $b' \in \mathbb{Z}$ tal que $c = b' \cdot b$.

Reemplazando obtenemos que:

$$\begin{array}{rcl} c & = & r \cdot b' \cdot b \cdot a + s \cdot a' \cdot a \cdot b \\ & = & (r \cdot b' + s \cdot a') \cdot a \cdot b. \end{array}$$

Esto último dice que $a \cdot b \mid c$.

(b) Como $(a, c) = 1$ existen $r, s \in \mathbb{Z}$ tales que

$$1 = r \cdot a + s \cdot c.$$

Multiplicando por b a ambos miembros:

$$b = r \cdot a \cdot b + s \cdot c \cdot b.$$

Ahora:

$$\left.\begin{array}{rcl} a \mid a & \Rightarrow & a \mid r \cdot a \cdot b \\ a \mid b \cdot c & \Rightarrow & a \mid s \cdot c \cdot b \end{array}\right\} \Rightarrow a \mid r \cdot a \cdot b + s \cdot c \cdot b$$
$$\Rightarrow a \mid b.$$ ■

Proposición 6.11
Sea $p \in \mathbb{N}$ primo. Entonces $\binom{p}{i}$ es divisible por p para $1 \leqslant i < p$.

Demostración.

Recordemos de la Definición 5.6 que

$$\binom{p}{i} = \frac{p \cdot (p-1) \cdot \ldots \cdot (p-(i-1))}{i!}$$

Veamos que si $1 \leqslant i < p$ entonces $(p, i!) = 1$. En efecto, llamando $d = (p, i!)$ se tiene que $d \mid p$ y $d \mid i!$. Luego, como $d \mid p$ y p es primo, tenemos solamente dos opciones: $d = 1$ o $d = p$. Si $d = 1$ listo, caso contrario, asumamos que $d = p$. Como también $d \mid i!$, el Teorema 6.6 nos dice que $p \mid i$ o $p \mid i-1$ o $\ldots$ o $p \mid 1$, pero esto es una contradicción debido a la Proposición 6.5.

Como

$$\binom{p}{i} \cdot i! = p \cdot (p-1) \cdot \ldots \cdot (p-(i-1)),$$

tenemos que $p \mid \binom{p}{i} \cdot i!$ (notar que es necesario pedir que $i \geqslant 1$ pues $\binom{p}{0} \cdot 0! = 1$). Pero como $(p, i!) = 1$, el Teorema 6.7-(b) nos asegura que $p \mid \binom{p}{i}$. ■

6.8. Mínimo común múltiplo

Consideremos $a, b \in \mathbb{Z}$ donde $a \neq 0$ y $b \neq 0$. Entonces $a \cdot b$ y $-a \cdot b$ son múltiplos de a y de b. Esto significa que a y b tienen al menos un múltiplo común positivo. Sea:

$$H = \{x \in \mathbb{N} : x \text{ es múltiplo de } a \text{ y de } b\}.$$

Por lo comentado anteriormente, $H \subset \mathbb{N}$ y $H \neq \varnothing$. Por Teorema 5.19 se tiene que H posee elemento minimal que llamaremos m. El número m cumple las siguientes propiedades:

- m es múltiplo de a y de b.
- $m \in \mathbb{N}$.
- Si $k \in \mathbb{N}$ y k es múltiplo de a y de b, entonces $m \leqslant k$.

Definición 6.8
Dados $a, b \in \mathbb{Z}$ no nulos. El elemento minimal del conjunto

$$H = \{x \in \mathbb{N} : x \text{ es múltiplo de } a \text{ y de } b\}.$$

se denomina el mínimo común múltiplo (m.c.m) de a y de b, y se denota por $[a, b]$. Si $a = 0$ o $b = 0$ se define $[a, b] = 0$.

Ejemplo 6.8

(a) Hallar $[8, 14]$:

Escribamos los múltiplos positivos de 8 y 14 y hallemos el primero que es común a ambos:

$$\begin{aligned} \text{múltiplos positivos de } 8: &\quad 8, 16, 24, 32, 40, 48, \boxed{56}, \ldots, \\ \text{múltiplos positivos de } 14: &\quad 14, 28, 42, \boxed{56}, 70, \ldots. \end{aligned}$$

Por lo tanto, $[8, 14] = 56$.

(b) Hallar $[12, 18]$:

Escribamos los múltiplos positivos de 12 y 18 y hallemos el primero que es común a ambos:

$$\begin{aligned} &\text{múltiplos positivos de } 12: && 12, 24, \boxed{36}, 48, \ldots, \\ &\text{múltiplos positivos de } 18: && 18, \boxed{36}, 54, \ldots. \end{aligned}$$

Por lo tanto, $[12, 18] = 36$.

Proposición 6.12
Sean $a, b \in \mathbb{Z}$ tales que $a \neq 0$ y $b \neq 0$. Si $k \in \mathbb{Z}$ satisface que $a \mid k$ y $b \mid k$ entonces $[a, b] \mid k$.

Demostración.
Por Definición 6.8 se tiene que $[a, b] \in \mathbb{N}$. Por el algoritmo de la división existen $q, r \in \mathbb{Z}$ tales que:

$$k = [a, b] \cdot q + r, \quad 0 \leqslant r < [a, b].$$

Ahora

$$\left.\begin{array}{l} a \mid k \\ a \mid [a, b] \Rightarrow a \mid [a, b] \cdot q \end{array}\right\} \begin{array}{ll} \Rightarrow & a \mid k - [a, b] \cdot q \text{ por Proposición 6.4-(f)} \\ \Rightarrow & a \mid r. \end{array}$$

Análogamente

$$\left.\begin{array}{l} b \mid k \\ b \mid [a, b] \Rightarrow b \mid [a, b] \cdot q \end{array}\right\} \begin{array}{ll} \Rightarrow & b \mid k - [a, b] \cdot q \text{ por Proposición 6.4-(f)} \\ \Rightarrow & b \mid r. \end{array}$$

Luego r es un múltiplo común de a y de b, pero $r < [a, b]$. Como $[a, b]$ es el múltiplo común más pequeño, la única posibilidad es que $r = 0$. Esto significa que $[a, b] \mid k$. ■

Teorema 6.8
Sean $a, b \in \mathbb{N}$. Entonces $a \cdot b = (a, b) \cdot [a, b]$.

Demostración.
Como $(a, b) \mid a$ entonces $(a, b) \mid a \cdot b$. Luego, existe $m \in \mathbb{N}$ tal que

$$m = \frac{a \cdot b}{(a, b)}.$$

Veamos primero que $[a, b] \mid m$.

$$\begin{aligned} (a, b) \mid a &\Rightarrow \exists x \in \mathbb{Z} : a = x \cdot (a, b) \Rightarrow m = \frac{a}{(a, b)} \cdot b = x \cdot b. \\ (a, b) \mid b &\Rightarrow \exists y \in \mathbb{Z} : b = y \cdot (a, b) \Rightarrow m = a \cdot \frac{b}{(a, b)} = a \cdot y. \end{aligned}$$

Por lo tanto m es múltiplo de a y de b. Por Proposición 6.12 se tiene que $[a, b] \mid m$.

Veamos ahora que $m \mid [a, b]$. Sabemos que existen $r, s \in \mathbb{Z}$ tales que $(a, b) = r \cdot a + s \cdot b$. Entonces

$$(a, b) = r \cdot a + s \cdot b \Rightarrow 1 = r \cdot \frac{a}{(a, b)} + s \cdot \frac{b}{(a, b)}$$

$$\Rightarrow \quad [a,b] = r \cdot \frac{a}{(a,b)} \cdot [a,b] + s \cdot \frac{b}{(a,b)} \cdot [a,b]$$

Además:

$$\begin{aligned} a \mid [a,b] &\Rightarrow \exists a' \in \mathbb{Z} : [a,b] = a \cdot a' \\ b \mid [a,b] &\Rightarrow \exists b' \in \mathbb{Z} : [a,b] = b \cdot b' \end{aligned}$$

Reemplazando:

$$\begin{aligned} [a,b] &= r \cdot \frac{a}{(a,b)} \cdot [a,b] + s \cdot \frac{b}{(a,b)} \cdot [a,b] \\ &= r \cdot \frac{a}{(a,b)} \cdot b \cdot b' + s \cdot \frac{b}{(a,b)} \cdot a \cdot a' \\ &= r \cdot \frac{a \cdot b}{(a,b)} \cdot b' + s \cdot \frac{a \cdot b}{(a,b)} \cdot a' \\ &= r \cdot m \cdot b' + s \cdot m \cdot a' \\ &= m \cdot (r \cdot b' + s \cdot a') \,. \end{aligned}$$

Esto dice que $m \mid [a,b]$.

Como $m, [a,b] \in \mathbb{N}$, $[a,b] \mid m$ y $m \mid [a,b]$ se tiene la igualdad expresada en el enunciado debido a la Proposición 6.4-(d). ■

Corolario 6.2
Sean $a, b \in \mathbb{N}$ coprimos. Entonces $[a,b] = a \cdot b$.

6.9. Teorema fundamental de la Aritmética

Teorema 6.9 (Teorema fundamental de la Aritmética)
Sea $n \in \mathbb{Z}$ tal que $n \neq 0, -1, 1$. Entonces existe un conjunto finito de primos $p_1, \ldots, p_k$ tales que $0 < p_1 \leqslant \ldots \leqslant p_k$ y

$$n = c \cdot p_1 \ldots p_k,$$

donde $c = 1$ o $c = -1$. La forma anterior de expresar a n es única.

Demostración.

Sin pérdida de generalidad podemos asumir que $n \in \mathbb{N}$ con $n > 1$.

Analicemos primero la existencia de la descomposición.

Razonemos por el absurdo y asumamos que el teorema es falso. Esto significa que existe al menos un número natural $n > 1$ que no admite una representación como producto de primos. Sea

$$H = \{x \in \mathbb{N} : x > 1 \text{ y } x \text{ no admite representación como producto de factores primos}\} \,.$$

Como $H \neq \varnothing$ (pues $n \in H$) y $H \subset \mathbb{N}$, entonces existe un elemento minimal en H que llamaremos m (pues $\mathbb{N}$ es bien ordenado). Claramente m no puede ser primo (de otro modo él sería su propia representación y esto no puede suceder pues $m \in H$). Como $m > 1$ entonces m es divisible por algún primo positivo q por Teorema 6.2. Sea

$$L = \{x \in \mathbb{N} : x \text{ es primo y } x \mid m\} \,.$$

Como $L \neq \varnothing$ (pues $q \in L$) y $L \subset \mathbb{N}$ se tiene que L tiene primer elemento que llamaremos p_1 (pues $\mathbb{N}$ es bien ordenado). Luego existe $m' \in \mathbb{N}$ tal que $m = p_1 \cdot m'$ (con lo cual también se tiene que $m' \mid m$). Como m no es primo, se sigue entonces que $m' > 1$. Además también tenemos que $m' < m$

por Proposición 6.5 y porque $p_1 > 1$. Luego este teorema es válido para m', es decir, existen primos positivos $p_2, \ldots, p_k$ tales que $p_2 \leqslant \ldots \leqslant p_k$ tales que $m' = p_2 \cdot \ldots \cdot p_k$. Esto dice que, en particular, $p_2 \mid m'$ (y por lo tanto $p_2 \mid m$), por lo que $p_2 \in L$. Luego $p_1 \leqslant p_2$, pues p_1 es elemento minimal de L. Por lo tanto tenemos que

$$m = p_1 \cdot m' = p_1 \cdot p_2 \cdot \ldots \cdot p_k, \quad p_1 \leqslant p_2 \leqslant \ldots \leqslant p_k,$$

por lo cual m admite una representación como producto de factores primos, que es una contradicción.

Analicemos ahora la unicidad de la representación. Supongamos que

$$\begin{aligned} n &= p_1 \cdot \ldots \cdot p_k, \quad 0 < p_1 \leqslant \ldots \leqslant p_k, \quad p_1, \ldots, p_k \text{ primos} \\ n &= q_1 \cdot \ldots \cdot q_t, \quad 0 < q_1 \leqslant \ldots \leqslant q_t, \quad q_1, \ldots, q_t \text{ primos} \end{aligned}$$

Probaremos que la representación es única utilizando inducción en k.

Si $k = 1$ entonces $t = 1$, de otro modo p_1 tendría mas de cuatro divisores, y entonces la unicidad quedaría probada. Supongamos que la unicidad está garantizada para k y vamos a probar para $k+1$. Tenemos entonces:

$$p_1 \cdot \ldots \cdot p_k \cdot p_{k+1} = q_1 \cdot \ldots \cdot q_t.$$

Luego tenemos que $p_1 \mid q_1 \cdot \ldots \cdot q_t$. Por Teorema 6.6 ocurre que $p_1 \mid q_j$ para algún $j = 1, \ldots, t$. Pero como p_1 y q_j son primos positivos debe pasar que

$$p_1 = q_j.$$

Análogamente, tenemos que $q_1 \mid p_1 \cdot \ldots \cdot p_{k+1}$. Por Teorema 6.6 ocurre que $q_1 \mid p_h$ para algún $h = 1, \ldots, k+1$. Pero como q_1 y p_h son primos positivos debe pasar que

$$q_1 = p_h.$$

Si ocurriese que $q_j > q_1$ tendríamos que

$$p_1 \leqslant p_h = q_1 < q_j = p_1,$$

lo que nos diría que $p_1 < p_1$ que es una contradicción. Por esto podemos afirmar que $q_1 = q_j$, y por lo tanto $p_1 = q_1$. Con lo cual:

$$p_2 \cdot \ldots \cdot p_{k+1} = q_2 \cdot \ldots \cdot \cdot q_t.$$

Ahora el miembro de la izquierda consta de k factores primos. Usando la hipótesis inductiva aseguramos que $k = t - 1$, con lo que $t = k + 1$ (esto significa que la cantidad de factores primos es la misma en ambos lados de la igualdad). Además,

$$\begin{aligned} p_1 &= q_1, \\ p_2 &= q_2, \\ &\vdots \\ p_{k+1} &= q_t. \end{aligned}$$

De esta manera queda demostrada la unicidad. ■

Ejemplo 6.9
Veamos los siguientes ejemplos de aplicación del Teorema fundamental de la Aritmética.

(a) No existen $m, n \in \mathbb{Z}$ no nulos tales que $m^2 = 15 \cdot n^2$.

Asumamos que existen $m, n \in \mathbb{Z}$ no nulos tales que $m^2 = 15 \cdot n^2$. Debido a la regla de los signos podemos asumir que $m, n \in \mathbb{N}$.

Si ocurre que $m = 1$ entonces tendríamos que $1 = 15 \cdot n^2$, lo cual es una contradicción pues diría que 15 es inversible en $\mathbb{Z}$ y habíamos visto antes que los únicos enteros inversibles en $\mathbb{Z}$ son 1 y -1. Podemos suponer de aquí en adelante que $m \neq 1$.

Si ocurre que $n = 1$ entonces $m^2 = 15$. Por el Teorema 6.9, sea $m = p_1 \cdot \ldots \cdot p_k$ la descomposición de m en factores primos. Entonces:

$$15 = m^2 = (p_1 \cdot \ldots \cdot p_k) \cdot (p_1 \cdot \ldots \cdot p_k) = p_1^2 \cdot \ldots \cdot p_k^2.$$

Esto significa que cada primo aparece dos veces en la descomposición. Sin embargo, sabemos que $15 = 3 \cdot 5$, y 3 aparece sólo una vez. Esto es una contradicción, por lo que podemos asumir de ahora en adelante que $m \neq 1$ y $n \neq 1$.

Supongamos que m y n tienen las siguientes descomposiciones en factores primos:

$$\begin{aligned} m &= p_1 \cdot \ldots \cdot p_k, \\ n &= q_1 \cdot \ldots \cdot q_h. \end{aligned}$$

Entonces de la igualdad $m^2 = 15 \cdot n^2$ obtenemos

$$p_1^2 \cdot \ldots \cdot p_k^2 = 3 \cdot 5 \cdot q_1^2 \cdot \ldots \cdot q_h^2,$$

pero esta igualdad contradice el Teorema 6.9 pues 3 aparece un número par de veces del lado izquierdo, pero un número impar de veces del lado derecho.

(b) No existen $m, n \in \mathbb{Z}$ no nulos tales que $m^2 = 2 \cdot n^2$.

Asumamos que existen $m, n \in \mathbb{Z}$ no nulos tales que $m^2 = 2 \cdot n^2$. Debido a la regla de los signos podemos asumir que $m, n \in \mathbb{N}$.

Si ocurre que $m = 1$ entonces tendríamos que $1 = 2 \cdot n^2$, lo cual es una contradicción pues diría que 2 es inversible en $\mathbb{Z}$ y habíamos visto antes que los únicos enteros inversibles en $\mathbb{Z}$ son 1 y -1. Podemos suponer de aquí en adelante que $m \neq 1$.

Si ocurre que $n = 1$ entonces $m^2 = 2$. Por el Teorema 6.9, sea $m = p_1 \cdot \ldots \cdot p_k$ la descomposición de m en factores primos. Entonces:

$$2 = m^2 = (p_1 \cdot \ldots \cdot p_k) \cdot (p_1 \cdot \ldots \cdot p_k) = p_1^2 \cdot \ldots \cdot p_k^2.$$

Esto significa que cada primo aparece dos veces en la descomposición. Sin embargo, sabemos que 2 aparece sólo una vez. Esto es una contradicción, por lo que podemos asumir de ahora en adelante que $m \neq 1$ y $n \neq 1$.

Supongamos que m y n tienen las siguientes descomposiciones en factores primos:

$$\begin{aligned} m &= p_1 \cdot \ldots \cdot p_k, \\ n &= q_1 \cdot \ldots \cdot q_h. \end{aligned}$$

Entonces de la igualdad $m^2 = 2 \cdot n^2$ obtenemos

$$p_1^2 \cdot \ldots \cdot p_k^2 = 2 \cdot q_1^2 \cdot \ldots \cdot q_h^2,$$

pero esta igualdad contradice el Teorema 6.9 pues 2 aparece un número par de veces del lado izquierdo, pero un número impar de veces del lado derecho.

Si tenemos que $m \in \mathbb{N}$ con $m > 1$, llamemos $p_1, \ldots, p_s$ los primos distintos que aparecen en la factorización de m. Entonces:

$$m = p_1^{t_1} \cdot \ldots \cdot p_s^{t_s}, \quad p_1 < \ldots < p_s.$$

De esta manera, dado $n \in \mathbb{N}$ con $n > 1$ ocurre que $n \mid m$ si y sólo si

$$n = p_1^{i_1} \cdot \ldots \cdot p_s^{i_s}, \quad 0 \leqslant i_j \leqslant t_j, \quad j = 1, \ldots, s.$$

Esto nos dice que la cantidad de divisores positivos es:

$$(t_1 + 1) \cdot \ldots \cdot (t_s + 1)\,.$$

6.10. Potenciación entera de números reales

Definición 6.9 (Potenciación entera)
Sea $a \in \mathbb{R}$ tal que $a \neq 0$. Se define para todo $m \in \mathbb{Z}$ la potencia $a^m \in \mathbb{R}$ como sigue:

$$a^m = \begin{cases} a^m, & \text{si } m > 0 \text{ (como en la Sección 5.5)}, \\ 1, & \text{si } m = 0, \\ (a^{-m})^{-1}, & \text{si } m < 0. \end{cases}$$

Notar que de la definición de potenciación entera, la potencia -1 coincide con el inverso, pues:

$$\begin{aligned} a \text{ elevado a la } -1 &= a^{-1} = \left(a^{-(-1)}\right)^{-1} \text{ por Definición 6.9} \\ &= \left(a^1\right)^{-1} \text{ por Definición 6.9} \\ &= a^{-1} = \text{ inverso de } a. \end{aligned}$$

Hasta ahora la potencia -1 y el inverso eran cosas distintas conceptualmente. Como se escriben igual, lo razonable es que sean iguales, y es lo que sucede realmente. De ahora en más no haremos más la distinción conceptual.

Teorema 6.10
Sean $a, b \in \mathbb{R}$ no nulos y $r, s \in \mathbb{Z}$. Entonces

(a) $a^r \cdot a^s = a^{r+s}$.

(b) $(a^r)^s = a^{r \cdot s}$.

(c) $\dfrac{a^r}{a^s} = a^{r-s}$.

(d) $(a \cdot b)^r = a^r \cdot b^r$.

(e) $\left(\dfrac{a}{b}\right)^r = \dfrac{a^r}{b^r}$.

Demostración.
(a) Si $r \geqslant 0$ y $s \geqslant 0$ ver Proposición 5.3-(a).
Si $r < 0$ y $s < 0$ entonces

$$\begin{aligned} a^r \cdot a^s &= \left(a^{-r}\right)^{-1} \cdot \left(a^{-s}\right)^{-1} \text{ por Definición 6.9} \\ &= \frac{1}{a^{-r}} \cdot \frac{1}{a^{-s}} \text{ por Definición 4.3} \end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{a^{-r}\cdot a^{-s}} \text{ por Teorema 4.6-(f)}\\
&= \frac{1}{a^{-r-s}} \text{ por Proposición 5.3-(a)}\\
&= \frac{1}{a^{-(r+s)}}\\
&= a^{r+s} \text{ pues } r+s<0 \text{ y Definición 6.9.}
\end{aligned}
$$

Asumamos que $r = 0$ y $s < 0$.

$$
\begin{aligned}
a^r \cdot a^s &= a^0 \cdot a^s = 1 \cdot a^s = a^s = a^{0+s}\\
&= a^{r+s}.
\end{aligned}
$$

Asumamos que $r > 0$ y $s < 0$. Demostraremos el resultado por inducción en r. Supongamos que $r = 1$. Asumamos primero que $s = -1$:

$$
\begin{aligned}
a^r \cdot a^s &= a^1 \cdot a^{-1} = 1 \text{ por comentario posterior a la Definición 6.9}\\
&= a^0 = a^{1+(-1)}\\
&= a^{r+s}.
\end{aligned}
$$

Si $s \leqslant -2$ entonces

$$
\begin{aligned}
a^r \cdot a^s &= a^1 \cdot \left(a^{-s}\right)^{-1} \text{ por Definición 6.9}\\
&= a \cdot \frac{1}{a^{-s}} \text{ por Definición 4.3}\\
&= \frac{a}{a^{-s}} \text{ por Teorema 4.6-(f)}\\
&= \frac{1}{a^{-s-1}} \text{ pues } a\cdot a^{-s-1} = a^{-s}\cdot 1 \text{ y por Teorema 4.6-(e)}\\
&= \frac{1}{a^{-(s+1)}}\\
&= a^{s+1} \text{ por Definición 6.9 pues } s+1<0\\
&= a^{1+s}\\
&= a^{r+s}.
\end{aligned}
$$

Ahora supongamos que vale $a^r \cdot a^s = a^{r+s}$ y probemos que $a^{r+1} \cdot a^s = a^{r+1+s}$.

$$
\begin{aligned}
a^{r+1} \cdot a^s &= a \cdot a^r \cdot a^s \text{ por Proposición 5.3-(a)}\\
&= a \cdot a^{r+s} \text{ por hipótesis inductiva}\\
&= a^{1+r+s} \text{ si } r+s \geqslant 0 \text{ ya se ha demostrado en la Proposición 5.3-(a)}\\
&\qquad \text{si } r+s<0, \text{ también vale cuando el exponente del factor de la izquierda es 1}\\
&= a^{r+1+s}.
\end{aligned}
$$

Finalmente falta considerar el caso cuando $r < 0$ y $s \geqslant 0$.

$$
\begin{aligned}
a^r \cdot a^s &= a^s \cdot a^r\\
&= a^{s+r} \text{ por casos anteriores}\\
&= a^{r+s}.
\end{aligned}
$$

(b) Si $r \geqslant 0$ y $s \geqslant 0$ ver Proposición 5.3-(b).

Si $r = 0$ y $s < 0$:

$$\begin{aligned}
(a^r)^s &= \left(a^0\right)^s \\
&= 1^s \\
&= \left(1^{-s}\right)^{-1} \text{ por Definición 6.9} \\
&= 1^{-1} \text{ pues } -s \in \mathbb{N} \\
&= 1 \\
&= a^0 \\
&= a^{0\cdot s} \\
&= a^{r\cdot s}
\end{aligned}$$

Si $r > 0$ y $s < 0$:

$$\begin{aligned}
(a^r)^s &= \left[(a^r)^{-s}\right]^{-1} \text{ por Definición 6.9} \\
&= \left(a^{r\cdot(-s)}\right)^{-1} \text{ por Proposición 5.3-(i)} \\
&= \left(a^{-r\cdot s}\right)^{-1} \\
&= a^{r\cdot s} \text{ por Definición 6.9}
\end{aligned}$$

Si $r < 0$ y $s = 0$:

$$\begin{aligned}
(a^r)^s &= (a^r)^0 \\
&= 1 \\
&= a^0 \\
&= a^{r\cdot 0} \\
&= a^{r\cdot s}
\end{aligned}$$

Si $r < 0$ y $s > 0$:

$$\begin{aligned}
(a^r)^s &= \left[\left(a^{-r}\right)^{-1}\right]^s \text{ por Definición 6.9} \\
&= \left[\left(a^{-r}\right)^s\right]^{-1} \text{ por Proposición 5.3-(i)} \\
&= \left[a^{(-r)\cdot s}\right]^{-1} \text{ por Proposición 5.3-(b)} \\
&= \left(a^{-r\cdot s}\right)^{-1} \\
&= a^{r\cdot s} \text{ por Definición 6.9}
\end{aligned}$$

Si $r < 0$ y $s < 0$:

$$\begin{aligned}
(a^r)^s &= \left[\left(a^{-r}\right)^{-1}\right]^s \text{ por Definición 6.9} \\
&= \left\{\left[\left(a^{-r}\right)^{-1}\right]^{-s}\right\}^{-1} \text{ por Definición 6.9} \\
&= \left\{\left[\left(a^{-r}\right)^{-1}\right]^{-1}\right\}^{-s} \text{ por Proposición 5.3-(i)} \\
&= \left(a^{-r}\right)^{-s} \\
&= a^{(-r)\cdot(-s)} \text{ por Proposición 5.3-(b)}
\end{aligned}$$

$$= a^{r\cdot s}$$

(c)

$$\begin{aligned}
\frac{a^r}{a^s} &= a^r \cdot (a^s)^{-1} \text{ por Definición 4.3} \\
&= a^r \cdot a^{s\cdot(-1)} \text{ por (b)} \\
&= a^r \cdot a^{-s} \\
&= a^{r+(-s)} \text{ por (a)} \\
&= a^{r-s} \text{ por (a)}
\end{aligned}$$

(d) Si $r \geqslant 0$ ver Proposición 5.3-(c).
Si $r < 0$:

$$\begin{aligned}
(a\cdot b)^r &= \left[(a\cdot b)^{-r}\right]^{-1} \text{ por Definición 6.9} \\
&= \left(a^{-r}\cdot b^{-r}\right)^{-1} \text{ por Proposición 5.3-(c)} \\
&= \left(a^{-r}\right)^{-1}\cdot\left(b^{-r}\right)^{-1} \text{ por Teorema 4.5-(x)} \\
&= a^r\cdot b^r \text{ por Definición 6.9}
\end{aligned}$$

(e)

$$\begin{aligned}
\left(\frac{a}{b}\right)^r &= \left(a\cdot b^{-1}\right)^r \text{ por Definición 4.3} \\
&= a^r\cdot\left(b^{-1}\right)^r \text{ por (d)} \\
&= a^r\cdot b^{(-1)\cdot r} \text{ por (b)} \\
&= a^r\cdot b^{r\cdot(-1)} \\
&= a^r\cdot(b^r)^{-1} \text{ por (b)} \\
&= \frac{a^r}{b^r} \text{ por Definición 4.3}
\end{aligned}$$

Esto concluye la prueba. ■

6.11. Desarrollos s–ádicos

Teorema 6.11 (Desarrollo s–ádico)
Sea $s \in \mathbb{N}$ con $s > 1$. Dado $n \in \mathbb{N}$ existe una única expresión, llamada el desarrollo s–ádico de n del tipo:

$$n = \sum_{i=0}^{t} a_i \cdot s^i, \quad a_i \in \mathbb{Z}, \quad 0 \leqslant a_i < s, \quad i = 0, \ldots, t, \quad a_t \neq 0.$$

En este caso, diremos que $(a_t \ldots a_0)_s$ es la expresión de n en base s.

Demostración.
Analicemos primero la existencia.
Probaremos la existencia por inducción en n.
Si $n = 1$, notemos que $1 = 1 \cdot s^0$, por lo que podemos definir $t = 0$, $a_0 = 1 \in \mathbb{Z}$ con $0 < a_0 < s$.

Asumamos que el teorema ha sido probado para todos los enteros positivos menores que n.

Veamos que el teorema vale para n.

Si $n < s$ notemos que $n = n \cdot s^0$, por lo que podemos definir $t = 0$, $a_0 = n$. Luego se cumple $0 < a_0 < s$.

Si $n = s$ notemos que $n = 0 \cdot s^0 + 1 \cdot s^1$ por lo que podemos definir $t = 1$, $a_0 = 0$, $a_1 = 1$. Luego se cumple $0 \leqslant a_0 < s$ y $0 < a_1 < s$.

Si $n > s$ usamos el algoritmo de la división, por lo que existen $q, r \in \mathbb{Z}$ tales que:

$$n = s \cdot q + r, \quad 0 \leqslant r < s.$$

Como $n > s$ obtenemos que $q > 0$. Luego

$$\begin{aligned} q &< q \cdot s \text{ pues } s > 1 \\ &\leqslant q \cdot s + r \text{ pues } r \geqslant 0 \\ &= n. \end{aligned}$$

Por hipótesis inductiva el teorema vale para q, es decir,

$$q = \sum_{i=0}^{l} a_i \cdot s^i, \quad a_i \in \mathbb{Z}, \quad 0 \leqslant a_i < s, \quad i = 0, \ldots, l, \quad a_l \neq 0.$$

Ahora

$$\begin{aligned} n &= s \cdot q + r \\ &= s \cdot \sum_{i=0}^{l} a_i \cdot s^i + r \\ &= \sum_{i=0}^{l} a_i \cdot s^{i+1} + r \\ &= a_l s^{l+1} + \ldots + a_0 \cdot s + r. \end{aligned}$$

Notar que esta es una expresión s–ádica de n. Esto garantiza la existencia del desarrollo para cada número natural.

Analicemos la unicidad.

Supongamos que tenemos dos descomposiciones para n:

$$\begin{aligned} n &= \sum_{i=0}^{t} a_i \cdot s^i, \quad a_i \in \mathbb{Z}, \quad 0 \leqslant a_i < s, \quad i = 0, \ldots, t, \quad a_t \neq 0, \\ n &= \sum_{j=0}^{h} b_j \cdot s^j, \quad b_j \in \mathbb{Z}, \quad 0 \leqslant b_j < s, \quad j = 0, \ldots, h, \quad b_h \neq 0. \end{aligned}$$

O sea que:

$$\sum_{i=0}^{t} a_i \cdot s^i = \sum_{j=0}^{h} b_j \cdot s^j.$$

Probemos la unicidad por inducción en el número de sumandos del lado izquierdo.

Cuando tenemos un sumando del lado izquierdo, es decir $t = 0$, se tiene que:

$$a_0 = \sum_{j=0}^{h} b_j \cdot s^j = b_0 + s \cdot \sum_{j=1}^{h} b_j \cdot s^{j-1}.$$

Tenemos dos casos:

- Si $a_0 \leqslant b_0$:

$$(b_0 - a_0) + s \cdot \sum_{j=1}^{h} b_j \cdot s^{j-1} = 0.$$

donde $0 \leqslant b_0 - a_0 < b_0 < s$. Por el algoritmo de la división (unicidad del cociente y el resto) se tiene que $a_0 = b_0$ y

$$\sum_{j=1}^{h} b_j \cdot s^{j-1} = 0.$$

Como cada sumando es no negativo y la suma es igual a cero, resulta que $b_j \cdot s^{j-1} = 0$ para $j = 1, \ldots, h$. Esto significa que $b_j = 0$ para cada $j = 1, \ldots, h$. Luego $h = 0$ y queda probada la unicidad para este caso.

- Si $a_0 > b_0$:

$$(a_0 - b_0) + s \cdot \sum_{j=1}^{h} (-b_j) \cdot s^{j-1} = 0.$$

donde $0 < a_0 - b_0 \leqslant a_0 < s$. Por el algoritmo de la división (unicidad del cociente y el resto) se tiene que $a_0 = b_0$ y

$$\sum_{j=1}^{h} (-b_j) \cdot s^{j-1} = 0.$$

Pasando de miembro tenemos que

$$\sum_{j=1}^{h} b_j \cdot s^{j-1} = 0.$$

Como cada sumando es no negativo y la suma es igual a cero, resulta que $b_j \cdot s^{j-1} = 0$ para $j = 1, \ldots, h$. Esto significa que $b_j = 0$ para cada $j = 1, \ldots, h$. Luego $h = 0$ y queda probada la unicidad para este caso.

Asumamos ahora que la unicidad ha sido probada cuando en el lado izquierdo tenemos k sumandos, es decir, $t = k - 1$.

Veamos que el teorema vale cuando en el lado izquierdo tenemos $k + 1$ sumandos, es decir, $t = k$. Luego, acomodando las sumas se obtiene

$$s \cdot \left(\sum_{i=1}^{k} a_i \cdot s^{i-1} \right) + a_0 = s \cdot \left(\sum_{j=1}^{h} b_j \cdot s^{j-1} \right) + b_0.$$

Como $0 \leqslant a_0 < s$ y $0 \leqslant b_0 < s$, se sigue del algoritmo de la división (unicidad del cociente y el resto) que:

$$a_0 = b_0, \quad \sum_{i=1}^{k} a_i \cdot s^{i-1} = \sum_{j=1}^{h} b_j \cdot s^{j-1}.$$

Por hipótesis inductiva, $k = h$ y $a_j = b_j$ con $j = 1, \ldots, k$. Esto concluye la prueba de la unicidad. ■

Nosotros representamos los números en base 10, es decir, cuando representamos los números estamos usando intrínsecamente el desarrollo 10-ádico. De esta manera:

$$2351 = 2 \cdot 10^3 + 3 \cdot 10^2 + 5 \cdot 10^1 + 1 \cdot 10^0,$$

donde tenemos 2 unidades de mil, 3 centenas, 5 decenas y 1 unidad.

Ejemplo 6.10

(a) Transformar el número 2351 a base 5 (realizar el desarrollo 5-ádico).

$$\begin{aligned} 2351 &= 470 \cdot 5 + 1 = (94 \cdot 5 + 0) \cdot 5 + 1 \cdot 5^0 \\ &= 94 \cdot 5^2 + 0 \cdot 5^1 + 1 \cdot 5^0 = (18 \cdot 5 + 4) \cdot 5^2 + 0 \cdot 5^1 + 1 \cdot 5^0 \\ &= 18 \cdot 5^3 + 4 \cdot 5^2 + 0 \cdot 5^1 + 1 \cdot 5^0 = (3 \cdot 5 + 3) \cdot 5^3 + 4 \cdot 5^2 + 0 \cdot 5^1 + 1 \cdot 5^0 \\ &= 3 \cdot 5^4 + 3 \cdot 5^3 + 4 \cdot 5^2 + 0 \cdot 5^1 + 1 \cdot 5^0. \end{aligned}$$

Luego $2351 = (33401)_5$. Observar que los dígitos del desarrollo 5-ádico son los restos de las divisiones sucesivas por 5 (ver Figura 6.1).

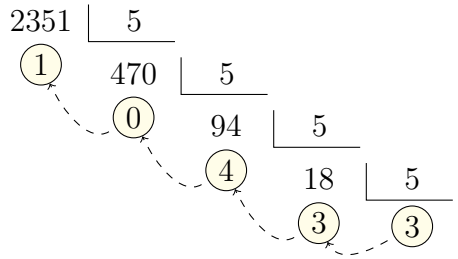


Figura 6.1: Calculando los restos de sucesivas divisiones para obtener el desarrollo 5-ádico.

(b) Transformar el número $(1848)_{11}$ a base 10 (realizar el desarrollo 10-ádico).

$$\begin{aligned} (1848)_{11} &= 1 \cdot 11^3 + 8 \cdot 11^2 + 4 \cdot 11^1 + 8 \cdot 11^0 \\ &= 1331 + 968 + 44 + 8 \\ &= 2351. \end{aligned}$$

6.12. Congruencias

Definición 6.10 (Congruencia)

Sea $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Diremos que a es congruente a b módulo m si $m \mid b - a$. Se denota por:

$$a \equiv b \bmod (m) \;\; o \;\; a \equiv b\,(m)\,.$$

Con $a \not\equiv b\,(m)$ denotamos la negación de $a \equiv b\,(m)$.

Ejemplo 6.11

(a) $3 \equiv 1\,(2)$ pues $2 \mid 1 - 3$.

(b) $-2 \equiv 7\,(9)$ pues $9 \mid 7 + 2$.

(c) $3 \not\equiv 2\,(2)$ pues $2 \nmid 2 - 3$.

Proposición 6.13

Sean $a, b, c, d \in \mathbb{Z}$ y $m \in \mathbb{N}$. Entonces

(a) $a \equiv a\,(m)$.

(b) $a \equiv b\,(m)$ si y sólo si $b \equiv a\,(m)$.

(c) Si $a \equiv b\,(m)$ y $b \equiv c\,(m)$ entonces $a \equiv c\,(m)$.

(d) $a \equiv b\,(m)$ si y sólo si $a + c \equiv b + c\,(m)$.

(e) $a \equiv b\,(m)$ *si y sólo si* $a + m \cdot c \equiv b\,(m)$.

(f) Si $a \equiv b\,(m)$ *entonces* $a \cdot c \equiv b \cdot c\,(m)$.

(g) $a \equiv 0\,(m)$ *si y sólo si* $m \mid a$.

(h) $a \equiv b\,(m)$ *si y sólo si* a *y* b *tienen el mismo resto en la división por* m.

(i) Si $a \equiv b\,(m)$ *y* $c \equiv d\,(m)$ *entonces* $a \cdot c \equiv b \cdot d\,(m)$.

(j) Si $a \equiv b\,(m)$ *y* $c \equiv d\,(m)$ *entonces* $a + c \equiv b + d\,(m)$.

Demostración.
(a) Como $m \cdot 0 = 0 = a - a$ se cumple que $m \mid a - a$. Esto significa que $a \equiv a\,(m)$.

(b)

$$\begin{aligned} a \equiv b\,(m) &\Leftrightarrow m \mid b - a \text{ por Definición 6.10} \\ &\Leftrightarrow m \mid a - b \text{ por Teorema 6.4-(h)} \\ &\Leftrightarrow b \equiv a\,(m) \text{ por Definición 6.10} \end{aligned}$$

(c)

$$\left.\begin{array}{lll} a \equiv b\,(m) & \Rightarrow & m \mid b - a \\ b \equiv c\,(m) & \Rightarrow & m \mid c - b \end{array}\right\} \Rightarrow m \mid b - a + c - b \text{ por Teorema 6.4-(f)}$$

$$\begin{aligned} &\Rightarrow m \mid c - a \\ &\Rightarrow a \equiv c\,(m) \text{ por Definición 6.10} \end{aligned}$$

(d)

$$\begin{aligned} a \equiv b\,(m) &\Leftrightarrow m \mid b - a \text{ por Definición 6.10} \\ &\Leftrightarrow m \mid b - a + c - c \\ &\Leftrightarrow m \mid (b + c) - (a + c) \\ &\Leftrightarrow a + c \equiv b + c\,(m) \text{ por Definición 6.10} \end{aligned}$$

(e)

$$\begin{aligned} a \equiv b\,(m) &\Leftrightarrow m \mid b - a \text{ por Definición 6.10} \\ &\Leftrightarrow \exists u \in \mathbb{Z} : b - a = m \cdot u \text{ por Definición 6.3} \\ &\Leftrightarrow \exists u \in \mathbb{Z} : b - a - m \cdot c = m \cdot u - m \cdot c \\ &\Leftrightarrow \exists u \in \mathbb{Z} : b - (a + m \cdot c) = m \cdot (u - c) \\ &\Leftrightarrow m \mid b - (a + m \cdot c) \text{ por Definición 6.3} \\ &\Leftrightarrow a + m \cdot c \equiv b\,(m) \text{ por Definición 6.10} \end{aligned}$$

(f)

$$a \equiv b\,(m) \Rightarrow m \mid b - a \text{ por Definición 6.10}$$

$$\begin{aligned} &\Rightarrow\ m \mid (b-a)\cdot c \text{ por Teorema 6.4-(h)}\\ &\Rightarrow\ m \mid b\cdot c - a\cdot c\\ &\Rightarrow\ a\cdot c \equiv b\cdot c\,(m) \text{ por Definición 6.10}\end{aligned}$$

(g)

$$\begin{aligned} a\equiv 0\,(m) &\Leftrightarrow 0\equiv a\,(m) \text{ por (b)}\\ &\Leftrightarrow m \mid a-0 \text{ por Definición 6.10}\\ &\Leftrightarrow m \mid a\end{aligned}$$

(h) Utilizando el algoritmo de la división se tiene que:

$$\begin{aligned} a &= m\cdot q_a + r_a, \quad 0\leqslant r_a < m,\\ b &= m\cdot q_b + r_b, \quad 0\leqslant r_b < m.\end{aligned}$$

Sin pérdida de generalidad, podemos asumir que $r_a \leqslant r_b$ (caso contrario les hacemos jugar el rol inverso a a y a b y volvemos a este caso). Luego obtenemos:

$$b-a = m\cdot(q_b-q_a) + (r_b-r_a), \quad 0\leqslant r_b-r_a < m.$$

Entonces,

$$\begin{aligned} a\equiv b\,(m) &\Leftrightarrow m \mid b-a \text{ por Definición 6.10}\\ &\Leftrightarrow m \mid r_b-r_a \text{ pues } m \mid b-a \text{ y } m \mid m\cdot(q_b-q_a)\\ &\Leftrightarrow r_a = r_b \text{ pues } 0\leqslant r_b-r_a < m\end{aligned}$$

(i)

$$\begin{array}{rcl} a &\equiv& b\,(m)\\ c &\equiv& d\,(m)\end{array} \Rightarrow \begin{array}{rcl} a\cdot c &\equiv& b\cdot c\,(m)\\ b\cdot c &\equiv& b\cdot d\,(m)\end{array} \text{ por (f)}$$
$$\Rightarrow\ a\cdot c\equiv b\cdot d\,(m) \text{ por (c)}$$

(j)

$$\begin{array}{rcl} a &\equiv& b\,(m)\\ c &\equiv& d\,(m)\end{array} \Rightarrow \begin{array}{rcl} a+c &\equiv& b+c\,(m)\\ b+c &\equiv& b+d\,(m)\end{array} \text{ por (d)}$$
$$\Rightarrow\ a+c\equiv b+d\,(m) \text{ por (c)}$$

Esto concluye la prueba. ■

Notemos que la Proposición 6.13-(a), 6.13-(b) y 6.13-(c) dice que la relación de congruencia es una relación de equivalencia. Por lo tanto, determina una partición de $\mathbb{Z}$ en clases de equivalencia. Por ejemplo, si $m=5$ entonces la partición está formada por las siguientes clases:

$$\begin{aligned} [0]_5 &= \{\ldots,-10,-5,0,5,10,\ldots\} = \{5\cdot k+0 : k\in\mathbb{Z}\},\\ [1]_5 &= \{\ldots,-9,-4,1,6,11,\ldots\} = \{5\cdot k+1 : k\in\mathbb{Z}\},\\ [2]_5 &= \{\ldots,-8,-3,2,7,12,\ldots\} = \{5\cdot k+2 : k\in\mathbb{Z}\},\\ [3]_5 &= \{\ldots,-7,-2,3,8,13,\ldots\} = \{5\cdot k+3 : k\in\mathbb{Z}\},\\ [4]_5 &= \{\ldots,-6,-1,4,9,14,\ldots\} = \{5\cdot k+4 : k\in\mathbb{Z}\}.\end{aligned}$$

La Proposición 6.13-(h) clasifica a los enteros por su resto en la división por m: dos enteros son equivalentes módulo m si y sólo si poseen el mismo resto en la división por m.

6.13. Reglas de divisibilidad

Los conceptos de congruencia, desarrollos s-ádicos y divisibilidad, nos permiten deducir de manera sencilla las reglas de divisibilidad aprendidas en la escuela primaria.

Dado un número natural a podemos escribirlo en su desarrollo 10–ádico de la siguiente manera (ver Teorema 6.11):

$$a = a_r \cdot 10^r + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0, \quad 0 \leqslant a_i \leqslant 9, \quad i = 0, \ldots, r, \quad a_r \neq 0.$$

6.13.1. Regla de divisibilidad por 2

Notemos que del hecho que $10 \equiv 0\,(2)$ y usando repetidamente la Proposición 6.13-(i) obtenemos que:

$$\begin{aligned} 10 &\equiv 0\,(2)\,, \\ 10^2 &\equiv 0\,(2)\,, \\ &\vdots \quad \vdots \quad \vdots \\ 10^r &\equiv 0\,(2)\,. \end{aligned}$$

Usando repetidamente la Proposición 6.13-(f) se tiene que:

$$\begin{aligned} a_1 \cdot 10 &\equiv 0\,(2)\,, \\ a_2 \cdot 10^2 &\equiv 0\,(2)\,, \\ &\vdots \quad \vdots \quad \vdots \\ a_r \cdot 10^r &\equiv 0\,(2)\,. \end{aligned}$$

Ahora, usando la Proposición 6.13-(j) se tiene

$$a_r \cdot 10^r + \ldots + a_1 \cdot 10 \equiv 0\,(2)\,.$$

Por lo tanto, utilizando la Proposición 6.13-(d) se obtiene

$$a_r \cdot 10^r + \ldots + a_1 \cdot 10 + a_0 \equiv a_0\,(2)\,,$$

con lo cual $a \equiv a_0\,(2)$. Luego, a y a_0 tienen el mismo resto al dividir por 2, lo cual dice que $2 \mid a$ si y sólo si $2 \mid a_0$. Esto sucede sólo cuando $a_0 = 0, 2, 4, 6, 8$, es decir, a es divisible por 2 si y sólo si a termina en una cifra par.

6.13.2. Regla de divisibilidad por 3

Notemos que del hecho que $10 \equiv 1\,(3)$ y usando repetidamente la Proposición 6.13-(i) obtenemos que:

$$\begin{aligned} 10 &\equiv 1\,(3)\,, \\ 10^2 &\equiv 1\,(3)\,, \\ &\vdots \quad \vdots \quad \vdots \\ 10^r &\equiv 1\,(3)\,. \end{aligned}$$

Usando la Proposición 6.13-(a) y repetidamente la Proposición 6.13-(f) se tiene que:

$$a_0 \equiv a_0\,(3)\,,$$

$$\begin{aligned} a_1 \cdot 10 &\equiv a_1\,(3)\,, \\ a_2 \cdot 10^2 &\equiv a_2\,(3)\,, \\ &\vdots \quad \vdots \quad \vdots \\ a_r \cdot 10^r &\equiv a_r\,(3)\,. \end{aligned}$$

Finalmente utilizando la Proposición 6.13-(j) obtenemos que:

$$a_r \cdot 10^r + \ldots + a_0 \equiv a_r + \ldots + a_0\,(3)\,.$$

es decir,

$$a \equiv a_r + \ldots + a_0\,(3)\,.$$

Esto significa que a y $a_r + \ldots + a_0$ tienen el mismo resto en la división por 3. Por lo tanto, un número es divisible por 3 si y sólo si la suma de sus cifras es divisible por 3.

Ejemplo 6.12

(a) Tomemos $a = 13244$. La suma de sus cifras es 14 y no es divisible por 3, por lo tanto 13244 no es divisible por 3.

(b) Tomemos $a = 9234$. La suma de sus cifras es 18 y es divisible por 3, por lo tanto 9234 es divisible por 3.

6.13.3. Regla de divisibilidad por 4

Notemos primero que $10 \equiv 2\,(4)$. Además $10^2 \equiv 0\,(4)$ y usando repetidamente la Proposición 6.13-(i) obtenemos que:

$$\begin{aligned} 10^2 &\equiv 0\,(4)\,, \\ 10^3 &\equiv 0\,(4)\,, \\ &\vdots \quad \vdots \quad \vdots \\ 10^r &\equiv 0\,(4)\,. \end{aligned}$$

Usando la Proposición 6.13-(a) y repetidamente la Proposición 6.13-(f) se tiene que:

$$\begin{aligned} a_0 &\equiv a_0\,(4)\,, \\ a_1 \cdot 10 &\equiv 2 \cdot a_1\,(4)\,, \\ a_2 \cdot 10^2 &\equiv 0\,(4)\,, \\ &\vdots \quad \vdots \quad \vdots \\ a_r \cdot 10^r &\equiv 0\,(4)\,. \end{aligned}$$

Finalmente utilizando la Proposición 6.13-(j) obtenemos que:

$$a_r \cdot 10^r + \ldots + a_0 \equiv 2 \cdot a_1 + a_0\,(4)\,.$$

es decir,

$$a \equiv 2 \cdot a_1 + a_0\,(4)\,.$$

Esto significa que a y $2 \cdot a_1 + a_0$ tienen el mismo resto en la división por 4. Por lo tanto, un número es divisible por 4 si y sólo si el doble de las decenas más las unidades es un número divisible por 4.

Ejemplo 6.13

(a) Tomemos $a = 324235$. El doble de las decenas más las unidades es 11 y no es divisible por 4, por lo tanto 324235 no es divisible por 4.

(b) Tomemos $a = 6434252$. El doble de las decenas más las unidades es 12 y es divisible por 4, por lo tanto 6434252 es divisible por 4.

6.13.4. Regla de divisibilidad por 5

Notemos que del hecho que $10 \equiv 0\,(5)$ y usando repetidamente la Proposición 6.13-(i) obtenemos que:

$$\begin{aligned} 10 &\equiv 0\,(5)\,, \\ 10^2 &\equiv 0\,(5)\,, \\ &\vdots \quad \vdots \quad \vdots \\ 10^r &\equiv 0\,(5)\,. \end{aligned}$$

Usando repetidamente la Proposición 6.13-(f) se tiene que:

$$\begin{aligned} a_1 \cdot 10 &\equiv 0\,(5)\,, \\ a_2 \cdot 10^2 &\equiv 0\,(5)\,, \\ &\vdots \quad \vdots \quad \vdots \\ a_r \cdot 10^r &\equiv 0\,(5)\,. \end{aligned}$$

Ahora, usando la Proposición 6.13-(j) se tiene

$$a_r \cdot 10^r + \ldots + a_1 \cdot 10 \equiv 0\,(5)\,.$$

Por lo tanto, utilizando la Proposición 6.13-(d) se obtiene

$$a_r \cdot 10^r + \ldots + a_1 \cdot 10 + a_0 \equiv a_0\,(5)\,,$$

con lo cual $a \equiv a_0\,(5)$. Luego, a y a_0 tienen el mismo resto al dividir por 5, lo cual dice que $5 \mid a$ si y sólo si $5 \mid a_0$. Esto sucede sólo cuando $a_0 = 0, 5$, es decir, a es divisible por 5 si y sólo si a termina en 0 o 5.

6.13.5. Regla de divisibilidad por 7

Veamos la siguiente cadena de equivalencias:

$$\begin{aligned} 7 \mid a &\Leftrightarrow 7 \mid a_r \cdot 10^r + \ldots + a_0 \\ &\Leftrightarrow \exists k \in \mathbb{Z} : a_r \cdot 10^r + \ldots + a_0 = 7 \cdot k \\ &\Leftrightarrow \exists k \in \mathbb{Z} : \left(a_r \cdot 10^{r-1} + \ldots + a_1\right) \cdot 10 + a_0 = 7 \cdot k \\ &\Leftrightarrow \exists k \in \mathbb{Z} : \left(a_r \cdot 10^{r-1} + \ldots + a_1\right) \cdot 10 - 2 \cdot a_0 \cdot 10 + 2 \cdot a_0 \cdot 10 + a_0 = 7 \cdot k \\ &\Leftrightarrow \exists k \in \mathbb{Z} : \left(a_r \cdot 10^{r-1} + \ldots + a_1 - 2 \cdot a_0\right) \cdot 10 + 21 \cdot a_0 = 7 \cdot k \\ &\Leftrightarrow \exists k \in \mathbb{Z} : \left(a_r \cdot 10^{r-1} + \ldots + a_1 - 2 \cdot a_0\right) \cdot 10 = 7 \cdot (k - 3 \cdot a_0) \\ &\Leftrightarrow 7 \mid \left(a_r \cdot 10^{r-1} + \ldots + a_1 - 2 \cdot a_0\right) \cdot 10 \\ &\Leftrightarrow 7 \mid \left(a_r \cdot 10^{r-1} + \ldots + a_1 - 2 \cdot a_0\right) \end{aligned}$$

Luego un número a es divisible por 7 si y sólo si al tomar el número que resulta de eliminar las unidades y restarle el doble de las unidades es divisible por 7.

Ejemplo 6.14

(a) Tomemos $a = 118242$.

- $11824 - 2 \cdot 2 = 11820$: todavía es difícil determinar si 11820 es divisible por 7.
- $1182 - 2 \cdot 0 = 1182$: todavía es difícil determinar si 1182 es divisible por 7.

- $118 - 2 \cdot 2 = 114$: todavía es difícil determinar si 114 es divisible por 7.
- $11 - 2 \cdot 4 = 3$: ¡ahora es fácil!

Esto dice que 118242 no es divisible por 7.

(b) Tomemos $a = 13244$.

- $1324 - 2 \cdot 4 = 1316$: todavía es difícil determinar si 1316 es divisible por 7.
- $131 - 2 \cdot 6 = 119$: todavía es difícil determinar si 119 es divisible por 7.
- $11 - 2 \cdot 9 = -7$: ¡ahora es fácil!

Esto dice que 13244 es divisible por 7.

6.13.6. Regla de divisibilidad por 8

Notemos primero que $10 \equiv 2\,(8)$. Usando repetidamente la Proposición 6.13-(i) obtenemos que:

$$\begin{aligned} 10 &\equiv 2\,(8)\,, \\ 10^2 &\equiv 4\,(8)\,, \\ 10^3 &\equiv 0\,(8)\,, \\ \vdots &\quad \vdots \quad \vdots \\ 10^r &\equiv 0\,(8)\,. \end{aligned}$$

Usando la Proposición 6.13-(a) y repetidamente la Proposición 6.13-(f) se tiene que:

$$\begin{aligned} a_0 &\equiv a_0\,(8)\,, \\ a_1 \cdot 10 &\equiv 2 \cdot a_1\,(8)\,, \\ a_2 \cdot 10^2 &\equiv 4 \cdot a_2\,(8)\,, \\ a_3 \cdot 10^3 &\equiv 0\,(8)\,, \\ \vdots &\quad \vdots \quad \vdots \\ a_r \cdot 10^r &\equiv 0\,(8)\,. \end{aligned}$$

Finalmente utilizando la Proposición 6.13-(j) obtenemos que:

$$a_r \cdot 10^r + \ldots + a_0 \equiv 4 \cdot a_2 + 2 \cdot a_1 + a_0\,(8)\,.$$

es decir,

$$a \equiv 4 \cdot a_2 + 2 \cdot a_1 + a_0\,(8)\,.$$

Esto significa que a y $4 \cdot a_2 + 2 \cdot a_1 + a_0$ tienen el mismo resto en la división por 8. Por lo tanto, un número es divisible por 8 si y sólo si el cuádruple de las centenas más el doble de las decenas más las unidades es un número divisible por 8.

Ejemplo 6.15

(a) Tomemos $a = 4532342$. El cuádruple de las centenas más el doble de las decenas más las unidades es 22 y no es divisible por 8, por lo tanto 4532342 no es divisible por 8.

(b) Tomemos $a = 3542344$. El cuádruple de las centenas más el doble de las decenas más las unidades es 24 y es divisible por 8, por lo tanto 3542344 es divisible por 8.

6.13.7. Regla de divisibilidad por 9

Notemos que del hecho que $10 \equiv 1\,(9)$ y usando repetidamente la Proposición 6.13-(i) obtenemos que:

$$\begin{aligned} 10 &\equiv 1\,(9)\,, \\ 10^2 &\equiv 1\,(9)\,, \\ \vdots &\ \vdots\ \vdots \\ 10^r &\equiv 1\,(9)\,. \end{aligned}$$

Usando la Proposición 6.13-(a) y repetidamente la Proposición 6.13-(f) se tiene que:

$$\begin{aligned} a_0 &\equiv a_0\,(9)\,, \\ a_1 \cdot 10 &\equiv a_1\,(9)\,, \\ a_2 \cdot 10^2 &\equiv a_2\,(9)\,, \\ \vdots &\ \vdots\ \vdots \\ a_r \cdot 10^r &\equiv a_r\,(9)\,. \end{aligned}$$

Finalmente utilizando la Proposición 6.13-(j) obtenemos que:

$$a_r \cdot 10^r + \ldots + a_0 \equiv a_r + \ldots + a_0\,(9)\,.$$

es decir,

$$a \equiv a_r + \ldots + a_0\,(9)\,.$$

Esto significa que a y $a_r + \ldots + a_0$ tienen el mismo resto en la división por 9. Por lo tanto, un número es divisible por 9 si y sólo si la suma de sus cifras es divisible por 9.

Ejemplo 6.16

(a) Tomemos $a = 13244$. La suma de sus cifras es 14 y no es divisible por 9, por lo tanto 13244 no es divisible por 9.

(b) Tomemos $a = 9234$. La suma de sus cifras es 18 y es divisible por 9, por lo tanto 9234 es divisible por 9.

6.13.8. Regla de divisibilidad por 10

Notemos que del hecho que $10 \equiv 0\,(10)$ y usando repetidamente la Proposición 6.13-(i) obtenemos que:

$$\begin{aligned} 10 &\equiv 0\,(10)\,, \\ 10^2 &\equiv 0\,(10)\,, \\ \vdots &\ \vdots\ \vdots \\ 10^r &\equiv 0\,(10)\,. \end{aligned}$$

Usando repetidamente la Proposición 6.13-(f) se tiene que:

$$\begin{aligned} a_1 \cdot 10 &\equiv 0\,(10)\,, \\ a_2 \cdot 10^2 &\equiv 0\,(10)\,, \\ \vdots &\ \vdots\ \vdots \\ a_r \cdot 10^r &\equiv 0\,(10)\,. \end{aligned}$$

Ahora, usando la Proposición 6.13-(j) se tiene

$$a_r \cdot 10^r + \ldots + a_1 \cdot 10 \equiv 0\,(10)\,.$$

Por lo tanto, utilizando la Proposición 6.13-(d) se obtiene

$$a_r \cdot 10^r + \ldots + a_1 \cdot 10 + a_0 \equiv a_0\,(10)\,,$$

con lo cual $a \equiv a_0\,(10)$. Luego, a y a_0 tienen el mismo resto al dividir por 10, lo cual dice que $10 \mid a$ si y sólo si $10 \mid a_0$. Esto sucede sólo cuando $a_0 = 0$, es decir, a es divisible por 10 si y sólo si a termina en 0.

6.13.9. Regla de divisibilidad por 11

Notemos primero que $10 \equiv -1\,(11)$. Usando repetidamente la Proposición 6.13-(i) obtenemos que:

$$\begin{aligned} 10 &\equiv -1\,(11)\,,\\ 10^2 &\equiv 1\,(11)\,,\\ 10^3 &\equiv -1\,(11)\,,\\ &\vdots \quad \vdots \quad \vdots\\ 10^r &\equiv (-1)^r\,(11)\,. \end{aligned}$$

Usando la Proposición 6.13-(a) y repetidamente la Proposición 6.13-(f) se tiene que:

$$\begin{aligned} a_0 &\equiv a_0\,(11)\,,\\ a_1 \cdot 10 &\equiv -a_1\,(11)\,,\\ a_2 \cdot 10^2 &\equiv a_2\,(11)\,,\\ a_3 \cdot 10^3 &\equiv -a_3\,(11)\,,\\ &\vdots \quad \vdots \quad \vdots\\ a_r \cdot 10^r &\equiv (-1)^r \cdot a_r\,(11)\,. \end{aligned}$$

Finalmente utilizando la Proposición 6.13-(j) obtenemos que:

$$a_r \cdot 10^r + \ldots + a_0 \equiv \sum_{i=0}^{r} (-1)^i \cdot a_i\,(11)\,.$$

es decir,

$$a \equiv \sum_{i=0}^{r} (-1)^i \cdot a_i\,(11)\,.$$

Esto significa que a y $\sum_{i=0}^{r} (-1)^i \cdot a_i$ tienen el mismo resto en la división por 11. Por lo tanto, un número es divisible por 11 si y sólo si la suma de las cifras que ocupan un lugar par menos la suma de las cifras que ocupan un lugar impar es divisible por 11.

Ejemplo 6.17

(a) Tomemos $a = 6423234$. La suma de las cifras que ocupan un lugar par menos la suma de las cifras que ocupan un lugar impar es igual a $4 - 3 + 2 - 3 + 2 - 4 + 6 = 4$ y no es divisible por 11, por lo tanto 6423234 no es divisible por 11.

(b) Tomemos $a = 6423241$. La suma de las cifras que ocupan un lugar par menos la suma de las cifras que ocupan un lugar impar es igual a $1 - 4 + 2 - 3 + 2 - 4 + 6 = 0$ y es divisible por 11, por lo tanto 6423241 es divisible por 11.

6.14. Ecuaciones lineales de congruencia

Trataremos de estudiar el problema de resolver la ecuación:

$$a \cdot x \equiv b\,(m)\,,$$

donde $a, x, b \in \mathbb{Z}$ y $m \in \mathbb{N}$.

Proposición 6.14
Sean $a, b \in \mathbb{Z}$ y $m \in \mathbb{N}$. Consideremos la ecuación lineal de congruencia:

$$a \cdot x \equiv b\,(m)\,.$$

(a) La ecuación lineal de congruencia no siempre tiene solución.

(b) Si la ecuación lineal de congruencia tiene solución, entonces admite infinitas soluciones. Por ello consideraremos como soluciones sólo aquellas soluciones x tales que $0 \leqslant x < m$.

Demostración.
(a) Veamos que el problema $2 \cdot x \equiv 3\,(2)$ no admite solución. Si tuviera, entonces existiría $x \in \mathbb{Z}$ tal que $2 \mid 2 \cdot x - 3$. Luego:

$$2 \mid 2 \cdot x \wedge 2 \mid 2 \cdot x - 3 \Rightarrow 2 \mid 3,$$

lo cual es falso.

(b) Supongamos que existe $x_0 \in \mathbb{Z}$ solución, entonces $x_0 + m \cdot k$, con $k \in \mathbb{Z}$, también es solución, pues

$$\left.\begin{array}{rcl} a \cdot x_0 & \equiv & b\,(m) \\ a \cdot m \cdot k & \equiv & 0\,(m) \end{array}\right\} \Rightarrow \; a \cdot x_0 + a \cdot m \cdot k \equiv b + 0\,(m) \text{ por Proposición 6.13-(j)}$$

$$\Rightarrow \; a \cdot (x_0 + m \cdot k) \equiv b\,(m)$$

$$\Rightarrow \; x_0 + m \cdot k \text{ es solución.}$$

■

Proposición 6.15
Sean $a, b \in \mathbb{Z}$ y $m \in \mathbb{N}$. La ecuación lineal de congruencia $a \cdot x \equiv b\,(m)$ admite solución si y sólo si $(a, m) \mid b$.

Además, si la ecuación tiene solución, entonces el conjunto de todas las soluciones es:

$$\left\{ x_0 + k \cdot \frac{m}{(a, m)} : k \in \mathbb{Z} \right\},$$

donde x_0 es una solución particular de la ecuación lineal de congruencia.

Demostración.
Supongamos primero que existe solución. Es decir, existe $x \in \mathbb{Z}$ tal que $a \cdot x \equiv b\,(m)$. Esto significa que $m \mid b - a \cdot x$, es decir, existe $k \in \mathbb{Z}$ tal que $b - a \cdot x = k \cdot m$. O sea $b = a \cdot x + k \cdot m$. Ahora:

$$\left.\begin{array}{rcl} (a, m) \mid a & \Rightarrow & (a, m) \mid a \cdot x \\ (a, m) \mid m & \Rightarrow & (a, m) \mid k \cdot m \end{array}\right\} \Rightarrow \; (a, m) \mid a \cdot x + k \cdot m \text{ por Proposición 6.4-(f)}$$

$$\Rightarrow \; (a, m) \mid b$$

Asumamos ahora que $(a, m) \mid b$. Por Teorema 6.5 existen $r, s \in \mathbb{Z}$ tal que $(a, m) = r \cdot a + s \cdot m$. Entonces:

$$(a, m) = r \cdot a + s \cdot m \;\; \Rightarrow \;\; 1 = r \cdot \frac{a}{(a, m)} + s \cdot \frac{m}{(a, m)} \text{ dividiendo por } (a, m)$$

$$\Rightarrow \quad b = a \cdot \left[r \cdot \frac{b}{(a,m)} \right] + m \cdot \left[s \cdot \frac{b}{(a,m)} \right] \text{ multiplicando por } b$$

Notar que, debido a nuestra hipótesis, se tiene que

$$\frac{b}{(a,m)} \in \mathbb{Z}.$$

Luego, tenemos que

$$\begin{aligned} b = a \cdot \left[r \cdot \frac{b}{(a,m)} \right] + m \cdot \left[s \cdot \frac{b}{(a,m)} \right] \quad &\Rightarrow \quad m \mid b - a \cdot \left[r \cdot \frac{b}{(a,m)} \right] \\ &\Rightarrow \quad a \cdot \left[r \cdot \frac{b}{(a,m)} \right] \equiv b\,(m) \text{ por Definición 6.10} \end{aligned}$$

Por lo tanto, $x_0 = r \cdot \dfrac{b}{(a,m)}$ es una solución de la ecuación lineal de congruencia.

Ahora asumamos que x_0 es una solución particular de la ecuación lineal de congruencia y caractericemos todas las soluciones.

Sea $k \in \mathbb{Z}$. Como x_0 es solución tenemos que:

$$\begin{aligned} a \cdot x_0 \equiv b\,(m) \quad &\Rightarrow \quad m \mid b - a \cdot x_0 \text{ por Definición 6.10} \\ &\Rightarrow \quad \exists l \in \mathbb{Z} : b - a \cdot x_0 = m \cdot l \text{ por Definición 6.3} \\ &\Rightarrow \quad \exists l \in \mathbb{Z} : b - a \cdot x_0 - a \cdot k \cdot \frac{m}{(a,m)} = m \cdot l - a \cdot k \cdot \frac{m}{(a,m)} \\ &\Rightarrow \quad \exists l \in \mathbb{Z} : b - a \cdot \left[x_0 + k \cdot \frac{m}{(a,m)} \right] = m \cdot l - m \cdot k \cdot \frac{a}{(a,m)} \\ &\Rightarrow \quad \exists l \in \mathbb{Z} : b - a \cdot \left[x_0 + k \cdot \frac{m}{(a,m)} \right] = m \cdot \left[l - k \cdot \frac{a}{(a,m)} \right] \\ &\Rightarrow \quad \exists \tilde{l} \in \mathbb{Z} : b - a \cdot \left[x_0 + k \cdot \frac{m}{(a,m)} \right] = m \cdot \tilde{l} \\ &\Rightarrow \quad m \mid b - a \cdot \left[x_0 + k \cdot \frac{m}{(a,m)} \right] \text{ por Definición 6.3} \\ &\Rightarrow \quad a \cdot \left[x_0 + k \cdot \frac{m}{(a,m)} \right] \equiv b\,(m) \text{ por Definición 6.10} \end{aligned}$$

Esto dice que $x_0 + k \cdot \dfrac{m}{(a,m)}$ es solución.

Recíprocamente, asumamos que x es una solución de la ecuación lineal de congruencia. Entonces:

$$\begin{aligned} \left.\begin{array}{l} a \cdot x_0 \equiv b\,(m) \\ a \cdot x \equiv b\,(m) \end{array}\right. \quad &\Rightarrow \quad a \cdot x - a \cdot x_0 \equiv b - b\,(m) \text{ por Proposición 6.13-(f) y 6.13-(j)} \\ &\Rightarrow \quad a \cdot (x - x_0) \equiv 0\,(m) \\ &\Rightarrow \quad m \mid a \cdot (x - x_0) \text{ por Proposición 6.13-(g)} \\ &\Rightarrow \quad \exists s \in \mathbb{Z} : a \cdot (x - x_0) = m \cdot s \text{ por Definición 6.3} \end{aligned}$$

$$
\begin{aligned}
&\Rightarrow \quad \exists s \in \mathbb{Z} : \frac{a}{(a,m)} \cdot (x - x_0) = \frac{m}{(a,m)} \cdot s \text{ dividiendo por } (a,m) \\
&\Rightarrow \quad \tilde{a} \cdot (x - x_0) = \tilde{m} \cdot s \text{ donde } \tilde{a} = \frac{a}{(a,m)} \text{ y } \tilde{m} = \frac{m}{(a,m)} \\
&\Rightarrow \quad \tilde{m} \mid \tilde{a} \cdot (x - x_0) \text{ por Definición 6.3} \\
&\Rightarrow \quad \tilde{m} \mid (x - x_0) \text{ por Proposición 6.7-(b) pues } (\tilde{a}, \tilde{m}) = 1 \text{ por Proposición 6.9-(b)} \\
&\Rightarrow \quad \exists k \in \mathbb{Z} : x - x_0 = \tilde{m} \cdot k \text{ por Definición 6.3} \\
&\Rightarrow \quad \exists k \in \mathbb{Z} : x - x_0 = \frac{m}{(a,m)} \cdot k \\
&\Rightarrow \quad \exists k \in \mathbb{Z} : x = x_0 + \frac{m}{(a,m)} \cdot k
\end{aligned}
$$

Esto concluye la demostración. ■

De acuerdo a la demostración de la Proposición 6.15, para hallar la solución de la ecuación lineal de congruencia se deben seguir los siguientes pasos:

- Calcular (a, m).
- Chequear que $(a, m) \mid b$. Si esto no ocurre la ecuación lineal de congruencia no tiene solución. Caso contrario, continuar al paso siguiente.
- Calcular la combinación lineal entera, es decir, hallar $r, s \in \mathbb{Z}$ tal que

$$(a, m) = r \cdot a + s \cdot m.$$

- Calcular una solución particular x_0. De acuerdo a la Proposición 6.15 se tiene que:

$$x_0 = r \cdot \frac{b}{(a,m)}.$$

- Hallar todas las soluciones $x_k = x_0 + k \cdot \frac{m}{(a,m)}$, con $k \in \mathbb{Z}$, tal que $0 \leqslant x_k < m$.

Ejemplo 6.18

(a) Resolver la ecuación $42 \cdot x \equiv 50\,(76)$.

De acuerdo a los lineamientos anteriores, procederemos a resolver la ecuación de congruencia. En este caso, $a = 42$, $b = 50$ y $m = 76$.

- Calcular (a, m).
  Haciendo uso repetido del algoritmo de la división se tiene que:

$$
\begin{aligned}
76 &= 42 \cdot 1 + 34 \text{ por lo tanto } (76, 42) = (42, 34) \\
42 &= 34 \cdot 1 + 8 \text{ por lo tanto } (42, 34) = (34, 8) \\
34 &= 8 \cdot 4 + 2 \text{ por lo tanto } (34, 8) = (8, 2) \\
8 &= 2 \cdot 4 + 0 \text{ por lo tanto } (8, 2) = 2
\end{aligned}
$$

  Luego $(42, 76) = 2$.
- Chequear que $(a, m) \mid b$.
  Esto sucede pues $2 \mid 50$. Ahora estamos seguros que la ecuación lineal de congruencia admite solución.

- Calculemos la combinación lineal entera.

$$\begin{aligned} 2 &= 34 + (-4)\cdot 8 \text{ pues } 34 = 8\cdot 4 + 2 \\ &= 34 + (-4)\cdot[42 + 34\cdot(-1)] = (-4)\cdot 42 + 5\cdot 34 \text{ pues } 42 = 34\cdot 1 + 8 \\ &= (-4)\cdot 42 + 5\cdot[76 + 42\cdot(-1)] \text{ pues } 76 = 42\cdot 1 + 34 \\ &= (-9)\cdot 42 + 5\cdot 76. \end{aligned}$$

  Por lo tanto $r = -9$ y $s = 5$.

- Calcular una solución particular x_0.

$$x_0 = (-9)\cdot\frac{50}{2} = -9\cdot 25 = -225.$$

- Hallar todas las soluciones $x_k = x_0 + k\cdot\dfrac{m}{(a,m)}$, con $k \in \mathbb{Z}$, tal que $0 \leqslant x_k < m$.

$$\begin{aligned} -225 + 5\cdot 38 &= -35 \text{ no!} \\ -225 + 6\cdot 38 &= 3 \text{ sí!} \\ -225 + 7\cdot 38 &= 41 \text{ sí!} \\ -225 + 8\cdot 38 &= 79 \text{ no!} \end{aligned}$$

Por lo tanto, las soluciones de la ecuación de congruencia son: 3 y 41.

(b) Resolver la ecuación $30\cdot x \equiv 18\,(78)$.

De acuerdo a los lineamientos anteriores, procederemos a resolver la ecuación de congruencia. En este caso, $a = 30$, $b = 18$ y $m = 78$.

- Calcular (a, m).
  Haciendo uso repetido del algoritmo de la división se tiene que:

$$\begin{aligned} 78 &= 30\cdot 2 + 18 \text{ por lo tanto } (78, 30) = (30, 18) \\ 30 &= 18\cdot 1 + 12 \text{ por lo tanto } (30, 18) = (18, 12) \\ 18 &= 12\cdot 1 + 6 \text{ por lo tanto } (18, 12) = (12, 6) \\ 12 &= 6\cdot 2 + 0 \text{ por lo tanto } (12, 6) = 6 \end{aligned}$$

  Luego $(30, 78) = 6$.

- Chequear que $(a, m) \mid b$.
  Esto sucede pues $6 \mid 18$. Ahora estamos seguros que la ecuación lineal de congruencia admite solución.

- Calculemos la combinación lineal entera.

$$\begin{aligned} 6 &= 18 + (-1)\cdot 12 \text{ pues } 18 = 12\cdot 1 + 6 \\ &= 18 + (-1)\cdot[30 + (-1)\cdot 18] = (-1)\cdot 30 + 2\cdot 18 \text{ pues } 30 = 18\cdot 1 + 12 \\ &= (-1)\cdot 30 + 2\cdot[78 + (-2)\cdot 30] \text{ pues } 78 = 30\cdot 2 + 18 \\ &= (-5)\cdot 30 + 2\cdot 78. \end{aligned}$$

  Por lo tanto $r = -5$ y $s = 2$.

- Calcular una solución particular x_0.

$$x_0 = (-5)\cdot\frac{18}{6} = -5\cdot 3 = -15.$$

- Hallar todas las soluciones $x_k = x_0 + k \cdot \dfrac{m}{(a,m)}$, con $k \in \mathbb{Z}$, tal que $0 \leqslant x_k < m$.

$$\begin{aligned}
-15 + 1 \cdot 13 &= -2 \text{ no!} \\
-15 + 2 \cdot 13 &= 11 \text{ sí!} \\
-15 + 3 \cdot 13 &= 24 \text{ sí!} \\
-15 + 4 \cdot 13 &= 37 \text{ sí!} \\
-15 + 5 \cdot 13 &= 50 \text{ sí!} \\
-15 + 6 \cdot 13 &= 63 \text{ sí!} \\
-15 + 7 \cdot 13 &= 76 \text{ sí!} \\
-15 + 8 \cdot 13 &= 89 \text{ no!}
\end{aligned}$$

Por lo tanto, las soluciones de la ecuación de congruencia son: 11, 24, 37, 50, 63 y 76.

Observemos que si la ecuación lineal de congruencia $a \cdot x \equiv b\,(m)$ tiene solución, entonces todas las soluciones no congruentes entre sí módulo m son:

$$x_0, x_0 + \frac{m}{(a,m)}, x_0 + 2 \cdot \frac{m}{(a,m)}, \ldots, x_0 + [(a,m) - 1] \cdot \frac{m}{(a,m)},$$

donde x_0 es una solución particular. Esto significa que si $(a,m) = 1$ entonces la ecuación lineal de congruencia admite "única" solución.

6.15. Sistemas de ecuaciones lineales de congruencia

Proposición 6.16
El sistema de congruencias

$$\begin{aligned}
x &\equiv a_1\,(m_1)\,, \\
x &\equiv a_2\,(m_2)\,,
\end{aligned}$$

admite solución si y sólo si $(m_1, m_2) \mid a_1 - a_2$.

Además, si el sistema tiene solución, entonces el conjunto de todas las soluciones es:

$$\{x_0 + k \cdot [m_1, m_2] : k \in \mathbb{Z}\}\,,$$

donde x_0 *es una solución particular del sistema lineal de congruencia. Esto dice que hay una única solución* x *tal que* $0 \leqslant x < [m_1, m_2]$.

Demostración.
Asumamos primero que el sistema lineal de congruencia admite solución que llamaremos x. Luego,

$$\begin{aligned}
x \equiv a_1\,(m_1) &\Leftrightarrow m_1 \mid a_1 - x \text{ por Definición 6.10} \\
&\Leftrightarrow \exists k \in \mathbb{Z} : a_1 - x = m_1 \cdot k \text{ por Definición 6.3} \\
&\Leftrightarrow \exists k \in \mathbb{Z} : a_1 = x + m_1 \cdot k.
\end{aligned}$$

$$\begin{aligned}
x \equiv a_2\,(m_2) &\Leftrightarrow m_2 \mid a_2 - x \text{ por Definición 6.10} \\
&\Leftrightarrow \exists h \in \mathbb{Z} : a_2 - x = m_2 \cdot h \text{ por Definición 6.3} \\
&\Leftrightarrow \exists h \in \mathbb{Z} : a_2 = x + m_2 \cdot h.
\end{aligned}$$

De esta manera,

$$a_1 - a_2 = m_1 \cdot k - m_2 \cdot h.$$

Ahora:

$$\left.\begin{array}{lll} (m_1, m_2) \mid m_1 & \Rightarrow & (m_1, m_2) \mid m_1 \cdot k \\ (m_1, m_2) \mid m_2 & \Rightarrow & (m_1, m_2) \mid -m_2 \cdot h \end{array}\right\} \Rightarrow (m_1, m_2) \mid m_1 \cdot k - m_2 \cdot h \text{ por Proposición 6.4-(f)}$$
$$\Rightarrow (m_1, m_2) \mid a_1 - a_2$$

Asumamos ahora que $(m_1, m_2) \mid a_1 - a_2$. Por Teorema 6.5-(b) existen $u, v \in \mathbb{Z}$ tal que:

$$\begin{aligned} (m_1, m_2) = u \cdot m_1 + v \cdot m_2 &\Rightarrow 1 = u \cdot \frac{m_1}{(m_1, m_2)} + v \cdot \frac{m_2}{(m_1, m_2)} \\ &\Rightarrow a_1 - a_2 = (a_1 - a_2) \cdot u \cdot \frac{m_1}{(m_1, m_2)} + (a_1 - a_2) \cdot v \cdot \frac{m_2}{(m_1, m_2)} \\ &\Rightarrow a_1 - a_2 = \left[\frac{a_1 - a_2}{(m_1, m_2)} \cdot u\right] \cdot m_1 + \left[\frac{a_1 - a_2}{(m_1, m_2)} \cdot v\right] \cdot m_2 \\ &\Rightarrow a_1 - a_2 = -t \cdot m_1 + h \cdot m_2, \end{aligned}$$

donde $t = -\dfrac{a_1 - a_2}{(m_1, m_2)} \cdot u$ y $h = \dfrac{a_1 - a_2}{(m_1, m_2)} \cdot v$. Notar que $h, t \in \mathbb{Z}$ pues $(m_1, m_2) \mid a_1 - a_2$. Luego tenemos que:

$$a_1 + t \cdot m_1 = a_2 + h \cdot m_2.$$

Definimos $x_0 = a_1 + t \cdot m_1$. Luego:

$$\begin{aligned} x_0 = a_1 + t \cdot m_1 &\Rightarrow x_0 \equiv a_1 \,(m_1)\,, \\ x_0 = a_2 + h \cdot m_2 &\Rightarrow x_0 \equiv a_2 \,(m_2)\,. \end{aligned}$$

Esto dice que x_0 es solución del sistema lineal de congruencia.

Ahora asumamos que x_0 es una solución particular del sistema lineal de congruencia y caracterizemos todas las soluciones.

Sea $k \in \mathbb{Z}$. Veamos que $x_0 + k \cdot [m_1, m_2]$ es también una solución. Por Definición 6.8 existen $r, s \in \mathbb{Z}$ tal que:

$$\begin{aligned} [m_1, m_2] &= r \cdot m_1, \\ [m_1, m_2] &= s \cdot m_2. \end{aligned}$$

Ahora,

$$\begin{array}{rcl} x_0 & \equiv & a_1 \,(m_1) \\ m_1 & \equiv & 0 \,(m_1) \end{array} \Rightarrow \begin{array}{rcl} x_0 & \equiv & a_1 \,(m_1) \\ k \cdot r \cdot m_1 & \equiv & 0 \,(m_1) \end{array}$$
$$\Rightarrow \begin{array}{rcl} x_0 & \equiv & a_1 \,(m_1) \\ k \cdot [m_1, m_2] & \equiv & 0 \,(m_1) \end{array}$$
$$\Rightarrow x_0 + k \cdot [m_1, m_2] \equiv a_1 \,(m_1)$$

Análogamente,

$$\begin{array}{rcl} x_0 & \equiv & a_2 \,(m_2) \\ m_2 & \equiv & 0 \,(m_2) \end{array} \Rightarrow \begin{array}{rcl} x_0 & \equiv & a_2 \,(m_2) \\ k \cdot s \cdot m_2 & \equiv & 0 \,(m_2) \end{array}$$
$$\Rightarrow \begin{array}{rcl} x_0 & \equiv & a_2 \,(m_2) \\ k \cdot [m_1, m_2] & \equiv & 0 \,(m_2) \end{array}$$

$$\Rightarrow \quad x_0 + k \cdot [m_1, m_2] \equiv a_2 \, (m_2)$$

Por lo tanto, $x_0 + k \cdot [m_1, m_2]$ es una solución del sistema lineal de congruencia.

Recíprocamente, asumamos que x es una solución del sistema lineal de congruencia. Entonces:

$$\begin{array}{rcll} x & \equiv & a_1 \, (m_1) & \\ x_0 & \equiv & a_1 \, (m_1) & \Rightarrow \quad x - x_0 \equiv 0 \, (m_1) \\ & & & \Rightarrow \quad m_1 \mid x - x_0 \end{array}$$

Análogamente,

$$\begin{array}{rcll} x & \equiv & a_2 \, (m_2) & \\ x_0 & \equiv & a_2 \, (m_2) & \Rightarrow \quad x - x_0 \equiv 0 \, (m_2) \\ & & & \Rightarrow \quad m_2 \mid x - x_0 \end{array}$$

Como $m_1 \mid x - x_0$ y $m_2 \mid x - x_0$, la Proposición 6.12 nos dice que $[m_1, m_2] \mid x - x_0$. Esto significa que existe $k \in \mathbb{Z}$ tal que $x - x_0 = k \cdot [m_1, m_2]$, es decir, $x = x_0 + k \cdot [m_1, m_2]$.

Esto concluye la demostración. ■

De acuerdo a la demostración de la Proposición 6.16, para hallar la solución del sistema lineal de congruencia se deben seguir los siguientes pasos:

- Calcular (m_1, m_2).
- Chequear que $(m_1, m_2) \mid a_1 - a_2$. Si esto no ocurre el sistema lineal de congruencia no tiene solución. Caso contrario, continuar al paso siguiente.
- Calcular la combinación lineal entera, es decir, hallar $u, v \in \mathbb{Z}$ tal que

$$(m_1, m_2) = u \cdot m_1 + v \cdot m_2.$$

- Calcular una solución particular x_0. De acuerdo a la Proposición 6.16 se tiene que:

$$x_0 = a_1 + t \cdot m_1,$$

donde

$$t = -\frac{a_1 - a_2}{(m_1, m_2)} \cdot u.$$

- Hallar la solución $x = x_0 + k \cdot [m_1, m_2]$, con $k \in \mathbb{Z}$, tal que $0 \leqslant x < [m_1, m_2]$.

Ejemplo 6.19

(a) Resolver

$$\begin{array}{rcl} x & \equiv & 4 \, (9) \, , \\ x & \equiv & 7 \, (12) \, . \end{array}$$

De acuerdo a los lineamientos anteriores, procederemos a resolver el sistema lineal de congruencia. En este caso, $a_1 = 4$, $a_2 = 7$, $m_1 = 9$ y $m_2 = 12$.

- Calcular (m_1, m_2).
  Haciendo uso repetido del algoritmo de la división se tiene que:

$$\begin{array}{rcl} 12 & = & 9 \cdot 1 + 3 \text{ por lo tanto } (12, 9) = (9, 3) \\ 9 & = & 3 \cdot 3 + 0 \text{ por lo tanto } (9, 3) = 3 \end{array}$$

  Luego $(9, 12) = 3$.

- Chequear que $(m_1, m_2) \mid a_1 - a_2$.
  Esto sucede pues $3 \mid 4 - 7$. Ahora estamos seguros que el sistema lineal de congruencia admite solución.
- Calculemos la combinación lineal entera.

$$3 = (-1) \cdot 9 + 1 \cdot 12 \text{ pues } 12 = 9 \cdot 1 + 3$$

  Por lo tanto $u = -1$ y $v = 1$.
- Calcular una solución particular x_0.

$$\begin{aligned} x_0 &= a_1 + t \cdot m_1 \\ &= a_1 - \frac{a_1 - a_2}{(m_1, m_2)} \cdot u \cdot m_1 \\ &= 4 - \frac{-3}{3} \cdot (-1) \cdot 9 \\ &= 4 - 9 \\ &= -5 \end{aligned}$$

- Hallar la solución $x = x_0 + k \cdot [m_1, m_2]$, con $k \in \mathbb{Z}$, tal que $0 \leqslant x < [m_1, m_2]$.
  Primero notemos que

$$[9, 12] = \frac{9 \cdot 12}{(9, 12)} = \frac{108}{3} = 36,$$

  y luego,

$$-5 + 1 \cdot 36 = 31 \text{ sí!}$$

  y tenemos que $0 \leqslant 31 < 36$.

Por lo tanto, la solución del sistema lineal de congruencia es: 31.

(b) Resolver

$$\begin{aligned} x &\equiv 17\,(36)\,, \\ x &\equiv 23\,(78)\,. \end{aligned}$$

De acuerdo a los lineamientos anteriores, procederemos a resolver el sistema lineal de congruencia. En este caso, $a_1 = 17$, $a_2 = 23$, $m_1 = 36$ y $m_2 = 78$.

- Calcular (m_1, m_2).
  Haciendo uso repetido del algoritmo de la división se tiene que:

$$\begin{aligned} 78 &= 36 \cdot 2 + 6 \text{ por lo tanto } (78, 36) = (36, 6) \\ 36 &= 6 \cdot 6 + 0 \text{ por lo tanto } (36, 6) = 6 \end{aligned}$$

  Luego $(36, 78) = 6$.
- Chequear que $(m_1, m_2) \mid a_1 - a_2$.
  Esto sucede pues $6 \mid 17 - 23$. Ahora estamos seguros que el sistema lineal de congruencia admite solución.
- Calculemos la combinación lineal entera.

$$6 = (-2) \cdot 36 + 1 \cdot 78 \text{ pues } 78 = 36 \cdot 2 + 6$$

  Por lo tanto $u = -2$ y $v = 1$.

- Calcular una solución particular x_0.

$$\begin{aligned} x_0 &= a_1 + t \cdot m_1 \\ &= a_1 - \frac{a_1 - a_2}{(m_1, m_2)} \cdot u \cdot m_1 \\ &= 17 - \frac{17 - 23}{6} \cdot (-2) \cdot 36 \\ &= 17 - 72 \\ &= -55 \end{aligned}$$

- Hallar la solución $x = x_0 + k \cdot [m_1, m_2]$, con $k \in \mathbb{Z}$, tal que $0 \leqslant x < [m_1, m_2]$.
  Primero notemos que

$$[36, 78] = \frac{36 \cdot 78}{(36, 78)} = \frac{2808}{6} = 468,$$

  y luego,

$$-55 + 1 \cdot 468 = 413 \text{ sí!}$$

  y tenemos que $0 \leqslant 413 < 468$.

Por lo tanto, la solución del sistema lineal de congruencia es: 413.

Una generalización de la situación anterior se puede mirar en el siguiente teorema que no demostraremos.

Teorema 6.12 (Teorema chino del resto)
Consideremos el siguiente sistema lineal de congruencias:

$$\begin{cases} x & \equiv & a_1 \, (m_1) \\ \vdots & \vdots & \vdots \\ x & \equiv & a_k \, (m_k) \end{cases}$$

donde

$$(m_i, m_j) = 1, \quad i \neq j.$$

Entonces este sistema admite una única solución módulo el producto $m_1 \cdot \ldots \cdot m_k$.

6.16. Algunos teoremas adicionales de congruencia

Proposición 6.17
Sean $a, b \in \mathbb{Z}$ y p un número primo positivo. Entonces:

$$(a + b)^p \equiv a^p + b^p \, (p) \, .$$

Demostración.
Si $a = 0$ entonces $(a + b)^p = b^p = a^p + b^p$. Luego $(a + b)^p \equiv a^p + b^p \, (p)$.
Si $b = 0$ entonces $(a + b)^p = a^p = a^p + b^p$. Luego $(a + b)^p \equiv a^p + b^p \, (p)$.
Asumamos ahora que $a \neq 0$ y $b \neq 0$. Luego tenemos

$$\begin{aligned} (a + b)^p &= \sum_{i=0}^{p} \binom{p}{i} \cdot a^{p-i} \cdot b^i \text{ por Teorema 5.17} \\ &= a^p + b^p + \sum_{i=1}^{p-1} \binom{p}{i} \cdot a^{p-i} \cdot b^i \text{ separando el primer y último sumando} \end{aligned}$$

$$= a^p + b^p + \sum_{i=1}^{p} p \cdot k_i \cdot a^{p-i} \cdot b^i \text{ con } k_i \in \mathbb{Z}, \text{ por Proposición 6.11}$$

$$= a^p + b^p + p \cdot \sum_{i=1}^{p} k_i \cdot a^{p-i} \cdot b^i \text{ sacando factor común}$$

Luego es claro que $(a+b)^p \equiv a^p + b^p \,(p)$. ■

Teorema 6.13 (Euler–Fermat–Vivaldi)
Sea p un número primo positivo. Entonces:

(a) $\forall a \in \mathbb{Z}, a^p \equiv a \,(p)$.

(b) $\forall a \in \mathbb{Z}$ *tal que* $(a,p) = 1$ *se cumple que* $a^{p-1} \equiv 1 \,(p)$.

Demostración.
(a) Mostraremos que $a^p \equiv a \,(p)$ para todo $a \in \mathbb{N}$. Veamos esto por induccción en a. Para $a = 1$ es claro que $1^p \equiv 1 \,(p)$ pues $1^p = 1$. Asumamos que $a^p \equiv a \,(p)$ y veamos que $(a+1)^p \equiv a+1 \,(p)$:

$$\begin{aligned} (a+1)^p &\equiv a^p + 1^p \,(p) \text{ por Proposición 6.17} \\ &\equiv a^p + 1 \,(p) \\ &\equiv a + 1 \,(p) \text{ debido a que } a^p \equiv a \,(p) \text{ y por Proposición 6.13-(d)} \end{aligned}$$

Además, para el caso que $a = 0$, es claro que se cumple que $0^p \equiv 0 \,(p)$.
Para el caso $a < 0$ se tiene que $-a \in \mathbb{N}$. Luego se tiene que $(-a)^p \equiv -a \,(p)$. Distinguimos dos casos:

- Si p es impar. Luego $-a^p \equiv -a \,(p)$. Luego $a^p \equiv a \,(p)$ debido a la Proposición 6.13-(f).
- Si p es par. Luego debe ocurrir que $p = 2$. Como $a^2 \equiv -a \,(2)$ y $1 \equiv -1 \,(2)$ se tiene que $a^2 \equiv a \,(2)$ debido a la Proposición 6.13-(i).

(b) Sabemos por (a) que $a^p \equiv a \,(p)$, es decir, $p \mid a^p - a$. O sea que $p \mid a \cdot (a^{p-1} - 1)$. Como $(a,p) = 1$ se tiene que $p \mid a^{p-1} - 1$ debido al Teorema 6.7-(b). O sea que $a^{p-1} \equiv 1 \,(p)$. ■

Ejemplo 6.20
Veamos algunos ejemplos de utilización de los teoremas de congruencia.

(a) Calcular el resto de dividir 3^{1000} por 7.

Por Teorema 6.13-(b) se tiene que $3^6 \equiv 1 \,(7)$. Luego, debido a que $1000 = 6 \cdot 166 + 4$ obtenemos que:

$$\begin{aligned} 3^6 \equiv 1 \,(7) &\Rightarrow \left(3^6\right)^{166} \equiv 1^{166} \,(7) \text{ por Proposición 6.13-(i)} \\ &\Rightarrow \left(3^6\right)^{166} \equiv 1 \,(7) \\ &\Rightarrow \left(3^6\right)^{166} \cdot 3^4 \equiv 1 \cdot 3^4 \,(7) \text{ por Proposición 6.13-(f)} \\ &\Rightarrow 3^{6 \cdot 166 + 4} \equiv 3^4 \,(7) \\ &\Rightarrow 3^{1000} \equiv 3^4 \,(7) \end{aligned}$$

Ahora $3^4 = 81 = 7 \cdot 11 + 4$, lo cual dice que $3^4 \equiv 4 \,(7)$. Por lo tanto, la Proposición 6.13-(c) dice que $3^{1000} \equiv 4 \,(7)$.

(b) Calcular el resto de dividir 7^{1015} por 31.

Por Teorema 6.13-(b) se tiene que $7^{30} \equiv 1\,(31)$. Luego, debido a que $1015 = 30 \cdot 33 + 25$ obtenemos que:

$$\begin{aligned} 7^{30} \equiv 1\,(31) &\Rightarrow \left(7^{30}\right)^{33} \equiv 1^{33}\,(31) \text{ por Proposición 6.13-(i)} \\ &\Rightarrow \left(7^{30}\right)^{33} \equiv 1\,(31) \\ &\Rightarrow \left(7^{30}\right)^{33} \cdot 7^{25} \equiv 1 \cdot 7^{25}\,(31) \text{ por Proposición 6.13-(i)} \\ &\Rightarrow 7^{30\cdot 33+25} \equiv 7^{25}\,(31) \\ &\Rightarrow 7^{1015} \equiv 7^{25}\,(31) \end{aligned}$$

Ahora,

$$\begin{aligned} 7^2 = 49 = 1 \cdot 31 + 18 &\Rightarrow 7^2 \equiv 18\,(31) \\ &\Rightarrow 7^4 \equiv 18 \cdot 18\,(31) \text{ por Proposición 6.13-(i)} \\ &\Rightarrow 7^4 \equiv 324\,(31) \\ &\Rightarrow 7^4 \equiv 14\,(31) \text{ pues } 324 = 31 \cdot 10 + 14 \\ &\Rightarrow 7^8 \equiv 14 \cdot 14\,(31) \text{ Proposición 6.13-(i)} \\ &\Rightarrow 7^8 \equiv 196\,(31) \\ &\Rightarrow 7^8 \equiv 10\,(31) \text{ pues } 196 = 31 \cdot 6 + 10 \\ &\Rightarrow 7^{16} \equiv 100\,(31) \text{ por Proposición 6.13-(i)} \\ &\Rightarrow 7^{16} \equiv 7\,(31) \text{ pues } 100 = 31 \cdot 3 + 7 \\ &\Rightarrow 7^{16} \cdot 7^8 \equiv 7 \cdot 10\,(31) \text{ por Proposición 6.13-(i)} \\ &\Rightarrow 7^{24} \equiv 70\,(31) \\ &\Rightarrow 7^{24} \equiv 8\,(31) \text{ pues } 70 = 31 \cdot 2 + 8 \\ &\Rightarrow 7^{24} \cdot 7 \equiv 8 \cdot 7\,(31) \text{ por Proposición 6.13-(f)} \\ &\Rightarrow 7^{25} \equiv 56\,(31) \\ &\Rightarrow 7^{25} \equiv 25\,(31) \text{ pues } 56 = 31 \cdot 1 + 25 \end{aligned}$$

Esto dice que $7^{1015} \equiv 25\,(31)$.

Corolario 6.3

Sea $a \in \mathbb{Z}$ y p primo positivo. Luego,

(a) $a^{p^n} \equiv a\,(p)$ para todo $n \in \mathbb{N}$.

(b) Si $(a, p) = 1$ se cumple que $a^{p^n-1} \equiv 1\,(p)$ para todo $n \in \mathbb{N}$.

Demostración.

(a) Probemos el resultado por inducción en n. Para $n = 1$, el Teorema 6.13-(a) nos dice que $a^p \equiv a\,(p)$, es decir, $a^{p^1} \equiv a\,(p)$. Asumamos que el resultado es válido para n y veamos que vale para $n + 1$.

$$\begin{aligned} a^{p^n} \equiv a\,(p) &\Rightarrow \left(a^{p^n}\right)^p \equiv a^p \text{ por Proposición 6.13-(i)} \\ &\Rightarrow a^{p\cdot p^n} \equiv a^p\,(p) \\ &\Rightarrow a^{p^{n+1}} \equiv a^p\,(p) \\ &\Rightarrow a^{p^{n+1}} \equiv a\,(p) \text{ pues } a^p \equiv a\,(p) \text{ por Teorema 6.13-(a)} \end{aligned}$$

(b) Por (a) se tiene que $a^{p^n} \equiv a\,(p)$, es decir, $p \mid a^{p^n} - a$. O sea $p \mid a \cdot \left(a^{p^n-1} - 1\right)$. Como $(a, p) = 1$ el Teorema 6.7-(b) nos dice que $p \mid a^{p^n-1} - 1$. O sea que $a^{p^n-1} \equiv 1\,(p)$. ■

7. LOS NÚMEROS RACIONALES

7.1. Concepto

Definición 7.1
Llamaremos número racional a todo número real expresable en la forma

$$\frac{m}{n}$$

donde $m, n \in \mathbb{Z}$ *y* $n \neq 0$. *Denotamos con* $\mathbb{Q}$ *al conjunto de todos los números racionales.*

Recordemos que debido al Teorema 4.6-(c) cada $m \in \mathbb{Z}$ puede expresarse como $\frac{m}{1}$. Esto significa que $\mathbb{Z} \subset \mathbb{Q}$. Sin embargo, en realidad ocurre que $\mathbb{Z} \subsetneq \mathbb{Q}$ pues $\frac{1}{2} \in \mathbb{Q}$ pero $\frac{1}{2} \notin \mathbb{Z}$ (ver Ejemplo 5.2-(c)).

Además tenemos que $\mathbb{Q} \subsetneq \mathbb{R}$, pues $\sqrt{2} \notin \mathbb{Q}$ (ver Ejemplo 1.13-(c)).

Proposición 7.1 ($\mathbb{Q}$ es un cuerpo ordenado)
Sean $u, v \in \mathbb{Q}$. *Entonces*

(a) $u \pm v \in \mathbb{Q}$.

(b) $u \cdot v \in \mathbb{Q}$.

(c) Si $u \neq 0$ *entonces* $u^{-1} \in \mathbb{Q}$.

Demostración.

Como $u, v \in \mathbb{Q}$, existen $a, b, c, d \in \mathbb{Z}$ con $b \neq 0$ y $d \neq 0$ tal que $u = \frac{a}{b}$ y $v = \frac{c}{d}$.

(a)

$$\begin{aligned} u \pm v &= \frac{a}{b} \pm \frac{c}{d} \\ &= \frac{a \cdot d \pm b \cdot c}{b \cdot d} \text{ por Teorema 4.6-(i)} \\ &\in \mathbb{Q} \text{ por Teorema 6.1 y Teorema 4.5-(i)} \end{aligned}$$

(b)

$$\begin{aligned} u \cdot v &= \frac{a}{b} \cdot \frac{c}{d} \\ &= \frac{a \cdot c}{b \cdot d} \text{ por Teorema 4.6-(f)} \\ &\in \mathbb{Q} \text{ por Teorema 6.1 y Teorema 4.5-(i)} \end{aligned}$$

(c) Si $u \neq 0$ entonces $a \neq 0$. Luego,

$$\begin{aligned} u^{-1} &= \left(\frac{a}{b}\right)^{-1} \\ &= \frac{b}{a} \text{ por Teorema 4.6-(g)} \\ &\in \mathbb{Q} \text{ pues } a \neq 0 \end{aligned}$$

■

7.2. Supremo e ínfimo

Definición 7.2
Un subconjunto no vacío $K \subset \mathbb{R}$ se dice acotado superiormente (inferiormente) en $\mathbb{R}$ si existe $c \in \mathbb{R}$ tal que

$$\forall x \in K, x \leqslant c \quad (\forall x \in K, c \leqslant x)\,.$$

Definición 7.3 (Supremo e ínfimo)
Sea $K \subset \mathbb{R}$ acotado superiormente (inferiormente) en $\mathbb{R}$. Llamaremos supremo (ínfimo) de K al número m (si existe) que satisface:

(a) m es cota superior (inferior) de K.

(b) Si t es cota superior (inferior) de K entonces $m \leqslant t$ $(m \geqslant t)$.

Ejemplo 7.1
(a) Si $K = \{x \in \mathbb{R} : 0 \leqslant x \leqslant 1\}$ entonces 1 es el supremo de K.

(b) Si $K = \left\{ \dfrac{1}{n} : n \in \mathbb{N} \right\}$ entonces 0 es el ínfimo de K.

(c) Si $K = \left\{ 1 - \dfrac{1}{n} : n \in \mathbb{N} \right\}$ entonces 1 es el supremo de K.

Proposición 7.2
La condición de la Definición 7.3-(b) es equivalente a la condición:

(c) $\forall \varepsilon \in \mathbb{R}, \varepsilon > 0$ existe $k \in K : m - \varepsilon < k \quad (k < m + \varepsilon)$.

Demostración.
Veamos primero que (b) implica (c). Si $\varepsilon > 0$, entonces (b) dice que $m - \varepsilon$ $(m + \varepsilon)$ no puede ser una cota superior (inferior) de K. Esto significa que existe $k \in K$ tal que $m - \varepsilon < k$ $(k < m + \varepsilon)$.

Probemos ahora que (c) implica (b). Supongamos que t es cota superior (inferior) de K. Si ocurriese que $m > t$ $(m < t)$ entonces (c) nos dice que existe $k \in K$ tal que $m - (m - t) < k$ $(k < m + (t - m))$. Esto significa que $t < k$ $(k < t)$, lo cual es una contradicción pues t es una cota superior (inferior) de K. Por lo tanto se tiene que $m \leqslant t$ $(m \geqslant t)$. ■

7.3. Completitud de $\mathbb{R}$

Notemos que $\mathbb{Q}$ cumple los mismos axiomas que satisface $\mathbb{R}$. Hay algo que distingue y define de manera precisa a $\mathbb{R}$. Necesitamos introducir una nueva propiedad en la lista de las propiedades de $\mathbb{R}$ que es el axioma de completitud. Este axioma es la diferencia fundamental entre $\mathbb{Q}$ y $\mathbb{R}$.

Enunciaremos ahora el axioma de completitud que define completamente a los números reales.

(AC) Todo subconjunto no vacío de $\mathbb{R}$ acotado superiormente en $\mathbb{R}$ posee supremo en $\mathbb{R}$.

De esta manera, con este axioma adicional, $\mathbb{R}$ se convierte en un cuerpo ordenado y completo mientras que $\mathbb{Q}$ no lo es.

Proposición 7.3
Todo subconjunto no vacío de $\mathbb{R}$ acotado inferiormente en $\mathbb{R}$ posee ínfimo en $\mathbb{R}$.

Demostración.

Sea $K \subset \mathbb{R}$, $K \neq \varnothing$, acotado inferiormente en $\mathbb{R}$. Definimos:

$$H = \{-k : k \in K\}.$$

Como K es acotado inferiormente en $\mathbb{R}$, esto dice que existe $t \in \mathbb{R}$ tal que $t \leqslant k$ para todo $k \in K$. Luego $-k \leqslant -t$ para todo $k \in K$. Esto significa que $h \leqslant -t$ para todo $h \in H$, que es lo mismo que decir que H es acotado superiormente en $\mathbb{R}$. Como $K \neq \varnothing$ entonces $H \neq \varnothing$. Por el Axioma (AC) se tiene que H tiene supremo en $\mathbb{R}$ que llamaremos m. Veamos que $-m$ es el ínfimo de K:

- $-m$ es una cota inferior de K:

$$\begin{aligned} m \text{ es cota superior de } H &\Leftrightarrow \forall h \in H, h \leqslant m \\ &\Leftrightarrow \forall k \in K, -k \leqslant m \text{ por definición de } H \\ &\Leftrightarrow \forall k \in K, -m \leqslant k \\ &\Leftrightarrow -m \text{ es cota inferior de } K. \end{aligned}$$

- Sea t una cota inferior de K, entonces $-t$ es una cota superior de H (ya demostrado más arriba). Como m es el supremo de H entonces $m \leqslant -t$, lo que significa que $t \leqslant -m$. ■

7.4. Arquimedianidad

Teorema 7.1 (Arquimedianidad)
Para todo $x \in \mathbb{R}$ existe $n \in \mathbb{N}$ tal que $n > x$.

Demostración.

Razonemos por el absurdo, es decir, supongamos que existe $x \in \mathbb{R}$ tal que para todo $n \in \mathbb{N}$ se satisface que $n \leqslant x$. Se sigue que $\mathbb{N}$ tiene a x como cota superior en $\mathbb{R}$. Por el Axioma de completitud (AC) existe supremo de $\mathbb{N}$ en $\mathbb{R}$ que llamaremos x^*.

Si $x^* = n$ para algún natural n se tendría que $x^* = n < n + 1$, lo cual es una contradicción pues x^* es una cota superior de $\mathbb{N}$.

Debido a que x^* es cota superior debe ocurrir que $n < x^*$ cualquiera sea $n \in \mathbb{N}$. En particular, $n + 1 < x^*$ para cada $n \in \mathbb{N}$, lo cual es equivalente a que $n < x^* - 1$ para todo $n \in \mathbb{N}$. Esto dice que $x^* - 1$ es una cota superior de $\mathbb{N}$ más chica que el supremo x^*. Pero esto es una contradicción, que provino de suponer que el resultado del teorema no era válido. ■

Corolario 7.1
Sean $a, b \in \mathbb{R}$ con $a > 0$. Entonces existe $n \in \mathbb{N}$ tal que $n \cdot a > b$.

Demostración.

Por el Teorema 7.1 se tiene que existe $n \in \mathbb{N}$ tal que $n > \dfrac{b}{a}$. Como $a > 0$ se tiene que $n \cdot a > b$. ■

7.5. Densidad de $\mathbb{Q}$ en $\mathbb{R}$

Corolario 7.2 (Densidad de $\mathbb{Q}$ en $\mathbb{R}$)
Sean $x, y \in \mathbb{R}$ con $x < y$. Entonces existe $q \in \mathbb{Q}$ tal que $x < q < y$.

Demostración.

Por Teorema 7.1, existe $m \in \mathbb{N}$ tal que $m > -x$. Esto significa que $x + m > 0$, y además

$$0 < x + m < y + m.$$

Llamamos $\tilde{x} = x + m$, $\tilde{y} = y + m$. Por lo tanto tenemos que $0 < \tilde{x} < \tilde{y}$.

Como $\tilde{y} - \tilde{x} > 0$ se tiene que existe $n \in \mathbb{N}$ tal que $n \cdot (\tilde{y} - \tilde{x}) > 1$ debido al Corolario 7.1.

Por Teorema 7.1 existe $t \in \mathbb{N}$ tal que $t > n \cdot \tilde{x}$.

Definimos el conjunto $H = \{l \in \mathbb{N} : n \cdot \tilde{x} < l\}$. Notemos que $H \subset \mathbb{N}$ y $H \neq \varnothing$ (pues $t \in H$). Como $\mathbb{N}$ es bien ordenado, esto significa que H posee primer elemento que llamaremos h. Notemos que como $h \in H$ se tiene que $n \cdot \tilde{x} < h$. Ahora supongamos que $h \geqslant n \cdot \tilde{y}$:

$$\begin{aligned} 1 &< n \cdot (\tilde{y} - \tilde{x}) \\ &= n \cdot \tilde{y} - n \cdot \tilde{x} \\ &\leqslant h - n \cdot \tilde{x}, \end{aligned}$$

lo que dice que $0 < n \cdot \tilde{x} < h - 1$. Esto significa que $h - 1 \in \mathbb{N}$ y por lo tanto $h - 1 \in H$, lo cual es una contradicción pues h es el elemento minimal de H. Por lo tanto se cumple que:

$$\begin{aligned} n \cdot \tilde{x} < h < n \cdot \tilde{y} \quad &\Rightarrow \quad \tilde{x} < \frac{h}{n} < \tilde{y}, \\ &\Rightarrow \quad x + m < \frac{h}{n} < y + m, \\ &\Rightarrow \quad x < \frac{h}{n} - m < y, \end{aligned}$$

con $\dfrac{h}{n} - m \in \mathbb{Q}$. ■

7.6. Radicación

A continuación se enunciará una serie de lemas técnicos que nos permitirán definir la raíz cuadrada.

Lema 7.1

Sean $m, n \in \mathbb{N}$ con $m > 1$. Entonces $m^n > n$.

Demostración.

Vamos a probar el resultado por inducción en n.

Para $n = 1$ la propiedad es verdadera por la hipótesis $m > 1$.

Asumamos que la proposición $m^n > n$ es verdadera y veamos que $m^{n+1} > n + 1$. Luego:

$$\begin{aligned} n < m^n \quad &\Rightarrow \quad m \cdot n < m^{n+1} \text{ multiplicando por } m \\ &\Rightarrow \quad n < m \cdot n < m^{n+1} \text{ multiplicando la desigualdad } 1 < m \text{ por } n \\ &\Rightarrow \quad n + 1 \leqslant m \cdot n < m^{n+1} \text{ por Corolario 5.2-(a)} \end{aligned}$$

Por el Criterio 5.1 se tiene que $m^n > n$ para todo $n \in \mathbb{N}$. ■

Lema 7.2

Si $r \in \mathbb{R}$ con $r > 0$ y $m \in \mathbb{N}$ con $m > 1$, entonces existe $s \in \mathbb{N}$ tal que $0 < \dfrac{1}{m^s} < r$.

Demostración.

Consideremos el conjunto $K = \left\{m^k : k \in \mathbb{N}\right\}$. Notemos que K no es acotado superiormente en $\mathbb{R}$, pues si lo fuera existiría una cota superior $c \in \mathbb{R}$. Por Teorema 7.1 existe $j \in \mathbb{N}$ tal que $c < j$. Luego, $m^i \leqslant c < j$ para todo $i \in \mathbb{N}$. En particular, $m^j < j$, lo cual es una contradicción por lo visto anteriormente en el Lema 7.1.

Por Corolario 7.1 existe $n \in \mathbb{N}$ tal que $n \cdot r > 1$. Como n no puede ser cota superior de K existe $s \in \mathbb{N}$ tal que $n < m^s$, lo que significa que $1 < n \cdot r < m^s \cdot r$, lo cual implica que $0 < \dfrac{1}{m^s} < r$. ■

Corolario 7.3

(a) Dado $x \in \mathbb{R}$ con $x > 0$, existe $s \in \mathbb{N}$ tal que $0 < \dfrac{1}{10^s} < x$.

(b) Dado $x \in \mathbb{R}$ con $x > 0$, existe $y \in \mathbb{Q}$ tal que $0 < y^2 < y < x$.

Demostración.
(a) Es una aplicación directa del Lema 7.2 cuando $m = 10$.

(b) Debido al Lema 7.2 cuando $m = 2$ existe $s \in \mathbb{N}$ tal que $0 < \dfrac{1}{2^s} < x$. Además como $1 < 2^s$ se tiene que $\dfrac{1}{2^s} < 1$, lo que también implica que $\left(\dfrac{1}{2^s}\right)^2 < \dfrac{1}{2^s}$. Juntando todo se tiene que $0 < \left(\dfrac{1}{2^s}\right)^2 < \dfrac{1}{2^s} < x$, donde $\dfrac{1}{2^s} \in \mathbb{Q}$. ■

Proposición 7.4
Sea $r \in \mathbb{R}$ con $r > 0$. Entonces existe un único $s \in \mathbb{R}$ tal que $s > 0$ y $s^2 = r$.

Demostración.
Probaremos primero la existencia. Para ello, definimos el siguiente conjunto:

$$K = \left\{x \in \mathbb{R} : x > 0 \text{ y } x^2 \leqslant r\right\}.$$

Por Corolario 7.3-(b) se ve que $K \neq \varnothing$.

Asumamos por un momento que $r > 1$. Debido a esto se tiene que $r^2 > r$, con lo que tenemos que

$$\forall x \in K, x^2 \leqslant r < r^2.$$

Notemos que esto implica que $\forall x \in K, x < r$, pues si existiera $x \in K$ tal que $r \leqslant x$ entonces:

$$\begin{aligned} r \leqslant x &\Rightarrow r^2 \leqslant r \cdot x \text{ multiplicando la desigualdad } r \leqslant x \text{ por } r \text{ y usando que } r > 0 \\ &\Rightarrow r^2 \leqslant r \cdot x \leqslant x^2 \text{ multiplicando la desigualdad } r \leqslant x \text{ por } x \text{ y usando que } x > 0 \end{aligned}$$

lo cual es una contradicción.

Como $\forall x \in K, x < r$, se tiene que K es acotado superiormente en $\mathbb{R}$ por r. Por el Axioma (AC) existe el supremo de K que llamaremos s. Notemos que $s > 0$ pues $x \leqslant s$ para cualquier elemento de K y debido a que cada elemento de K es positivo.

Ahora veremos que $s^2 = r$. Razonando por el absurdo, asumamos que $s^2 \neq r$:

- Si $s^2 < r$:

  Por Corolario 7.3-(b) existe $\varepsilon > 0$ tal que $0 < \varepsilon^2 < \varepsilon < \dfrac{r - s^2}{1 + 2 \cdot s}$. Luego,

  $$r - s^2 > \varepsilon \cdot (1 + 2 \cdot s) = \varepsilon + 2 \cdot s \cdot \varepsilon > \varepsilon^2 + 2 \cdot s \cdot \varepsilon.$$

  Luego se tiene $r > s^2 + 2 \cdot s \cdot \varepsilon + \varepsilon^2 = (s + \varepsilon)^2$. Esto implica que $s + \varepsilon \in K$. Como s es, en particular, una cota superior de K se obtiene que $s + \varepsilon \leqslant s$, lo cual dice que $\varepsilon \leqslant 0$. Esto último es una contradicción.

- Si $s^2 > r$:

  Por Corolario 7.3-(b) existe $\varepsilon > 0$ tal que $0 < \varepsilon^2 < \varepsilon < \dfrac{s^2 - r}{2 \cdot s}$. Luego,

  $$s^2 - r > 2 \cdot s \cdot \varepsilon > 2 \cdot s \cdot \varepsilon - \varepsilon^2.$$

Luego se tiene $r < s^2 - 2 \cdot s \cdot \varepsilon + \varepsilon^2 = (s - \varepsilon)^2$. Notemos también que $0 < s - \varepsilon < s$, pues:

$$\varepsilon < \frac{s^2 - r}{2 \cdot s} = \frac{s}{2} - \frac{r}{2 \cdot s} < \frac{s}{2} < s.$$

Debido al hecho que s es el supremo de K, la Proposición 7.2 nos dice que existe $t \in K$ tal que $s - \varepsilon < t$, de donde se deduce que $(s - \varepsilon)^2 < t^2 \leqslant r$, lo cual es una contradicción.

Asumamos ahora que $r < 1$. Luego $\dfrac{1}{r} > 1$, y por lo demostrado anteriormente existe $s > 0$ tal que $s^2 = \dfrac{1}{r}$. Luego:

$$\begin{aligned} s^2 = \frac{1}{r} &\Rightarrow r = \frac{1}{s^2} \\ &\Rightarrow r = \left(\frac{1}{s}\right)^2. \end{aligned}$$

Por lo tanto existe un número real positivo tal que su cuadrado es igual a r.

Asumamos ahora que $r = 1$. En este caso, también existe $s \in \mathbb{R}$ tal que $s^2 = 1$ (la opción $s = 1$ sirve).

Probaremos ahora la unicidad. Supongamos que existen $s, h \in \mathbb{R}$ números positivos tales que $s^2 = r = h^2$. Luego

$$0 = s^2 - h^2 = (s - h) \cdot (s + h).$$

Esto significa que $h = s$ o $h = -s$. Supongamos que $h = -s$, entonces $0 < h = -s < 0$ lo cual es una contradicción. Por lo tanto $h = s$. ■

Definición 7.4
Sea $r \in \mathbb{R}$ con $r > 0$. Llamamos la raíz cuadrada positiva de r al único número real $s > 0$ que satisface $s^2 = r$ y lo denotamos con $\sqrt{r}$.

Más generalmente podemos probar que para todo $n \in \mathbb{N}$ y $r \in \mathbb{R}$ con $r > 0$ existe un único número real positivo y tal que $y^n = r$. El número y se denomina la raíz n-ésima de r y se denota por $\sqrt[n]{r}$.

A continuación veremos algunas propiedades de la radicación.

Proposición 7.5
Sean $a, b \in \mathbb{R}$ con $a > 0$ y $b > 0$, y $m, n \in \mathbb{N}$. Entonces:

(a) $\sqrt{a} > 0$.

(b) $(\sqrt{a})^2 = a$.

(c) $\sqrt{a^2} = a$.

(d) $\sqrt[n]{a \cdot b} = \sqrt[n]{a} \cdot \sqrt[n]{b}$.

(e) $\sqrt[n]{a^{-1}} = (\sqrt[n]{a})^{-1}$.

(f) $\sqrt[m]{\sqrt[n]{a}} = \sqrt[m \cdot n]{a}$.

(g) $a \leqslant b \Leftrightarrow \sqrt[n]{a} \leqslant \sqrt[n]{b}$.

(h) Si $a > 1$ y $n < m$ entonces $\sqrt[m]{a} < \sqrt[n]{a}$

Demostración.
(a) Por Definición 7.4.

(b) Por Definición 7.4.

(c) La ecuación $x^2 = a^2$ tiene sólo dos soluciones, a saber, $x = a$ o $x = -a$, pues

$$0 = x^2 - a^2 = (x + a) \cdot (x - a).$$

Como la raíz cuadrada es la solución positiva, tenemos que $\sqrt{a^2} = a$.

(d) Por definición se sabe que $\sqrt[n]{a} > 0$ y $\sqrt[n]{b} > 0$. Por lo tanto $\sqrt[n]{a} \cdot \sqrt[n]{b} > 0$. Además,

$$\left(\sqrt[n]{a} \cdot \sqrt[n]{b}\right)^n = \left(\sqrt[n]{a}\right)^n \cdot \left(\sqrt[n]{b}\right)^n = a \cdot b.$$

Por unicidad se tiene que $\sqrt[n]{a \cdot b} = \sqrt[n]{a} \cdot \sqrt[n]{b}$.

(e) Por definición se sabe que $\sqrt[n]{a} > 0$. Por lo tanto $\left(\sqrt[n]{a}\right)^{-1} > 0$. Además,

$$\left[\left(\sqrt[n]{a}\right)^{-1}\right]^n = \left(\frac{1}{\sqrt[n]{a}}\right)^n = \frac{1}{\left(\sqrt[n]{a}\right)^n} = \frac{1}{a} = a^{-1}.$$

Por unicidad se tiene que $\sqrt[n]{a^{-1}} = \left(\sqrt[n]{a}\right)^{-1}$.

(f) Por definición se sabe que $\sqrt[m]{\sqrt[n]{a}} > 0$. Ahora,

$$\left(\sqrt[m]{\sqrt[n]{a}}\right)^{m \cdot n} = \left[\left(\sqrt[m]{\sqrt[n]{a}}\right)^m\right]^n = \left[\sqrt[n]{a}\right]^n = a.$$

Por unicidad se tiene que $\sqrt[m]{\sqrt[n]{a}} = \sqrt[m \cdot n]{a}$.

(g) Asumamos que $a \leqslant b$. Si ocurriera que $\sqrt[n]{a} > \sqrt[n]{b}$ entonces $\left(\sqrt[n]{a}\right)^n > \left(\sqrt[n]{b}\right)^n$ por Proposición 5.3-(d). Luego $a > b$, lo cual es una contradicción, por lo que resulta que $\sqrt[n]{a} \leqslant \sqrt[n]{b}$.
Asumamos ahora que $\sqrt[n]{a} \leqslant \sqrt[n]{b}$. Entonces $\left(\sqrt[n]{a}\right)^n \leqslant \left(\sqrt[n]{b}\right)^n$ por Proposición 5.3-(d). Luego $a \leqslant b$.

(h) Supongamos que $\sqrt[m]{a} \geqslant \sqrt[n]{a}$. Ahora

$$\begin{aligned}
\sqrt[m]{a} \geqslant \sqrt[n]{a} &\Rightarrow \left(\sqrt[m]{a}\right)^m \geqslant \left(\sqrt[n]{a}\right)^m \text{ por Proposición 5.3-(d)} \\
&\Rightarrow a \geqslant \left(\sqrt[n]{a}\right)^m \\
&\Rightarrow a \geqslant \sqrt[n]{a^m} \text{ por (d)} \\
&\Rightarrow a^n \geqslant \left(\sqrt[n]{a^m}\right)^n \text{ por Proposición 5.3-(d)} \\
&\Rightarrow a^n \geqslant a^m
\end{aligned}$$

lo cual es una contradicción, debido a la Proposición 5.3-(g). ■

7.7. Potenciación racional de números reales

Definición 7.5 (Potenciación con exponentes racionales)
Sean $a \in \mathbb{R}$ con $a > 0$, $p, q \in \mathbb{Z}$ con $q > 0$. Definimos

$$a^{p/q} = \left(\sqrt[q]{a}\right)^p.$$

Cabe preguntarnos si la Definición 7.5 está bien definida cuando el exponente es un racional escrito de dos maneras distintas.

Observación 7.1
La potenciación con exponentes racionales está bien definida. Es decir, si $p, q, u, v \in \mathbb{Z}$ con $q > 0$ y $v > 0$, se tiene que:

$$\frac{p}{q} = \frac{u}{v} \Rightarrow a^{p/q} = a^{u/v}.$$

Demostración.
Asumamos primero que $p = 0$. Luego, debe ocurrir que $u = 0$. Ahora

$$\begin{aligned} a^{p/q} &= \left(\sqrt[q]{a}\right)^p \text{ por Definición 7.5} \\ &= \left(\sqrt[q]{a}\right)^0 \\ &= 1 \\ &= \left(\sqrt[v]{a}\right)^0 \\ &= \left(\sqrt[v]{a}\right)^u \\ &= a^{u/v} \text{ por Definición 7.5} \end{aligned}$$

Asumamos ahora que $p > 0$. Luego, debe ocurrir que $u > 0$. Ahora si ocurriera que $a^{p/q} < a^{u/v}$ tendríamos:

$$\begin{aligned} a^{p/q} < a^{u/v} &\Rightarrow \left(\sqrt[q]{a}\right)^p < \left(\sqrt[v]{a}\right)^u \text{ por Definición 7.5} \\ &\Rightarrow \left[\left(\sqrt[q]{a}\right)^p\right]^q < \left[\left(\sqrt[v]{a}\right)^u\right]^q \text{ por Proposición 5.3-(d)} \\ &\Rightarrow \left(\sqrt[q]{a}\right)^{p\cdot q} < \left(\sqrt[v]{a}\right)^{u\cdot q} \text{ por Proposición 5.3-(b)} \\ &\Rightarrow \left(\sqrt[q]{a}\right)^{q\cdot p} < \left(\sqrt[v]{a}\right)^{q\cdot u} \\ &\Rightarrow \left[\left(\sqrt[q]{a}\right)^q\right]^p < \left(\sqrt[v]{a}\right)^{q\cdot u} \text{ por Proposición 5.3-(b)} \\ &\Rightarrow a^p < \left(\sqrt[v]{a}\right)^{q\cdot u} \text{ por definición de raíz } q\text{–ésima} \\ &\Rightarrow \sqrt[p]{a^p} < \sqrt[p]{\left(\sqrt[v]{a}\right)^{q\cdot u}} \text{ por Proposición 7.5-(g)} \\ &\Rightarrow \left(\sqrt[p]{a}\right)^p < \sqrt[p]{\sqrt[v]{a^{q\cdot u}}} \text{ por Proposición 7.5-(d)} \\ &\Rightarrow a < \sqrt[p\cdot v]{a^{q\cdot u}} \text{ por Proposición 7.5-(f) y definición de raíz } p\text{–ésima} \\ &\Rightarrow a < \sqrt[q\cdot u]{a^{q\cdot u}} \text{ pues } p\cdot v = q\cdot u \\ &\Rightarrow a < \left(\sqrt[q\cdot u]{a}\right)^{q\cdot u} \text{ por Proposición 7.5-(d)} \\ &\Rightarrow a < a \text{ por definición de raíz } q\cdot u\text{–ésima} \end{aligned}$$

lo cual es una contradicción. Lo mismo ocurre si suponemos que $a^{p/q} > a^{u/v}$.
Asumamos ahora que $p < 0$. Luego, debe ocurrir que $u < 0$. Ahora

$$\begin{aligned} a^{p/q} &= \left(\sqrt[q]{a}\right)^p \text{ por Definición 7.5} \\ &= \left(\frac{1}{\sqrt[q]{a}}\right)^{-p} = \frac{1}{\left(\sqrt[q]{a}\right)^{-p}} \text{ por propiedades de la potenciación} \\ &= \frac{1}{a^{(-p)/q}} \\ &= \frac{1}{a^{(-u)/v}} \text{ pues } \frac{-p}{q} = \frac{-u}{v} \text{ donde } -p, q, -u, v \in \mathbb{N} \end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{(\sqrt[v]{a})^{-u}} = \left(\frac{1}{\sqrt[v]{a}}\right)^{-u} \text{ por propiedades de la potenciación} \\
&= \left(\sqrt[v]{a}\right)^{u} \\
&= a^{u/v}
\end{aligned}
$$

■

Observación 7.2
Sean $a \in \mathbb{R}$ con $a > 0$, $p, q \in \mathbb{Z}$ con $q > 0$. Entonces

$$a^{p/q} = \sqrt[q]{a^p}.$$

Demostración.

Asumamos que $p = 0$. Luego,

$$a^{p/q} = \left(\sqrt[q]{a}\right)^0 = 1 = \sqrt[q]{1} = \sqrt[q]{a^0} = \sqrt[q]{a^p}.$$

Asumamos que $p > 0$. Luego,

$$
\begin{aligned}
a^{p/q} &= \left(\sqrt[q]{a}\right)^p \text{ por Definición 7.5} \\
&= \sqrt[q]{a^p} \text{ por Proposición 7.5-(d)}
\end{aligned}
$$

Asumamos que $p < 0$. Luego,

$$
\begin{aligned}
a^{p/q} &= \left(\sqrt[q]{a}\right)^p \text{ por Definición 7.5} \\
&= \left(\frac{1}{\sqrt[q]{a}}\right)^{-p} = \frac{1}{(\sqrt[q]{a})^{-p}} \\
&= \frac{1}{\sqrt[q]{a^{-p}}} \text{ por caso anterior} \\
&= \frac{\sqrt[q]{1}}{\sqrt[q]{a^{-p}}} \\
&= \sqrt[q]{\frac{1}{a^{-p}}} \text{ por Proposición 7.5-(d) y 7.5-(e)} \\
&= \sqrt[q]{\left(\frac{1}{a}\right)^{-p}} \\
&= \sqrt[q]{a^p}
\end{aligned}
$$

■

Proposición 7.6
Sean $a, b \in \mathbb{R}$ con $a > 0$ y $b > 0$. Si $r, s \in \mathbb{Q}$ entonces:

(a) $a^r \cdot a^s = a^{r+s}$.

(b) $(a^r)^{-1} = a^{-r}$.

(c) $\dfrac{a^r}{a^s} = a^{r-s}$.

(d) $(a^r)^s = a^{r \cdot s}$.

(e) $(a \cdot b)^r = a^r \cdot b^r$.

Demostración.

Supongamos que $r = p/q$ y $s = u/v$ con $p, q, u, v \in \mathbb{Z}$, $q > 0$ y $v > 0$.

(a)

$$\begin{aligned}
a^r \cdot a^s &= a^{\frac{p}{q}} \cdot a^{\frac{u}{v}} \\
&= a^{\frac{p\cdot v}{q\cdot v}} \cdot a^{\frac{q\cdot u}{q\cdot v}} \text{ por Observación 7.1} \\
&= \left(\sqrt[q\cdot v]{a}\right)^{p\cdot v} \cdot \left(\sqrt[q\cdot v]{a}\right)^{q\cdot u} \text{ por Definición 7.5} \\
&= \sqrt[q\cdot v]{a^{p\cdot v}} \cdot \sqrt[q\cdot v]{a^{q\cdot u}} \text{ por Observación 7.2} \\
&= \sqrt[q\cdot v]{a^{p\cdot v} \cdot a^{q\cdot u}} \text{ por Proposición 7.5-(d)} \\
&= \sqrt[q\cdot v]{a^{p\cdot v+q\cdot u}} \text{ por Teorema 6.10-(a)} \\
&= \left(\sqrt[q\cdot v]{a}\right)^{p\cdot v+q\cdot u} \text{ por Observación 7.2} \\
&= a^{\frac{p\cdot v+q\cdot u}{q\cdot v}} \text{ por Definición 7.5} \\
&= a^{\frac{p}{q}+\frac{u}{v}} \\
&= a^{r+s}
\end{aligned}$$

(b)

$$\begin{aligned}
a^r \cdot a^{-r} &= a^{r-r} \text{ por (a)} \\
&= a^0 \\
&= 1
\end{aligned}$$

Por unicidad del inverso, tenemos que $(a^r)^{-1} = a^{-r}$.

(c)

$$\begin{aligned}
\frac{a^r}{a^s} &= a^r \cdot (a^s)^{-1} \\
&= a^r \cdot a^{-s} \text{ por (b)} \\
&= a^{r-s} \text{ por (a)}
\end{aligned}$$

(d)

$$\begin{aligned}
(a^r)^s &= \left(a^{p/q}\right)^{u/v} \\
&= \left[\left(\sqrt[q]{a}\right)^p\right]^{u/v} \text{ por Definición 7.5} \\
&= \left(\sqrt[q]{a^p}\right)^{u/v} \text{ por Observación 7.2} \\
&= \left(\sqrt[v]{\sqrt[q]{a^p}}\right)^u \text{ por Definición 7.5} \\
&= \sqrt[v]{\left(\sqrt[q]{a^p}\right)^u} \text{ por Observación 7.2} \\
&= \sqrt[v]{\sqrt[q]{(a^p)^u}} \text{ por Observación 7.2} \\
&= \sqrt[v]{\sqrt[q]{a^{p\cdot u}}} \text{ por Teorema 6.10-(b)} \\
&= \sqrt[v\cdot q]{a^{p\cdot u}} \text{ por Proposición 7.5-(f)} \\
&= \sqrt[q\cdot v]{a^{p\cdot u}}
\end{aligned}$$

$$
\begin{aligned}
&= \left(\sqrt[q\cdot v]{a}\right)^{p\cdot u} \text{ por Observación 7.2}\\
&= a^{\frac{p\cdot u}{q\cdot v}} \text{ por Definición 7.5}\\
&= a^{\frac{p}{q}\cdot\frac{u}{v}}\\
&= a^{r\cdot s}
\end{aligned}
$$

(e)

$$
\begin{aligned}
(a\cdot b)^r &= (a\cdot b)^{\frac{p}{q}}\\
&= \left(\sqrt[q]{a\cdot b}\right)^p \text{ por Definición 7.5}\\
&= \sqrt[q]{(a\cdot b)^p} \text{ por Observación 7.2}\\
&= \sqrt[q]{a^p\cdot b^p} \text{ por Teorema 6.10-(d)}\\
&= \sqrt[q]{a^p}\cdot\sqrt[q]{b^p} \text{ por Proposición 7.5-(d)}\\
&= \left(\sqrt[q]{a}\right)^p\cdot\left(\sqrt[q]{b}\right)^p \text{ por Observación 7.2}\\
&= a^{\frac{p}{q}}\cdot b^{\frac{p}{q}} \text{ por Definición 7.5}\\
&= a^r\cdot b^r
\end{aligned}
$$

Esto concluye la prueba. ■

8. LOS NÚMEROS COMPLEJOS

8.1. Concepto: forma de par ordenado

Definición 8.1 (Forma de par ordenado)
Definimos el conjunto de los números complejos como el conjunto $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ *equipado con dos operaciones*

$$\begin{aligned} + &: \mathbb{C} \times \mathbb{C} \to \mathbb{C}, \quad \textit{suma}, \\ \cdot &: \mathbb{C} \times \mathbb{C} \to \mathbb{C}, \quad \textit{producto}, \end{aligned}$$

definidas por

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

Proposición 8.1 ($\mathbb{C}$ es un cuerpo)
En el conjunto $\mathbb{C}$ *las operaciones de suma y producto satisfacen las siguientes propiedades:*

(a) La suma es asociativa: dados $(a,b), (c,d), (e,f) \in \mathbb{C}$*, entonces*

$$(a,b) + [(c,d) + (e,f)] = [(a,b) + (c,d)] + (e,f).$$

(b) La suma es conmutativa: dados $(a,b), (c,d) \in \mathbb{C}$*, entonces*

$$(a,b) + (c,d) = (c,d) + (a,b).$$

(c) Existencia del elemento neutro para la suma: dado $(a,b) \in \mathbb{C}$*, entonces*

$$(a,b) + (0,0) = (a,b).$$

(d) Existencia del opuesto: dado un elemento $(a,b) \in \mathbb{C}$*, entonces*

$$(a,b) + (-a,-b) = (0,0).$$

(e) El producto es asociativo: dados $(a,b), (c,d), (e,f) \in \mathbb{C}$*, entonces*

$$(a,b) \cdot [(c,d) \cdot (e,f)] = [(a,b) \cdot (c,d)] \cdot (e,f).$$

(f) El producto es conmutativo: dados $(a,b), (c,d) \in \mathbb{C}$*, entonces*

$$(a,b) \cdot (c,d) = (c,d) \cdot (a,b).$$

(g) Existencia del elemento neutro para el producto: dado $(a,b) \in \mathbb{C}$*, entonces*

$$(a,b) \cdot (1,0) = (a,b).$$

(notar que $(1,0) \neq (0,0)$*).*

(h) Existencia del inverso: dado un elemento $(a,b) \in \mathbb{C}$*, con* $(a,b) \neq (0,0)$ *entonces*

$$(a,b) \cdot \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2} \right) = (1,0).$$

(i) Distributiva del producto respecto de la suma: dados dados $(a,b),(c,d),(e,f) \in \mathbb{C}$*, entonces*

$$(a,b)\cdot[(c,d)+(e,f)] = (a,b)\cdot(c,d)+(a,b)\cdot(e,f).$$

Demostración.
(a) Vamos a mostrar que $(a,b)+[(c,d)+(e,f)] = [(a,b)+(c,d)]+(e,f)$.

$$\begin{aligned}
(a,b)+[(c,d)+(e,f)] &= (a,b)+(c+e,d+f) \text{ por definición de suma en } \mathbb{C}\\
&= (a+(c+e),b+(d+f)) \text{ por definición de suma en } \mathbb{C}\\
&= ((a+c)+e,(b+d)+f) \text{ por Axioma (S1)}\\
&= (a+c,b+d)+(e,f) \text{ por definición de suma en } \mathbb{C}\\
&= [(a,b)+(c,d)]+(e,f) \text{ por definición de suma en } \mathbb{C}
\end{aligned}$$

(b) Demostraremos que $(a,b)+(c,d) = (c,d)+(a,b)$.

$$\begin{aligned}
(a,b)+(c,d) &= (a+c,b+d) \text{ por definición de suma en } \mathbb{C}\\
&= (c+a,d+b) \text{ por Axioma (S2)}\\
&= (c,d)+(a,b) \text{ por definición de suma en } \mathbb{C}
\end{aligned}$$

(c) Probaremos que $(a,b)+(0,0) = (a,b)$.

$$\begin{aligned}
(a,b)+(0,0) &= (a+0,b+0) \text{ por definición de suma en } \mathbb{C}\\
&= (a,b) \text{ por Axioma (S3)}
\end{aligned}$$

(d) Mostraremos que $(a,b)+(-a,-b) = (0,0)$.

$$\begin{aligned}
(a,b)+(-a,-b) &= (a+(-a),b+(-b)) \text{ por definición de suma en } \mathbb{C}\\
&= (0,0) \text{ por Axioma (S4)}
\end{aligned}$$

(e) Veremos que $(a,b)\cdot[(c,d)\cdot(e,f)] = [(a,b)\cdot(c,d)]\cdot(e,f)$. Aplicando la definición del producto en $\mathbb{C}$ repetidas veces y el Axioma (D) se tiene

$$\begin{aligned}
(a,b)\cdot[(c,d)\cdot(e,f)] &= (a,b)\cdot(c\cdot e-d\cdot f,c\cdot f+d\cdot e)\\
&= (a\cdot(c\cdot e-d\cdot f)-b\cdot(c\cdot f+d\cdot e),a\cdot(c\cdot f+d\cdot e)+b\cdot(c\cdot e-d\cdot f))\\
&= (a\cdot c\cdot e-a\cdot d\cdot f-b\cdot c\cdot f-b\cdot d\cdot e,a\cdot c\cdot f+a\cdot d\cdot e+b\cdot c\cdot e-b\cdot d\cdot f)
\end{aligned}$$

Análogamente,

$$\begin{aligned}
[(a,b)\cdot(c,d)]\cdot(e,f) &= (a\cdot c-b\cdot d,a\cdot d+b\cdot c)\cdot(e,f)\\
&= ((a\cdot c-b\cdot d)\cdot e-(a\cdot d+b\cdot c)\cdot f,(a\cdot c-b\cdot d)\cdot f+(a\cdot d+b\cdot c)\cdot e)\\
&= (a\cdot c\cdot e-b\cdot d\cdot e-a\cdot d\cdot f-b\cdot c\cdot f,a\cdot c\cdot f-b\cdot d\cdot f+a\cdot d\cdot e+b\cdot c\cdot e)
\end{aligned}$$

Se puede comprobar que se cumple la propiedad asociativa comparando término a término.

(f) Vamos a probar que $(a,b)\cdot(c,d) = (c,d)\cdot(a,b)$.

$$(a,b)\cdot(c,d) = (a\cdot c-b\cdot d,a\cdot d+b\cdot c) \text{ por definición de producto en } \mathbb{C}$$

$$
\begin{aligned}
&= (c\cdot a - d\cdot b, d\cdot a + c\cdot b) \text{ por Axioma (P2)}\\
&= (c,d)\cdot(a,b) \text{ por definición de producto en } \mathbb{C}
\end{aligned}
$$

(g) Demostraremos que $(a,b)\cdot(1,0) = (a,b)$.

$$
\begin{aligned}
(a,b)\cdot(1,0) &= (a\cdot 1 - b\cdot 0, a\cdot 0 + b\cdot 1) \text{ por definición de producto en } \mathbb{C}\\
&= (a,b) \text{ por propiedades de } \mathbb{R}
\end{aligned}
$$

(h) Probaremos que $(a,b)\cdot\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right) = (1,0)$. Notar que como $(a,b)\neq(0,0)$ se tiene que $a^2+b^2\neq 0$ (ver Teorema 4.7-(r)). Aplicando la definición de producto en $\mathbb{C}$ tenemos:

$$
\begin{aligned}
(a,b)\cdot\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right) &= \left(a\cdot\left(\frac{a}{a^2+b^2}\right) - b\cdot\left(\frac{-b}{a^2+b^2}\right), a\cdot\left(\frac{-b}{a^2+b^2}\right) + b\cdot\left(\frac{a}{a^2+b^2}\right)\right)\\
&= \left(\frac{a^2+b^2}{a^2+b^2}, \frac{-a\cdot b + a\cdot b}{a^2+b^2}\right)\\
&= (1,0)
\end{aligned}
$$

(i) Mostraremos que $(a,b)\cdot[(c,d)+(e,f)] = (a,b)\cdot(c,d) + (a,b)\cdot(e,f)$.

$$
\begin{aligned}
(a,b)\cdot[(c,d)+(e,f)] &= (a,b)\cdot(c+e, d+f) \text{ por definición de suma en } \mathbb{C}\\
&= (a\cdot(c+e) - b\cdot(d+f), a\cdot(d+f) + b\cdot(c+e)) \text{ por definición de producto en } \mathbb{C}\\
&= (a\cdot c + a\cdot e - b\cdot d - b\cdot f, a\cdot d + a\cdot f + b\cdot c + b\cdot e) \text{ por Axioma (D)}
\end{aligned}
$$

Análogamente,

$$
\begin{aligned}
(a,b)\cdot(c,d) + (a,b)\cdot(e,f) &= (a\cdot c - b\cdot d, a\cdot d + b\cdot c)\\
&+ (a\cdot e - b\cdot f, a\cdot f + b\cdot e) \text{ por definición de producto en } \mathbb{C}\\
&= (a\cdot c - b\cdot d + a\cdot e - b\cdot f, a\cdot d + b\cdot c + a\cdot f + b\cdot e) \text{ por definición de suma en } \mathbb{C}
\end{aligned}
$$

Se puede comprobar que se cumple la propiedad distributiva comparando término a término. ■

Debido a que $\mathbb{C}$ satisface las propiedades del Teorema 8.1 se dice que $\mathbb{C}$ es un cuerpo. A diferencia de $\mathbb{R}$, $\mathbb{C}$ no dispone de un orden.

Ejemplo 8.1

(a) Sumar los números complejos $(-1,2)$ y $(3,5)$.

La suma, de acuerdo a la Definición 8.1, es:

$$
\begin{aligned}
(-1,2) + (3,5) &= (-1+3, 2+5)\\
&= (2,7)\,.
\end{aligned}
$$

(b) Multiplicar los números complejos $(7,-1)$ y $(-3,4)$.

El producto, de acuerdo a la Definición 8.1, es:

$$
\begin{aligned}
(7,-1)\cdot(-3,4) &= (7\cdot(-3) - (-1)\cdot 4, 7\cdot 4 + (-1)\cdot(-3))\\
&= (-21+4, 28+3)\\
&= (-17,31)\,.
\end{aligned}
$$

(c) Calcular el opuesto de $(6,-9)$.

El opuesto (de acuerdo a la Proposición 8.1-(d)) es $(-6,9)$. Comprobando:

$$\begin{aligned}(6,-9)+(-6,9) &= (6-6,-9+9)\\ &= (0,0)\,.\end{aligned}$$

(d) Calcular el inverso de $(3,-4)$.

El inverso (de acuerdo a la Proposición 8.1-(h)) es $\left(\frac{3}{25},\frac{4}{25}\right)$. Comprobando:

$$\begin{aligned}(3,-4)\cdot\left(\frac{3}{25},\frac{4}{25}\right) &= \left(3\cdot\frac{3}{25}-(-4)\cdot\frac{4}{25},3\cdot\frac{4}{25}+(-4)\cdot\frac{3}{25}\right)\\ &= \left(\frac{9}{25}+\frac{16}{25},\frac{12}{25}-\frac{12}{25}\right)\\ &= (1,0)\,.\end{aligned}$$

8.2. Concepto: forma binómica

Observación 8.1
Sean $a,b\in\mathbb{R}$. Entonces:

(a) $(a,b)=(a,0)+(b,0)\cdot(0,1)$.

(b) Si llamamos $i=(0,1)$ entonces $i^2=(-1,0)$ (aquí interpretamos $i^2=(0,1)\cdot(0,1)$).

Demostración.
(a) Vamos a probar que $(a,b)=(a,0)+(b,0)\cdot(0,1)$.

$$\begin{aligned}(a,0)+(b,0)\cdot(0,1) &= (a,0)+(b\cdot 0-0\cdot 1,b\cdot 1+0\cdot 0) \text{ por definición de producto en } \mathbb{C}\\ &= (a,0)+(0,b) \text{ por propiedades de } \mathbb{R}\\ &= (a,b) \text{ por definición de suma en } \mathbb{C}\end{aligned}$$

(b) Mostraremos que $i^2=(-1,0)$.

$$\begin{aligned}i^2 &= (0,1)\cdot(0,1)\\ &= (0\cdot 0-1\cdot 1,0\cdot 1+1\cdot 0) \text{ por definición de producto en } \mathbb{C}\\ &= (-1,0)\end{aligned}$$

■

Observación 8.2
La función $f:\mathbb{R}\to\mathbb{C}$ definida por

$$f(a)=(a,0)\,,$$

satisface las siguientes propiedades:

(a) f es inyectiva.

(b) f preserva la suma, es decir:

$$f(a+b)=f(a)+f(b)\,.$$

(c) f preserva el producto, es decir:

$$f(a \cdot b) = f(a) \cdot f(b).$$

Demostración.
(a) Veamos que f es inyectiva.

$$\begin{aligned} f(a) = f(b) &\Rightarrow (a,0) = (b,0) \\ &\Rightarrow a = b. \end{aligned}$$

(b) Observemos que $f(a+b) = f(a) + f(b)$.

$$\begin{aligned} f(a+b) &= (a+b,0) \\ &= (a,0) + (b,0) \\ &= f(a) + f(b). \end{aligned}$$

(c) Comprobemos que $f(a \cdot b) = f(a) \cdot f(b)$.

$$\begin{aligned} f(a) \cdot f(b) &= (a,0) \cdot (b,0) \\ &= (a \cdot b - 0 \cdot 0, a \cdot 0 + 0 \cdot b) \\ &= (a \cdot b, 0) \\ &= f(a \cdot b). \end{aligned}$$

■

La Observación 8.2 dice, en otras palabras, que hay una copia de $\mathbb{R}$ en $\mathbb{C}$, y esa copia no es otra cosa que $\mathbb{R} \times \{0\}$. Por lo tanto, podemos realizar una identificación (o cambio de nombre) entre $\mathbb{R}$ y $\mathbb{R} \times \{0\}$. Notar también que la identificación también involucra a las operaciones de suma y producto. Esta es la razón por la cual se dice que $\mathbb{R} \subset \mathbb{C}$. De ahora en más no haremos más la distinción entre la suma y producto en $\mathbb{C}$ y la suma y producto en $\mathbb{R}$.

En virtud de las observaciones 8.1 y 8.2 cualquier número complejo se puede identificar de la siguiente manera:

$$(a,b) \leftrightarrow a + b \cdot i, \qquad \text{forma binómica de un número complejo}$$

donde $i^2 = -1$. Esta última expresión no nos permite escribir $i = \sqrt{-1}$, primero debido a que la raíz cuadrada no está definida para números negativos. Pero si pudiéramos hacerlo y valieran las propiedades de la radicación, sería válido razonar de la siguiente manera:

$$-1 = i^2 = \sqrt{-1} \cdot \sqrt{-1} = \sqrt{(-1) \cdot (-1)} = \sqrt{1} = 1,$$

lo cual es falso.

De ahora en más pensaremos siempre en esta identificación, pero sabiendo siempre su significado. De esta manera la traducción vía esta identificación sería:

- Definición del conjunto $\mathbb{C}$ (en forma binómica):

$$\mathbb{C} = \{a + b \cdot i : a, b \in \mathbb{R}\}.$$

- El conjunto de los números reales puede pensarse como un subconjunto de $\mathbb{C}$, a saber:

$$\mathbb{R} = \{a + b \cdot i \in \mathbb{C} : b = 0\}.$$

- Suma y producto:

$$\begin{aligned}(a+b\cdot i)+(c+d\cdot i) &= (a+c)+(b+d)\cdot i,\\ (a+b\cdot i)\cdot(c+d\cdot i) &= (a\cdot c-b\cdot d)+(a\cdot d+b\cdot c)\cdot i.\end{aligned}$$

  Notar que para el producto sólo basta con utilizar la propiedad distributiva:

$$\begin{aligned}(a+b\cdot i)\cdot(c+d\cdot i) &= a\cdot c+a\cdot d\cdot i+b\cdot i\cdot c+b\cdot d\cdot i^2\\ &= a\cdot c+a\cdot d\cdot i+b\cdot c\cdot i-b\cdot d \text{ pues } i^2=-1\\ &= (a\cdot c-b\cdot d)+(a\cdot d+b\cdot c)\cdot i.\end{aligned}$$

- Elemento neutro para la suma: 0.
- Elemento neutro para el producto: 1.
- Si $z=a+b\cdot i$ entonces su opuesto es $-z=-a-b\cdot i$.
- Si $z=a+b\cdot i$ donde $z\neq 0$ entonces su inverso es $z^{-1}=\dfrac{a-b\cdot i}{a^2+b^2}$.

Ejemplo 8.2
La fórmula del inverso de un número complejo no nulo puede obtenerse "racionalizando", es decir, multiplicando y dividiendo por el mismo número complejo pero cambiando el signo del término que tiene a i. Veamos los siguientes ejemplos:

(a)

$$\begin{aligned}\frac{1}{2+3\cdot i} &= \frac{1}{2+3\cdot i}\cdot\frac{2-3\cdot i}{2-3\cdot i}\\ &= \frac{2-3\cdot i}{(2+3\cdot i)\cdot(2-3\cdot i)}\\ &= \frac{2-3\cdot i}{2^2-3^2\cdot i^2}\\ &= \frac{2-3\cdot i}{2^2+3^2}\\ &= \frac{2-3\cdot i}{13}\\ &= \frac{2}{13}-\frac{3}{13}\cdot i\end{aligned}$$

(b)

$$\begin{aligned}\frac{1}{-3-4\cdot i} &= \frac{1}{-3-4\cdot i}\cdot\frac{-3+4\cdot i}{-3+4\cdot i}\\ &= \frac{-3+4\cdot i}{(-3-4\cdot i)\cdot(-3+4\cdot i)}\\ &= \frac{-3+4\cdot i}{(-3)^2-4^2\cdot i^2}\\ &= \frac{-3+4\cdot i}{3^2+4^2}\\ &= \frac{-3+4\cdot i}{25}\\ &= -\frac{3}{25}+\frac{4}{25}\cdot i\end{aligned}$$

8.3. Partes real e imaginaria, conjugado y módulo

Definición 8.2 (Parte real e imaginaria)
Dado $z = a + b \cdot i \in \mathbb{C}$ diremos que

(a) a es la parte real de z y lo denotaremos de la siguiente manera: $a = \mathrm{Re}\,(z)$.

(b) b es la parte imaginaria de z y lo denotaremos de la siguiente manera: $b = \mathrm{Im}\,(z)$.

Ejemplo 8.3
(a) Si $z = 3 - 7 \cdot i$ entonces $\mathrm{Re}\,(z) = 3$ y $\mathrm{Im}\,(z) = -7$.

(b) Si $z = -4 + 2 \cdot i$ entonces $\mathrm{Re}\,(z) = -4$ y $\mathrm{Im}\,(z) = 2$.

(c) Si $z = 6$ entonces $\mathrm{Re}\,(z) = 6$ y $\mathrm{Im}\,(z) = 0$.

(d) Si $z = 9 \cdot i$ entonces $\mathrm{Re}\,(z) = 0$ y $\mathrm{Im}\,(z) = 9$.

Es claro que la parte real e imaginaria de un número complejo son números reales. Además es claro que si $z, w \in \mathbb{C}$:

$$z = w \Leftrightarrow \begin{cases} \mathrm{Re}\,(z) &= \mathrm{Re}\,(w) \\ \mathrm{Im}\,(z) &= \mathrm{Im}\,(w) \end{cases}$$

Definición 8.3 (Conjugado y módulo)
Sea $z = a + b \cdot i \in \mathbb{C}$.

(a) Se define el conjugado de z al número complejo $\overline{z} = a - b \cdot i$.

(b) Se define el módulo de z al número real no negativo $|z| = \sqrt{a^2 + b^2}$.

Ejemplo 8.4
(a) Si $z = 5 + 2 \cdot i$ entonces $\overline{z} = 5 - 2 \cdot i$ y $|z| = \sqrt{5^2 + 2^2} = \sqrt{29}$.

(b) Si $z = 4 - 3 \cdot i$ entonces $\overline{z} = 4 + 3 \cdot i$ y $|z| = \sqrt{4^2 + (-3)^2} = \sqrt{25} = 5$.

(c) Si $z = 7$ entonces $\overline{z} = 7$ y $|z| = \sqrt{7^2 + 0^2} = \sqrt{49} = 7$.

(d) Si $z = 9 \cdot i$ entonces $\overline{z} = -9 \cdot i$ y $|z| = \sqrt{0^2 + 9^2} = \sqrt{81} = 9$.

Proposición 8.2
Sean $z, w \in \mathbb{C}$. Entonces:

(a) $\overline{z + w} = \overline{z} + \overline{w}$.

(b) $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$.

(c) $\overline{\overline{z}} = z$.

(d) $z + \overline{z} = 2 \cdot \mathrm{Re}\,(z)$ y $z - \overline{z} = 2 \cdot \mathrm{Im}\,(z) \cdot i$.

(e) $z \in \mathbb{R}$ si y sólo si $z = \overline{z}$.

(f) Si $a \in \mathbb{R}$ entonces el módulo de a, visto como número complejo, es igual al valor absoluto de a, con lo cual no hay ambigüedad en la notación.

(g) $|z|$ es la distancia del número complejo z al origen de coordenadas $(0, 0)$.

(h) $|z| = 0$ si y sólo si $z = 0$.

(i) $z \cdot \overline{z} = |z|^2$.

(j) *Si* $z \neq 0$ *entonces* $z^{-1} = \dfrac{\overline{z}}{|z|^2}$.

(k) *Si* $z \neq 0$ *entonces* $(\overline{z})^{-1} = \overline{z^{-1}}$.

(l) $|\overline{z}| = |z|$.

(m) $|\mathrm{Re}\,(z)| \leqslant |z|$ *y* $|\mathrm{Im}\,(z)| \leqslant |z|$.

(n) $|z \cdot w| = |z| \cdot |w|$.

(ñ) *Si* $z \neq 0$ *entonces* $|z^{-1}| = |z|^{-1}$.

(o) $|z + w| \leqslant |z| + |w|$ *(desigualdad triangular).*

(p) $|-z| = |z|$.

(q) $\Big|\,|z| - |w|\,\Big| \leqslant |z - w|$.

Demostración.
En toda la demostración, asumiremos que $z = a + b \cdot i$ y $w = c + d \cdot i$.

(a) Vamos a probar que $\overline{z + w} = \overline{z} + \overline{w}$.

$$\begin{aligned}
\overline{z + w} &= \overline{(a + b \cdot i) + (c + d \cdot i)} \\
&= \overline{(a + c) + (b + d) \cdot i} \text{ por definición de suma de complejos} \\
&= (a + c) - (b + d) \cdot i \text{ por Definición 8.3-(a)} \\
&= (a - b \cdot i) + (c - d \cdot i) \text{ por definición de suma de complejos} \\
&= \left(\overline{a + b \cdot i}\right) + \left(\overline{c + d \cdot i}\right) \text{ por Definición 8.3-(a)} \\
&= \overline{z} + \overline{w}.
\end{aligned}$$

(b) Demostraremos que $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$.

$$\begin{aligned}
\overline{z \cdot w} &= \overline{(a + b \cdot i) \cdot (c + d \cdot i)} \\
&= \overline{(a \cdot c - b \cdot d) + (a \cdot d + b \cdot c) \cdot i} \text{ por definición de producto de complejos} \\
&= (a \cdot c - b \cdot d) - (a \cdot d + b \cdot c) \cdot i \text{ por Definición 8.3-(a)} \\
&= (a - b \cdot i) \cdot (c - d \cdot i) \text{ por definición de producto de complejos} \\
&= \left(\overline{a + b \cdot i}\right) \cdot \left(\overline{c + d \cdot i}\right) \text{ por Definición 8.3-(a)} \\
&= \overline{z} \cdot \overline{w}.
\end{aligned}$$

(c) Comprobemos que $\overline{\overline{z}} = z$.

$$\begin{aligned}
\overline{\overline{z}} &= \overline{\overline{a + b \cdot i}} \\
&= \overline{a - b \cdot i} \text{ por Definición 8.3-(a)} \\
&= a - (-b) \cdot i \text{ por Definición 8.3-(a)} \\
&= a + b \cdot i \\
&= z
\end{aligned}$$

(d) Mostremos que $z + \overline{z} = 2 \cdot \mathrm{Re}\,(z)$.

$$\begin{aligned} z + \overline{z} &= (a + b \cdot i) + \left(\overline{a + b \cdot i}\right) \\ &= (a + b \cdot i) + (a - b \cdot i) \text{ por Definición 8.3-(a)} \\ &= (a + a) + (b - b) \cdot i \text{ por definición de suma de complejos} \\ &= 2 \cdot a + 0 \cdot i \\ &= 2 \cdot a \\ &= 2 \cdot \mathrm{Re}\,(z) \text{ por Definición 8.2-(a)} \end{aligned}$$

Ahora demostremos que $z - \overline{z} = 2 \cdot \mathrm{Im}\,(z) \cdot i$.

$$\begin{aligned} z - \overline{z} &= (a + b \cdot i) - \left(\overline{a + b \cdot i}\right) \\ &= (a + b \cdot i) - (a - b \cdot i) \text{ por Definición 8.3-(a)} \\ &= (a + b \cdot i) + (-a + b \cdot i) \\ &= (a - a) + (b + b) \cdot i \text{ por definición de suma de complejos} \\ &= 0 + 2 \cdot b \cdot i \\ &= 2 \cdot b \cdot i \\ &= 2 \cdot \mathrm{Im}\,(z) \cdot i \text{ por Definición 8.2-(b)} \end{aligned}$$

(e) Vamos a demostrar que $z \in \mathbb{R}$ si y sólo si $z = \overline{z}$.

$$\begin{aligned} z = \overline{z} &\Leftrightarrow a + b \cdot i = \overline{a + b \cdot i} \\ &\Leftrightarrow a + b \cdot i = a - b \cdot i \text{ por Definición 8.3-(a)} \\ &\Leftrightarrow b = -b \\ &\Leftrightarrow b + b = 0 \\ &\Leftrightarrow b = 0 \\ &\Leftrightarrow z \in \mathbb{R} \end{aligned}$$

(f) Supongamos que pensamos que $a = a + 0 \cdot i$. Luego:

$$\text{módulo de } a = \sqrt{a^2 + 0^2} = \sqrt{a^2} = \begin{cases} a, & \text{si } a \geqslant 0, \\ -a, & \text{si } a < 0, \end{cases} = \text{valor absoluto de } a.$$

(g) Podemos representar a z como par ordenado en un gráfico cartesiano como se muestra en la Figura 8.1. Notemos que $|z| = \sqrt{a^2 + b^2}$, que es la longitud de la línea azul. Es decir, el módulo es la distancia desde el punto (a, b) al origen $(0, 0)$.

(h) Mostraremos que $|z| = 0$ si y sólo si $z = 0$.

$$\begin{aligned} |z| = 0 &\Leftrightarrow \sqrt{a^2 + b^2} = 0 \text{ por Definición 8.3-(b)} \\ &\Leftrightarrow a^2 + b^2 = 0 \text{ pues } a^2 + b^2 \geqslant 0 \text{ para cualesquiera } a, b \in \mathbb{R} \\ &\Leftrightarrow a = b = 0 \text{ por Teorema 4.7-(r)} \\ &\Leftrightarrow z = 0 \end{aligned}$$

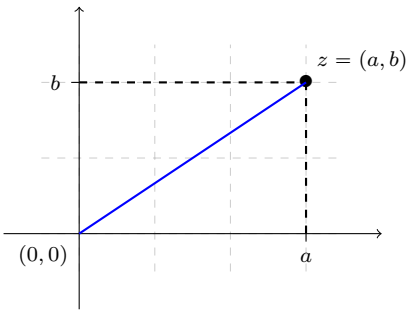


Figura 8.1: El módulo de un número complejo se puede considerar como la distancia al origen.

(i) Comprobemos que $z \cdot \overline{z} = |z|^2$.

$$\begin{aligned} z \cdot \overline{z} &= (a + b \cdot i) \cdot \overline{(a + b \cdot i)} \\ &= (a + b \cdot i) \cdot (a - b \cdot i) \text{ por Definición 8.3-(a)} \\ &= [a \cdot a - b \cdot (-b)] + [a \cdot (-b) + b \cdot a] \cdot i \text{ por definición de producto de complejos} \\ &= \left(a^2 + b^2\right) + 0 \cdot i \\ &= a^2 + b^2 \\ &= |z|^2 \text{ por Definición 8.3-(b)} \end{aligned}$$

(j) Demostremos que si $z \neq 0$ entonces $z^{-1} = \dfrac{\overline{z}}{|z|^2}$. Si $z \neq 0$ entonces $|z| \neq 0$ debido a (h). Luego,

$$\begin{aligned} z \cdot \frac{\overline{z}}{|z|^2} &= \frac{z \cdot \overline{z}}{|z|^2} \\ &= \frac{|z|^2}{|z|^2} \text{ por (i)} \\ &= 1 \end{aligned}$$

Luego el inverso multiplicativo queda completamente determinado, es decir, $z^{-1} = \dfrac{\overline{z}}{|z|^2}$.

(k) Vamos a probar que si $z \neq 0$ entonces $(\overline{z})^{-1} = \overline{z^{-1}}$. Si $z \neq 0$ entonces $a \neq 0$ o $b \neq 0$, entonces $\overline{z} = a - b \cdot i \neq 0$, por lo que tiene inverso. Ahora

$$\begin{aligned} \overline{z} \cdot \overline{z^{-1}} &= \overline{z \cdot z^{-1}} \text{ por (b)} \\ &= \overline{1} \\ &= 1 \end{aligned}$$

Luego el inverso multiplicativo de $\overline{z}$ queda completamente determinado, es decir, $(\overline{z})^{-1} = \overline{z^{-1}}$.

(l) Mostremos que $|\overline{z}| = |z|$.

$$|\overline{z}| = \left|\overline{a + b \cdot i}\right| = |a - b \cdot i| = \sqrt{a^2 + (-b)^2} = \sqrt{a^2 + b^2} = |z|\,.$$

(m) Comprobemos que $|\mathrm{Re}\,(z)| \leqslant |z|$. Por Teorema 4.7-(i) y 4.7-(j) se tiene que $b^2 \geqslant 0$. Luego,

$$0 \leqslant b^2 \quad \Leftrightarrow \quad a^2 \leqslant a^2 + b^2$$

$$
\begin{aligned}
&\Leftrightarrow \quad |a|^2 \leqslant a^2 + b^2 \\
&\Leftrightarrow \quad |\mathrm{Re}\,(z)|^2 \leqslant |z|^2 \text{ por Definición 8.2-(a) y Definición 8.3-(b)} \\
&\Leftrightarrow \quad |\mathrm{Re}\,(z)| \leqslant |z| \text{ por Teorema 4.7-(q)}
\end{aligned}
$$

Ahora veamos que $|\mathrm{Im}\,(z)| \leqslant |z|$. Por Teorema 4.7-(i) y 4.7-(j) se tiene que $a^2 \geqslant 0$. Luego,

$$
\begin{aligned}
0 \leqslant a^2 \quad &\Leftrightarrow \quad b^2 \leqslant a^2 + b^2 \\
&\Leftrightarrow \quad |b|^2 \leqslant a^2 + b^2 \\
&\Leftrightarrow \quad |\mathrm{Im}\,(z)|^2 \leqslant |z|^2 \text{ por Definición 8.2-(a) y Definición 8.3-(b)} \\
&\Leftrightarrow \quad |\mathrm{Im}\,(z)| \leqslant |z| \text{ por Teorema 4.7-(q)}
\end{aligned}
$$

(n) Demostremos que $|z \cdot w| = |z| \cdot |w|$.

$$
\begin{aligned}
|z \cdot w| &= |(a + b \cdot i) \cdot (c + d \cdot i)| \\
&= |(a \cdot c - b \cdot d) + (a \cdot d + b \cdot c) \cdot i| \\
&= \sqrt{(a \cdot c - b \cdot d)^2 + (a \cdot d + b \cdot c)^2} \\
&= \sqrt{a^2 \cdot c^2 - 2 \cdot a \cdot c \cdot b \cdot d + b^2 \cdot d^2 + a^2 \cdot d^2 + 2 \cdot a \cdot d \cdot b \cdot c + b^2 \cdot c^2} \\
&= \sqrt{a^2 \cdot c^2 + b^2 \cdot d^2 + a^2 \cdot d^2 + b^2 \cdot c^2}
\end{aligned}
$$

Por otra parte

$$
\begin{aligned}
|z| \cdot |w| &= |a + b \cdot i| \cdot |c + d \cdot i| \\
&= \sqrt{a^2 + b^2} \cdot \sqrt{c^2 + d^2} \text{ por Definición 8.3-(b)} \\
&= \sqrt{(a^2 + b^2) \cdot (c^2 + d^2)} \text{ por Proposición 7.5-(d)} \\
&= \sqrt{a^2 \cdot c^2 + a^2 \cdot d^2 + b^2 \cdot c^2 + b^2 \cdot d^2}
\end{aligned}
$$

Comparando término a término se puede ver que $|z \cdot w| = |z| \cdot |w|$.

(ñ) Vamos a probar que si $z \neq 0$ entonces $|z^{-1}| = |z|^{-1}$. Si $z \neq 0$ entonces $|z| \neq 0$ debido a (h). Luego,

$$
\begin{aligned}
|z| \cdot \left|z^{-1}\right| &= \left|z \cdot z^{-1}\right| \text{ por (n)} \\
&= |1| \\
&= 1
\end{aligned}
$$

Luego el inverso multiplicativo de $|z|$ queda completamente determinado, es decir, $|z|^{-1} = |z^{-1}|$.

(o) Mostremos que $|z + w| \leqslant |z| + |w|$.

$$
\begin{aligned}
|z + w| \leqslant |z| + |w| \quad &\Leftrightarrow \quad |z + w|^2 \leqslant (|z| + |w|)^2 \text{ por Teorema 4.7-(q)} \\
&\Leftrightarrow \quad (z + w) \cdot \overline{(z + w)} \leqslant |z|^2 + |w|^2 + 2 \cdot |z| \cdot |w| \text{ por (i)} \\
&\Leftrightarrow \quad (z + w) \cdot (\overline{z} + \overline{w}) \leqslant z \cdot \overline{z} + w \cdot \overline{w} + 2 \cdot |z| \cdot |w| \text{ por (a) y (i)} \\
&\Leftrightarrow \quad z \cdot \overline{z} + z \cdot \overline{w} + w \cdot \overline{z} + w \cdot \overline{w} \leqslant z \cdot \overline{z} + w \cdot \overline{w} + 2 \cdot |z| \cdot |w| \\
&\Leftrightarrow \quad z \cdot \overline{w} + w \cdot \overline{z} \leqslant 2 \cdot |z| \cdot |w| \\
&\Leftrightarrow \quad z \cdot \overline{w} + \overline{\overline{w}} \cdot \overline{z} \leqslant 2 \cdot |z| \cdot |w| \text{ por (c)} \\
&\Leftrightarrow \quad z \cdot \overline{w} + \overline{z} \cdot \overline{\overline{w}} \leqslant 2 \cdot |z| \cdot |w|
\end{aligned}
$$

$$
\begin{aligned}
&\Leftrightarrow \quad z \cdot \overline{w} + \overline{z \cdot \overline{w}} \leqslant 2 \cdot |z| \cdot |w| \ \text{ por (b)} \\
&\Leftrightarrow \quad 2 \cdot \operatorname{Re}(z \cdot \overline{w}) \leqslant 2 \cdot |z| \cdot |w| \ \text{ por (d)} \\
&\Leftrightarrow \quad \operatorname{Re}(z \cdot \overline{w}) \leqslant |z| \cdot |w| \\
&\Leftrightarrow \quad \operatorname{Re}(z \cdot \overline{w}) \leqslant |z| \cdot |\overline{w}| \ \text{ por (l)} \\
&\Leftrightarrow \quad \operatorname{Re}(z \cdot \overline{w}) \leqslant |z \cdot \overline{w}| \ \text{ por (n)}
\end{aligned}
$$

La última proposición es verdadera debido a (m), con lo cual la desigualdad triangular se cumple.

(p) Probemos que $|-z| = |z|$.

$$|-z| = |(-1) \cdot z| = |-1| \cdot |z| = 1 \cdot |z| = |z| \,.$$

(q) Demostremos que $\Big|\, |z| - |w| \,\Big| \leqslant |z - w|$. Notemos primero que:

$$|z| = |(z - w) + w| \leqslant |z - w| + |w| \,.$$

Luego $|z| - |w| \leqslant |z - w|$.

Análogamente,

$$|w| = |(w - z) + z| \leqslant |w - z| + |z| \Rightarrow |w| - |z| \leqslant |w - z| = |z - w| \,.$$

Luego $-|z - w| \leqslant |z| - |w|$.

Juntando ambas cosas se obtiene que $-|z - w| \leqslant |z| - |w| \leqslant |z - w|$, lo cual indica que

$$\Big|\, |z| - |w| \,\Big| \leqslant |z - w| \,,$$

debido al Teorema 4.8-(i). ■

8.4. Forma trigonométrica

Hemos visto que los números complejos pueden representarse en un gráfico cartesiano. Si $z \in \mathbb{C}$ tal que $z \neq 0$ hay una manera alternativa de referenciarlo: a través de su longitud y del ángulo que forma con el semieje horizontal positivo (ver Figura 8.2).

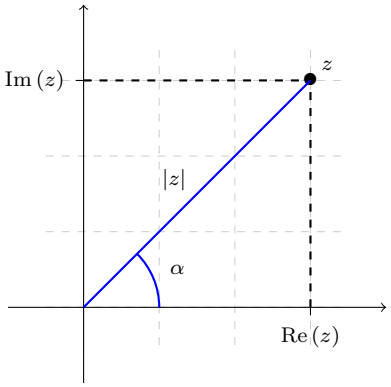


Figura 8.2: Forma de referenciar un número complejo no nulo a través de su módulo y un ángulo.

Notemos que existe un único ángulo $\alpha \in [0, 2 \cdot \pi)$ tal que

$$\cos(\alpha) \quad = \quad \frac{\operatorname{Re}(z)}{|z|},$$

$$\sin(\alpha) = \frac{\mathrm{Im}(z)}{|z|}.$$

Diremos que α es el argumento de z y se denotará $\arg(z)$.

Con esta notación, cualquier número complejo z no nulo se podrá escribir de la siguiente manera:

$$\begin{aligned} z &= \mathrm{Re}(z) + \mathrm{Im}(z) \cdot i \\ &= |z| \cdot \cos(\alpha) + |z| \cdot \sin(\alpha) \cdot i \\ &= |z| \cdot [\cos(\alpha) + \sin(\alpha) \cdot i]. \end{aligned}$$

Definición 8.4
Sea $z \in \mathbb{C}$ tal que $z \neq 0$. Si $\alpha = \arg(z)$ la expresión

$$z = |z| \cdot [\cos(\alpha) + \sin(\alpha) \cdot i],$$

se llama la forma trigonométrica de z.

Ejemplo 8.5

(a) Sea $z = 1 + i$. Ver Figura 8.3.

Calculemos el módulo de z:

$$|z| = \sqrt{1^2 + 1^2} = \sqrt{2}.$$

Calculemos el argumento de z. Como $\mathrm{Re}(z) = 1 > 0$ y $\mathrm{Im}(z) = 1 > 0$ entonces z está en el primer cuadrante, por lo que su argumento es un ángulo en $[0, \pi/2]$ que calcularemos, por ejemplo, utilizando la función arc cos [8]. Luego

$$\arccos\left(\frac{\mathrm{Re}(z)}{|z|}\right) = \arccos\left(\frac{1}{\sqrt{2}}\right) = \frac{\pi}{4}.$$

Como z está en el primer cuadrante, el resultado obtenido por el arc cos corresponde al argumento de z, por lo que

$$\arg(z) = \frac{\pi}{4},$$

que corresponde a $45°$. Luego la forma trigonométrica es:

$$1 + i = \sqrt{2} \cdot \left[\cos\left(\frac{\pi}{4}\right) + \sin\left(\frac{\pi}{4}\right) \cdot i\right].$$

(b) Sea $z = 2 - 2 \cdot i$. Ver Figura 8.4.

Calculemos el módulo de z:

$$|z| = \sqrt{2^2 + (-2)^2} = \sqrt{8}.$$

Calculemos el argumento de z. Como $\mathrm{Re}(z) = 2 > 0$ y $\mathrm{Im}(z) = -2 < 0$ entonces z está en el cuarto cuadrante, por lo que su argumento es un ángulo en $[\, 3 \cdot \pi/2, 2 \cdot \pi\,)$, que calcularemos,

[8] Es fácil ver que la función $\cos : [0, \pi] \to [-1, 1]$ es una función biyectiva. Luego la función cos posee inversa que llamaremos $\arccos : [-1, 1] \to [0, \pi]$. Una vez hallado un ángulo a través del arc cos deberemos analizar el cuadrante al cual pertenece z para ver si debemos modificar el resultado obtenido al utilizar la función arc cos para hallar el argumento.

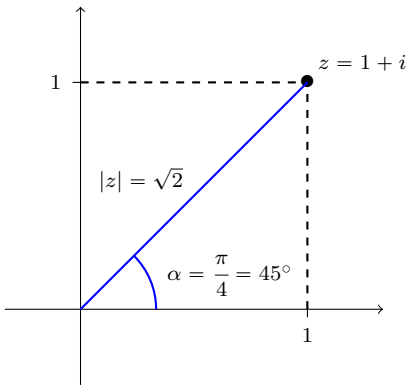


Figura 8.3: Ejemplo de forma trigonométrica de $z = 1 + i$.

por ejemplo, utilizando la función arcsin [9]. Luego

$$\arcsin\left(\frac{\mathrm{Im}\,(z)}{|z|}\right) = \arcsin\left(\frac{-2}{\sqrt{8}}\right) = \arcsin\left(\frac{-1}{\sqrt{2}}\right) = -\frac{\pi}{4}.$$

Como z está en el cuarto cuadrante, al resultado obtenido por el arcsin debemos sumarle $2 \cdot \pi$, por lo que:

$$\arg(z) = 2 \cdot \pi - \frac{\pi}{4} = \frac{7 \cdot \pi}{4},$$

que corresponde a 315°. Luego la forma trigonométrica es:

$$2 - 2 \cdot i = \sqrt{8} \cdot \left[\cos\left(\frac{7 \cdot \pi}{4}\right) + \sin\left(\frac{7 \cdot \pi}{4}\right) \cdot i\right].$$

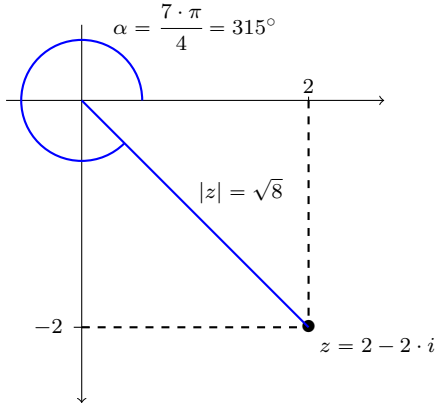


Figura 8.4: Ejemplo de forma trigonométrica de $z = 2 - 2 \cdot i$.

[9] Es fácil ver que la función $\sin : \left[-\frac{\pi}{2}, \frac{\pi}{2}\right] \to [-1, 1]$ es una función biyectiva. Luego la función sin posee inversa que llamaremos $\arcsin : [-1, 1] \to \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$. Una vez hallado un ángulo a través del arcsin deberemos analizar el cuadrante al cual pertenece z para ver si debemos modificar el resultado obtenido al utilizar la función arcsin para hallar el argumento.

Observación 8.3
(a) Si $z = r \cdot [\cos(\beta) + \sin(\beta) \cdot i]$ *con* $r \in \mathbb{R}$ *y* $r > 0$, *entonces:*

$$\begin{aligned} r &= |z|, \\ \beta &= \arg(z) + 2 \cdot k \cdot \pi, \quad \text{para algún } k \in \mathbb{Z}. \end{aligned}$$

En particular, si $\beta \in [\, 0, 2 \cdot \pi \,)$ *entonces* $\beta = \arg(z)$.

(b) Sean $z, w \in \mathbb{C}$ *no nulos. Entonces:*

$$z = w \Leftrightarrow \begin{cases} |z| &= |w| \\ \arg(z) &= \arg(w) \end{cases}$$

Demostración.
(a) Calculemos el módulo de z:

$$\begin{aligned} |z| &= |r| \cdot |\cos(\beta) + \sin(\beta) \cdot i| \text{ por Proposición 8.2-(n)} \\ &= r \cdot \sqrt{\cos^2(\beta) + \sin^2(\beta)} \text{ pues } r > 0 \text{ y Definición 8.3-(b)} \\ &= r \cdot \sqrt{1} \\ &= r \cdot 1 \\ &= r \end{aligned}$$

Llamemos $\alpha = \arg(z)$. Entonces:

$$\begin{aligned} \cos(\alpha) &= \frac{\operatorname{Re}(z)}{|z|} = \frac{\operatorname{Re}(z)}{r} = \cos(\beta), \\ \sin(\alpha) &= \frac{\operatorname{Im}(z)}{|z|} = \frac{\operatorname{Im}(z)}{r} = \sin(\beta), \end{aligned}$$

Luego, como $\cos(\alpha) = \cos(\beta)$ y $\sin(\alpha) = \sin(\beta)$ se tiene que $\beta = \alpha + 2 \cdot k \cdot \pi$ para algún $k \in \mathbb{Z}$.

(b)
Es consecuencia inmediata de la Definición 8.4. ■

8.5. Multiplicando complejos en forma trigonométrica

Vamos a tratar de determinar el argumento y el módulo del producto de dos números complejos no nulos.

Teorema 8.1 (De Moivre)
Sean $z, w \in \mathbb{C}$ *no nulos. Entonces:*

$$\arg(z \cdot w) = \arg(z) + \arg(w) - 2 \cdot k \cdot \pi,$$

para algún $k \in \mathbb{Z}$.

Demostración.
Llamemos $\alpha = \arg(z)$ y $\beta = \arg(w)$. Entonces de la Definición 8.4 se desprende que:

$$\begin{aligned} z &= |z| \cdot [\cos(\alpha) + \sin(\alpha) \cdot i], \\ w &= |w| \cdot [\cos(\beta) + \sin(\beta) \cdot i]. \end{aligned}$$

Luego hacemos el producto:

$$\begin{aligned} z \cdot w &= |z| \cdot [\cos(\alpha) + \sin(\alpha) \cdot i] \cdot |w| \cdot [\cos(\beta) + \sin(\beta) \cdot i] \\ &= |z| \cdot |w| \cdot \{[\cos(\alpha) \cdot \cos(\beta) - \sin(\alpha) \cdot \sin(\beta)] + [\cos(\alpha) \cdot \sin(\beta) + \sin(\alpha) \cdot \cos(\beta)] \cdot i\} \\ &= |z| \cdot |w| \cdot [\cos(\alpha + \beta) + \sin(\alpha + \beta) \cdot i] \end{aligned}$$

Por la Observación 8.3-(a) se tiene que

$$\alpha + \beta = \arg(z \cdot w) + 2 \cdot k \cdot \pi,$$

para algún $k \in \mathbb{Z}$. O sea que:

$$\arg(z \cdot w) = \arg(z) + \arg(w) - 2 \cdot k \cdot \pi,$$

lo cual concluye la demostración. ■

Ejemplo 8.6

(a) Consideremos grados sexagesimales para los siguientes dos números complejos:

$$\begin{aligned} z &= 2 \cdot [\cos(120^\circ) + \sin(120^\circ) \cdot i], \\ w &= 3 \cdot [\cos(315^\circ) + \sin(315^\circ) \cdot i]. \end{aligned}$$

Luego, utilizando el Teorema 8.1 se tiene que:

$$\begin{aligned} z \cdot w &= 2 \cdot 3 \cdot [\cos(120^\circ + 315^\circ) + \sin(120^\circ + 315^\circ) \cdot i], \\ &= 6 \cdot [\cos(435^\circ) + \sin(435^\circ) \cdot i], \\ &= 6 \cdot [\cos(75^\circ) + \sin(75^\circ) \cdot i], \end{aligned}$$

pues $435 = 360 \cdot 1 + 75$, con lo cual $\arg(z \cdot w) = 75^\circ$ y $|z \cdot w| = 6$.

Notemos que el $k \in \mathbb{Z}$ del Teorema 8.1 debe satisfacer que

$$0 \leqslant \arg(z) + \arg(w) - 2 \cdot k \cdot \pi < 2 \cdot \pi.$$

Corolario 8.1

Sea $z \in \mathbb{C}$ tal que $z \neq 0$ y $n \in \mathbb{N}$. Entonces

(a) $z^n = |z|^n [\cos(n \cdot \alpha) + \sin(n \cdot \alpha) \cdot i]$ *donde* $\alpha = \arg(z)$.

(b) $\arg(z^n) = n \cdot \arg(z) - 2 \cdot k \cdot \pi$ *para algún* $k \in \mathbb{Z}$.

(c) $\arg(z^{-1}) = -\arg(z) + 2 \cdot k \cdot \pi$ *para algún* $k \in \mathbb{Z}$.

(d) $\arg(\overline{z}) = -\arg(z) + 2 \cdot k \cdot \pi$ *para algún* $k \in \mathbb{Z}$.

Demostración.

(a) Vamos a probar la validez de la expresión por inducción en n.

Cuando $n = 1$ la propiedad vale por la Definición 8.4.

Supongamos que vale para n. Veamos que vale para $n + 1$. Luego:

$$\begin{aligned} z^{n+1} &= z \cdot z^n = \{|z| \cdot [\cos(\alpha) + \sin(\alpha) \cdot i]\} \cdot \{|z| \cdot [\cos(\alpha) + \sin(\alpha) \cdot i]\}^n \text{ por Definición 8.4} \\ &= \{|z| \cdot [\cos(\alpha) + \sin(\alpha) \cdot i]\} \cdot \{|z|^n \cdot [\cos(n \cdot \alpha) + \sin(n \cdot \alpha) \cdot i]\} \text{ por hipótesis inductiva} \\ &= |z|^{n+1} \cdot \{[\cos(\alpha) \cdot \cos(n \cdot \alpha) - \sin(\alpha) \cdot \sin(n \cdot \alpha)] \\ &+ [\cos(\alpha) \cdot \sin(n \cdot \alpha) + \sin(\alpha) \cdot \cos(n \cdot \alpha)] \cdot i\} \end{aligned}$$

$$= |z|^{n+1} \cdot \{\cos[(n+1)\cdot\alpha] + \sin[(n+1)\cdot\alpha]\cdot i\} \text{ por propiedades de trigonometría}$$

Por el Criterio 5.1 resulta lo que queríamos demostrar.

(b) Por lo ya demostrado en (a) y la Observación 8.3-(a) se tiene que

$$n\cdot\alpha = \arg(z^n) + 2\cdot k\cdot\pi,$$

para algún $k \in \mathbb{Z}$. O sea que:

$$\arg(z^n) = n\cdot\arg(z) - 2\cdot k\cdot\pi.$$

(c) Vamos a probar que $\arg(z^{-1}) = -\arg(z) + 2\cdot k\cdot\pi$ para algún $k \in \mathbb{Z}$. Notemos que:

$$\begin{aligned} 0 &= \arg(1) \text{ pues } 1 = 1\cdot[\cos(0) + \sin(0)\cdot i] \\ &= \arg\left(z\cdot z^{-1}\right) \text{ pues } 1 = z\cdot z^{-1} \\ &= \arg(z) + \arg\left(z^{-1}\right) - 2\cdot k\cdot\pi \text{ por Teorema 8.1} \end{aligned}$$

Luego

$$\arg\left(z^{-1}\right) = -\arg(z) + 2\cdot k\cdot\pi.$$

(d) Demostraremos que $\arg(\overline{z}) = -\arg(z) + 2\cdot k\cdot\pi$ para algún $k \in \mathbb{Z}$. Notemos que:

$$\begin{aligned} \arg\left(z^{-1}\right) &= \arg\left(\frac{1}{|z|^2}\cdot\overline{z}\right) \text{ por Proposición 8.2-(j)} \\ &= \arg\left(\frac{1}{|z|^2}\right) + \arg(\overline{z}) - 2\cdot k\cdot\pi \text{ por Teorema 8.1} \\ &= 0 + \arg(\overline{z}) - 2\cdot k\cdot\pi \\ &= \arg(\overline{z}) - 2\cdot k\cdot\pi \end{aligned}$$

Como $\arg\left(z^{-1}\right), \arg(\overline{z}) \in [0, 2\cdot\pi)$. Luego

$$2\cdot|k|\cdot\pi = \left|\arg\left(z^{-1}\right) - \arg(\overline{z})\right| < 2\cdot\pi,$$

por lo que $k = 0$. Esto significa que $\arg\left(z^{-1}\right) = \arg(\overline{z})$. Por (c) se deduce que

$$\arg(\overline{z}) = -\arg(z) + 2\cdot k\cdot\pi,$$

para algún $k \in \mathbb{Z}$. ■

Ejemplo 8.7

(a) Hallar $z = (1+i)^{3523}$.

Primero determinemos el módulo de z:

$$\begin{aligned} |z| &= \left|(1+i)^{3523}\right| \\ &= |1+i|^{3523} \text{ por Proposición 8.2-(n)} \\ &= \left(\sqrt{2}\right)^{3523} \text{ ya visto en el Ejemplo 8.5-(a)} \end{aligned}$$

Ahora determinemos el argumento:

$$\arg(z) = \arg\left((1+i)^{3523}\right)$$

$$
\begin{aligned}
&= 3523 \cdot \arg(1+i) - 2 \cdot k \cdot \pi \text{ por Corolario 8.1-(b)} \\
&= 3523 \cdot \frac{\pi}{4} - 2 \cdot k \cdot \pi \text{ ya visto en el Ejemplo 8.5-(a)}
\end{aligned}
$$

para algún $k \in \mathbb{Z}$. Tal entero k debe ser tal que $0 \leqslant \arg(z) < 2 \cdot \pi$. Es decir,

$$
\begin{aligned}
0 \leqslant 3523 \cdot \frac{\pi}{4} - 2 \cdot k \cdot \pi < 2 \cdot \pi &\Leftrightarrow 0 \leqslant 3523 \cdot \pi - 8 \cdot k \cdot \pi < 8 \cdot \pi \\
&\Leftrightarrow 0 \leqslant 3523 - 8 \cdot k < 8,
\end{aligned}
$$

Haciendo unos pequeños cálculos se obtiene que $k = 440$, por lo que

$$
\arg(z) = 3523 \cdot \frac{\pi}{4} - 2 \cdot 440 \cdot \pi = \frac{3}{4} \cdot \pi.
$$

Resumiendo se tiene

$$
\begin{aligned}
z &= \left(\sqrt{2}\right)^{3523} \cdot \left[\cos\left(\frac{3}{4} \cdot \pi\right) + \sin\left(\frac{3}{4} \cdot \pi\right) \cdot i\right] \\
&= \left(\sqrt{2}\right)^{3523} \cdot \left(-\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} \cdot i\right) \\
&= \frac{\left(\sqrt{2}\right)^{3523}}{\sqrt{2}} \cdot (-1+i) \\
&= \left(\sqrt{2}\right)^{3522} \cdot (-1+i) \\
&= 2^{1761} \cdot (-1+i).
\end{aligned}
$$

8.6. Raíces n-ésimas

Sean $z \in \mathbb{C}$ tal que $z \neq 0$ y sea $n \in \mathbb{N}$. Queremos hallar todos los $w \in \mathbb{C}$ tales que $w^n = z$. Llamemos $r = |z|$ y $\alpha = \arg(z)$.

Notemos que w no puede ser cero, pues de otro modo $z = w^n = 0$ lo cual es una contradicción. Por lo tanto $w \neq 0$. Ahora:

$$
\begin{aligned}
w^n = z &\Leftrightarrow \begin{cases} |w^n| &= |z| \\ \arg(w^n) &= \arg(z) \end{cases} \text{ por Observación 8.3-(b)} \\
&\Leftrightarrow \begin{cases} |w|^n &= r \\ n \cdot \arg(w) - 2 \cdot k \cdot \pi &= \alpha \end{cases} \text{ por Proposición 8.2-(n) y Corolario 8.1-(b)} \\
&\Leftrightarrow \begin{cases} |w| &= \sqrt[n]{r} \\ \arg(w) &= \dfrac{\alpha + 2 \cdot k \cdot \pi}{n} \end{cases}
\end{aligned}
$$

donde k debe satisfacer que

$$
0 \leqslant \frac{\alpha + 2 \cdot k \cdot \pi}{n} < 2 \cdot \pi.
$$

Luego $k = 0, 1, \ldots, n-1$. Por lo tanto las raíces n-ésimas de z son:

$$
w_k = \sqrt[n]{|z|} \cdot \left[\cos\left(\frac{\arg(z) + 2 \cdot k \cdot \pi}{n}\right) + \sin\left(\frac{\arg(z) + 2 \cdot k \cdot \pi}{n}\right) \cdot i\right], \quad k = 0, \ldots, n-1.
$$

Ejemplo 8.8

(a) Hallar las raíces quintas de $z = -2 \cdot i$.

Es claro que:

$$\begin{aligned} |z| &= 2, \\ \arg(z) &= \frac{3}{2} \cdot \pi. \end{aligned}$$

Luego las raíces quintas de z son:

$$\begin{aligned} w_0 &= \sqrt[5]{2} \cdot \left[\cos\left(\frac{3}{10} \cdot \pi \right) + \sin\left(\frac{3}{10} \cdot \pi \right) \cdot i \right], \\ w_1 &= \sqrt[5]{2} \cdot \left[\cos\left(\frac{7}{10} \cdot \pi \right) + \sin\left(\frac{7}{10} \cdot \pi \right) \cdot i \right], \\ w_2 &= \sqrt[5]{2} \cdot \left[\cos\left(\frac{11}{10} \cdot \pi \right) + \sin\left(\frac{11}{10} \cdot \pi \right) \cdot i \right], \\ w_3 &= \sqrt[5]{2} \cdot \left[\cos\left(\frac{15}{10} \cdot \pi \right) + \sin\left(\frac{15}{10} \cdot \pi \right) \cdot i \right], \\ w_4 &= \sqrt[5]{2} \cdot \left[\cos\left(\frac{19}{10} \cdot \pi \right) + \sin\left(\frac{19}{10} \cdot \pi \right) \cdot i \right]. \end{aligned}$$

En el caso particular de que $z = 1$ se tiene que $|z| = 1$ y $\arg(z) = 0$. Si calculamos las raíces n-ésimas de la unidad se tiene que:

$$w_k = \cos\left(\frac{2 \cdot k \cdot \pi}{n} \right) + \sin\left(\frac{2 \cdot k \cdot \pi}{n} \right) \cdot i, \quad k = 0, \ldots, n-1.$$

Definición 8.5

Sea $n \in \mathbb{N}$. Llamaremos G_n al conjunto de raíces n-ésimas de la unidad, es decir:

$$G_n = \{ w \in \mathbb{C} : w^n = 1 \} = \left\{ \cos\left(\frac{2 \cdot k \cdot \pi}{n} \right) + \sin\left(\frac{2 \cdot k \cdot \pi}{n} \right) \cdot i : 0 \leqslant k < n \right\}.$$

Proposición 8.3

Sea $n \in \mathbb{N}$.

(a) Si $z \in G_n$ y $m \in \mathbb{Z}$, se tiene que si $m = n \cdot q + r$ entonces $z^m = z^r$.

(b) Si $z, w \in G_n$ entonces $z \cdot w \in G_n$.

(c) $1 \in G_n$.

(d) Si $z \in G_n$ entonces $\overline{z} \in G_n$.

(e) Si $z \in G_n$ entonces $z^{-1} \in G_n$.

(f) Si $z \in G_n$ entonces $\overline{z}^k = z^{-k} = z^{n-k}$ para todo $k \in \mathbb{Z}$.

Demostración.
(a) Vamos a demostrar que si $z \in G_n$ y $m \in \mathbb{Z}$, se tiene que si $m = n \cdot q + r$ entonces $z^m = z^r$. Observemos que:

$$\begin{aligned} z^m &= z^{n\cdot q+r} \\ &= z^{n\cdot q} \cdot z^r \\ &= (z^n)^q \cdot z^r \\ &= 1^q \cdot z^r \text{ pues } z \in G_n \\ &= z^r. \end{aligned}$$

(b) Veamos que si $z, w \in G_n$ entonces $z \cdot w \in G_n$. Notemos que:

$$\begin{aligned} (z \cdot w)^n &= z^n \cdot w^n \\ &= 1 \cdot 1 \text{ pues } z, w \in G_n \\ &= 1. \end{aligned}$$

Luego $z \cdot w \in G_n$.

(c) Claramente $1 \in G_n$, pues $1^n = 1$. Además observar que $1 = w_0$.

(d) Probemos que si $z \in G_n$ entonces $\overline{z} \in G_n$. Observemos que:

$$\begin{aligned} (\overline{z})^n &= \overline{z^n} \text{ por Proposición 8.2-(b)} \\ &= \overline{1} \text{ pues } z \in G_n \\ &= 1. \end{aligned}$$

Luego $\overline{z} \in G_n$.

(e) Demostremos que si $z \in G_n$ entonces $z^{-1} \in G_n$. Notemos que:

$$\begin{aligned} \left(z^{-1}\right)^n &= \left(\frac{\overline{z}}{|z|^2}\right)^n \text{ por Proposición 8.2-(j)} \\ &= \left(\frac{\overline{z}}{1}\right)^n \\ &= (\overline{z})^n \\ &= 1 \text{ por (d)} \end{aligned}$$

Luego $z^{-1} \in G_n$.

(f) Comprobemos que si $z \in G_n$ entonces $\overline{z}^k = z^{-k} = z^{n-k}$ para todo $k \in \mathbb{Z}$. Observemos que:

$$\begin{aligned} z^k \cdot \overline{z}^k &= (z \cdot \overline{z})^k \\ &= \left(|z|^2\right)^k \text{ por Proposición 8.2-(i)} \\ &= 1^k \\ &= 1. \end{aligned}$$

Como el inverso es único, se tiene que $\overline{z}^k = z^{-k}$.

Análogamente,

$$\begin{aligned} z^k \cdot z^{n-k} &= z^{n-k+k} \\ &= z^n \\ &= 1 \text{ pues } z \in G_n \end{aligned}$$

Como el inverso es único, se tiene que $z^{n-k} = z^{-k}$. ■

9. POLINOMIOS

Para comprender totalmente la unidad correspondiente a polinomios es aconsejable estudiar primero nociones de estructuras algebraicas, más precisamente los conceptos de grupos, anillos y cuerpos, y sus propiedades. En nuestra asignatura veremos una introducción a los polinomios considerando estructuras estudiadas hasta el momento, a saber: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$. Estas estructuras son casos particulares de estructuras generales. Más precisamente:

- $\mathbb{Z}$ es un caso particular de un anillo conmutativo con identidad.
- $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son casos particulares de cuerpos (además son también anillos conmutativos con identidad).

Por tal motivo, cuando hablemos de un anillo conmutativo con identidad estaremos asumiendo que tal anillo es $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$, y cuando hablemos de cuerpos, estaremos asumiendo que nos referimos a $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$. Igualmente, para no causar confusión, los enunciados aclararán a qué conjuntos específicos estamos haciendo referencia.

9.1. El anillo de polinomios

Definición 9.1
Sea A un anillo conmutativo con identidad ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$) y sea X una indeterminada sobre A, es decir, X satisface

$$a_0 + a_1 \cdot X + \ldots + a_n \cdot X^n = b_0 + b_1 \cdot X + \ldots + b_n \cdot X^n \Leftrightarrow a_j = b_j, \quad j = 0, \ldots, n.$$

(Por ejemplo, si $A = \mathbb{Q}$ entonces el número π satisface esta propiedad).

Definimos el anillo de polinomios con coeficientes en A, al que denotaremos $A[X]$, como:

$$A[X] = \{a_0 + a_1 \cdot X + \ldots + a_n \cdot X^n : n \in \mathbb{N} \cup \{0\} \ \text{ y } a_i \in A, i = 0, \ldots, n\}.$$

El número a_i se llama el coeficiente de X^i.

Se definen las siguientes operaciones de suma y producto dadas por:

$$\begin{aligned} \sum_{i=0}^{n} a_i \cdot X^i + \sum_{i=0}^{m} b_i \cdot X^i &= \sum_{i=0}^{\text{máx}\{n,m\}} (a_i + b_i) \cdot X^i, \\ \left(\sum_{i=0}^{n} a_i \cdot X^i\right) \cdot \left(\sum_{j=0}^{m} b_j \cdot X^j\right) &= \sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_i \cdot b_j\right) \cdot X^k \end{aligned}$$

donde $a_i = 0$ para $i > n$ y $b_i = 0$ para $i > m$ y, por convención $X^0 = 1$. A los elementos de $A[X]$ los llamaremos polinomios con coeficientes en A.

Para aquellos alumnos que estén interesados en saber qué significa realmente una indeterminada, pueden leer el Apéndice III del libro "Notas de Álgebra I" cuyo autor es Enzo R. Gentile. En tal apéndice se prueba que dado un anillo B que sea conmutativo con identidad, se puede construir otro anillo A con las siguientes propiedades:

- A es un anillo conmutativo con identidad.
- B es un subanillo de A.
- A posee un elemento trascendente sobre B (es decir, existe una indeterminada sobre B).

Ejemplo 9.1
Consideremos que $f, g \in \mathbb{Z}[X]$, donde

$$\begin{aligned} f &= X^4 + 2 \cdot X^3 + 3 \cdot X^2 - 2 \cdot X + 1, \\ g &= 3 \cdot X^2 + 5 \cdot X - 7. \end{aligned}$$

(a) Suma de f y g:

$$\begin{aligned} f + g &= \left(X^4 + 2 \cdot X^3 + 3 \cdot X^2 - 2 \cdot X + 1\right) + \left(3 \cdot X^2 + 5 \cdot X - 7\right), \\ &= \left(X^4 + 2 \cdot X^3 + 3 \cdot X^2 - 2 \cdot X + 1\right) + \left(0 \cdot X^4 + 0 \cdot X^3 + 3 \cdot X^2 + 5 \cdot X - 7\right), \\ &= (1+0) \cdot X^4 + (2+0) \cdot X^3 + (3+3) \cdot X^2 + (-2+5) \cdot X^1 + (1-7) \cdot X^0 \\ &= X^4 + 2 \cdot X^3 + 6 \cdot X^2 + 3 \cdot X - 6. \end{aligned}$$

En otras palabras, hay que sumar los coeficientes asociados a las potencias de X que sean iguales.

(b) Producto de f y g:

$$\begin{aligned} f \cdot g &= \left(X^4 + 2 \cdot X^3 + 3 \cdot X^2 - 2 \cdot X + 1\right) \cdot \left(3 \cdot X^2 + 5 \cdot X - 7\right), \\ &= (1 \cdot 3) \cdot X^6 + (1 \cdot 5 + 2 \cdot 3) \cdot X^5 + [1 \cdot (-7) + 2 \cdot 5 + 3 \cdot 3] \cdot X^4 \\ &+ [2 \cdot (-7) + 3 \cdot 5 + (-2) \cdot 3] \cdot X^3 + [3 \cdot (-7) + (-2) \cdot 5 + 1 \cdot 3] \cdot X^2 \\ &+ [(-2) \cdot (-7) + 1 \cdot 5] \cdot X^1 + [1 \cdot (-7)] \cdot X^0 \\ &= 3 \cdot X^6 + 11 \cdot X^5 + 12 \cdot X^4 - 5 \cdot X^3 - 28 \cdot X^2 + 19 \cdot X - 7. \end{aligned}$$

En otras palabras, el producto de dos polinomios se calcula simplemente utilizando la propiedad distributiva.

Proposición 9.1
Sea A un anillo conmutativo con identidad ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$). Entonces

(a) $A \subset A[X]$.

(b) $A[X]$ *es un anillo conmutativo con identidad.*

Demostración.
(a) Cada elemento $a \in A$ puede ser visto de la siguiente manera:

$$a = \sum_{i=0}^{n} a_i \cdot X^i,$$

donde $n = 0$ y $a_0 = a$.

(b) Sean $f, g, h \in A[X]$ definidos por

$$f = \sum_{i=0}^{n} a_i \cdot X^i, \quad g = \sum_{j=0}^{m} b_j \cdot X^j, \quad h = \sum_{k=0}^{p} c_k \cdot X^k.$$

Veamos que la suma es asociativa. Podemos asumir que $m = p = n$.

$$(f+g)+h = \left(\sum_{i=0}^{n} a_i \cdot X^i + \sum_{i=0}^{n} b_i \cdot X^i\right) + \sum_{i=0}^{n} c_i \cdot X^i$$

$$
\begin{aligned}
&= \sum_{i=0}^{n} (a_i + b_i) \cdot X^i + \sum_{i=0}^{n} c_i \cdot X^i \text{ por definición de suma de polinomios} \\
&= \sum_{i=0}^{n} [(a_i + b_i) + c_i] \cdot X^i \text{ por definición de suma de polinomios} \\
&= \sum_{i=0}^{n} [a_i + (b_i + c_i)] \cdot X^i \text{ por propiedad asociativa de } + \text{ en } A \\
&= \sum_{i=0}^{n} a_i \cdot X^i + \sum_{i=0}^{n} (b_i + c_i) \cdot X^i \text{ por definición de suma de polinomios} \\
&= \sum_{i=0}^{n} a_i \cdot X^i + \left(\sum_{i=0}^{n} b_i \cdot X^i + \sum_{i=0}^{n} c_i \cdot X^i \right) \text{ por definición de suma de polinomios} \\
&= f + (g + h)
\end{aligned}
$$

Veamos que la suma es conmutativa. Podemos asumir que $m = n$.

$$
\begin{aligned}
f + g &= \sum_{i=0}^{n} a_i \cdot X^i + \sum_{i=0}^{n} b_i \cdot X^i \\
&= \sum_{i=0}^{n} (a_i + b_i) \cdot X^i \text{ por definición de suma de polinomios} \\
&= \sum_{i=0}^{n} (b_i + a_i) \cdot X^i \text{ por propiedad conmutativa de } + \text{ en } A \\
&= \sum_{i=0}^{n} b_i \cdot X^i + \sum_{i=0}^{n} a_i \cdot X^i \text{ por definición de suma de polinomios} \\
&= g + f
\end{aligned}
$$

El neutro es el polinomio 0.

$$
\begin{aligned}
f + 0 &= \sum_{i=0}^{n} a_i \cdot X^i + \sum_{i=0}^{n} 0 \cdot X^i \\
&= \sum_{i=0}^{n} (a_i + 0) \cdot X^i \text{ por definición de suma de polinomios} \\
&= \sum_{i=0}^{n} a_i \cdot X^i \text{ por propiedad del neutro de la } + \text{ en } A \\
&= f
\end{aligned}
$$

Cada elemento de $A[X]$ posee opuesto. De hecho, el opuesto de un polinomio f es un polinomio $\widehat{f}$ cuyos coeficientes son los opuestos de los coeficientes de f.

$$
\begin{aligned}
f + \widehat{f} &= \sum_{i=0}^{n} a_i \cdot X^i + \sum_{i=0}^{n} (-a_i) \cdot X^i \\
&= \sum_{i=0}^{n} [a_i + (-a_i)] \cdot X^i \text{ por definición de suma de polinomios} \\
&= \sum_{i=0}^{n} 0 \cdot X^i \text{ por propiedad de los opuestos en } A \\
&= 0
\end{aligned}
$$

El producto es asociativo.

$$\begin{aligned}
(f\cdot g)\cdot h &= \left[\left(\sum_{i=0}^{n} a_i\cdot X^i\right)\cdot\left(\sum_{j=0}^{m} b_j\cdot X^j\right)\right]\cdot\left(\sum_{k=0}^{p} c_k\cdot X^k\right)\\
&= \left[\sum_{s=0}^{n+m}\left(\sum_{i+j=s} a_i\cdot b_j\right)\cdot X^s\right]\cdot\left(\sum_{k=0}^{p} c_k\cdot X^k\right) \text{ por definición de producto de polinomios}\\
&= \sum_{t=0}^{(n+m)+p}\left[\sum_{s+k=t}\left(\sum_{i+j=s} a_i\cdot b_j\right)\cdot c_k\right]\cdot X^t \text{ por definición de producto de polinomios}\\
&= \sum_{t=0}^{(n+m)+p}\left(\sum_{i+j+k=t} a_i\cdot b_j\cdot c_k\right)\cdot X^t \text{ reordenando las sumas}\\
&= \sum_{t=0}^{n+(m+p)}\left[\sum_{i+s=t} a_i\cdot\left(\sum_{j+k=s} b_j\cdot c_k\right)\right]\cdot X^t \text{ reordenando las sumas}\\
&= \left(\sum_{i=0}^{n} a_i\cdot X^i\right)\cdot\left[\sum_{s=0}^{m+p}\left(\sum_{j+k=s} b_j\cdot c_k\right)\cdot X^s\right] \text{ por definición de producto de polinomios}\\
&= \left(\sum_{i=0}^{n} a_i\cdot X^i\right)\cdot\left[\left(\sum_{j=0}^{m} b_j\cdot X^j\right)\cdot\left(\sum_{k=0}^{p} c_k\cdot X^k\right)\right] \text{ por definición de producto}\\
&= f\cdot(g\cdot h)
\end{aligned}$$

El producto distribuye respecto de la suma. Podemos asumir que $p = m$.

$$\begin{aligned}
f\cdot(g+h) &= \left(\sum_{i=0}^{n} a_i\cdot X^i\right)\cdot\left(\sum_{j=0}^{m} b_j\cdot X^j+\sum_{j=0}^{m} c_j\cdot X^j\right)\\
&= \left(\sum_{i=0}^{n} a_i\cdot X^i\right)\cdot\left[\sum_{j=0}^{m}(b_j+c_j)\cdot X^j\right] \text{ por definición de suma de polinomios}\\
&= \sum_{s=0}^{n+m}\left[\sum_{i+j=s} a_i\cdot(b_j+c_j)\right]\cdot X^s \text{ por definición de producto de polinomios}\\
&= \sum_{s=0}^{n+m}\left[\sum_{i+j=s}(a_i\cdot b_j+a_i\cdot c_j)\right]\cdot X^s \text{ por propiedad distributiva en } A\\
&= \sum_{s=0}^{n+m}\left[\left(\sum_{i+j=s} a_i\cdot b_j\right)+\left(\sum_{i+j=s} a_i\cdot c_j\right)\right]\cdot X^s \text{ reordenando sumas}\\
&= \sum_{s=0}^{n+m}\left(\sum_{i+j=s} a_i\cdot b_j\right)\cdot X^s+\sum_{s=0}^{n+m}\left(\sum_{i+j=s} a_i\cdot c_j\right)\cdot X^s \text{ por definición de suma}\\
&= \left(\sum_{i=0}^{n} a_i\cdot X^i\right)\cdot\left(\sum_{j=0}^{m} b_j\cdot X^j\right)+\left(\sum_{i=0}^{n} a_i\cdot X^i\right)\cdot\left(\sum_{k=0}^{m} c_k\cdot X^k\right)\\
&= f\cdot g+f\cdot h
\end{aligned}$$

Veamos que $A[X]$ posee elemento neutro para el producto y es igual a 1.

$$f\cdot 1 = \left(\sum_{i=0}^{n} a_i\cdot X^i\right)\cdot 1$$

$$
\begin{aligned}
&= \sum_{i=0}^{n} (a_i \cdot 1) \cdot X^i \text{ usamos la propiedad distributiva} \\
&= \sum_{i=0}^{n} a_i \cdot X^i \text{ por propiedad del neutro del producto en } A \\
&= f
\end{aligned}
$$

Demostraremos que $A[X]$ es conmutativo.

$$
\begin{aligned}
f \cdot g &= \left(\sum_{i=0}^{n} a_i \cdot X^i \right) \cdot \left(\sum_{j=0}^{m} b_j \cdot X^j \right) \\
&= \sum_{s=0}^{n+m} \left(\sum_{i+j=s} a_i \cdot b_j \right) \cdot X^s \text{ por definición de producto de polinomios} \\
&= \sum_{s=0}^{m+n} \left(\sum_{j+i=s} b_j \cdot a_i \right) \cdot X^s \text{ por propiedad conmutativa del producto en } A \\
&= \left(\sum_{j=0}^{m} b_j \cdot X^j \right) \cdot \left(\sum_{i=0}^{n} a_i \cdot X^i \right) \text{ por definición de producto de polinomios} \\
&= g \cdot f
\end{aligned}
$$

■

Los anillos que estamos considerando ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$) satisfacen una propiedad similar a la propiedad que aparece en el Teorema 4.5-(i) que dice que $a \cdot b = 0 \Leftrightarrow a = 0$ o $b = 0$. Los anillos que cumplan esta propiedad se denominan dominios de integridad. A continuación veremos que el anillo de polinomios heredará esta cualidad.

Proposición 9.2
Sea A un anillo conmutativo con identidad que sea dominio de integridad ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$). Entonces $A[X]$ es un dominio de integridad (es decir, si $f, g \in A[X]$ entonces $f \cdot g = 0$ si y sólo si $f = 0$ o $g = 0$).

Demostración.
Sean $f, g \in A[X]$ tales que $f \neq 0$ y $g \neq 0$. Luego

$$
\begin{aligned}
f &= \sum_{i=0}^{n} a_i \cdot X^i, \quad a_n \neq 0, \\
g &= \sum_{j=0}^{m} b_j \cdot X^j, \quad b_m \neq 0.
\end{aligned}
$$

Ahora

$$
\begin{aligned}
f \cdot g &= \sum_{s=0}^{n+m} \left(\sum_{i+j=s} a_i \cdot b_j \right) \cdot X^s \text{ por definición de producto de polinomios} \\
&= a_n \cdot b_m \cdot X^{n+m} + \sum_{s=0}^{n+m-1} \left(\sum_{i+j=s} a_i \cdot b_j \right) \cdot X^s.
\end{aligned}
$$

Como A es un dominio de integridad se tiene que $a_n \cdot b_m \neq 0$, por lo que $f \cdot g \neq 0$, lo cual dice que $A[X]$ es un dominio de integridad.

Consideremos ahora $f, g \in A[X]$, con

$$\begin{aligned} f &= \sum_{i=0}^{n} a_i \cdot X^i, \\ g &= \sum_{j=0}^{m} b_j \cdot X^j. \end{aligned}$$

Queremos demostrar que si $f \cdot g \neq 0$ entonces $f \neq 0$ y $g \neq 0$. Por la contrarrecíproca, debemos demostrar que si $f = 0$ o $g = 0$ entonces $f \cdot g = 0$.

Si $f = 0$ entonces

$$\begin{aligned} f \cdot g &= 0 \cdot \left(\sum_{j=0}^{m} b_j \cdot X^j \right) \\ &= \sum_{j=0}^{m} (0 \cdot b_j) \cdot X^j \text{ por propiedad distributiva} \\ &= \sum_{j=0}^{m} 0 \cdot X^j \\ &= 0 \end{aligned}$$

Si $g = 0$ entonces

$$\begin{aligned} f \cdot g &= \left(\sum_{i=0}^{n} a_i \cdot X^i \right) \cdot 0 \\ &= \sum_{i=0}^{n} (a_i \cdot 0) \cdot X^i \text{ por propiedad distributiva} \\ &= \sum_{i=0}^{n} 0 \cdot X^i \\ &= 0 \end{aligned}$$

Esto concluye la demostración. ■

9.2. Grado de un polinomio

Dado un anillo A ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$), el anillo de polinomios $A[X]$ no posee un orden como ocurre con los números reales. Sin embargo se puede de cierta manera "medir" un polinomio sin que esto signifique contar con un orden total en $A[X]$.

Definición 9.2
Sea A un anillo conmutativo con identidad ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$) y $f \in A[X]$ dado por:

$$f = \sum_{i=0}^{n} a_i \cdot X^i, \quad a_n \neq 0.$$

Diremos que n es el grado de f y se denota como $\operatorname{gr}(f) = n$. Además diremos que a_n es el coeficiente principal de f. Diremos que f es mónico si $a_n = 1$.

Notar que el grado del polinomio nulo no está definido.

Proposición 9.3 (Propiedades del grado de un polinomio)
Sea A un anillo conmutativo con identidad que sea dominio de integridad ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$). Además consideremos $f, g \in A[X]$ tal que $f \neq 0$ y $g \neq 0$.

(a) Se cumple que $f \cdot g \neq 0$ *y* $\operatorname{gr}(f \cdot g) = \operatorname{gr}(f) + \operatorname{gr}(g)$.

(b) Para todo $k \in \mathbb{N}$ *vale que* $f^k \neq 0$ *y* $\operatorname{gr}\left(f^k\right) = k \cdot \operatorname{gr}(f)$.

(c) Si $\operatorname{gr}(f) \neq \operatorname{gr}(g)$ *entonces* $f + g \neq 0$ *y* $\operatorname{gr}(f+g) = \operatorname{máx}\{\operatorname{gr}(f), \operatorname{gr}(g)\}$.

(d) Si $f + g \neq 0$ *entonces* $\operatorname{gr}(f+g) \leqslant \operatorname{máx}\{\operatorname{gr}(f), \operatorname{gr}(g)\}$.

Demostración.
(a) Por Proposición 9.2 se tiene que $f \cdot g \neq 0$. Vamos a probar ahora que $\operatorname{gr}(f \cdot g) = \operatorname{gr}(f) + \operatorname{gr}(g)$. Si

$$\begin{aligned} f &= \sum_{i=0}^{n} a_i \cdot X^i, \quad a_n \neq 0, \\ g &= \sum_{j=0}^{m} b_j \cdot X^j, \quad b_m \neq 0, \end{aligned}$$

entonces

$$\begin{aligned} f \cdot g &= \left(\sum_{i=0}^{n} a_i \cdot X^i\right) \cdot \left(\sum_{j=0}^{m} b_j \cdot X^j\right) \\ &= \sum_{s=0}^{n+m} \left(\sum_{i+j=s} a_i \cdot b_j\right) \cdot X^s \\ &= a_n \cdot b_m \cdot X^{n+m} + \sum_{s=0}^{n+m-1} \left(\sum_{i+j=s} a_i \cdot b_j\right) \cdot X^s. \end{aligned}$$

Como $a_n \cdot b_m \neq 0$ se tiene que

$$\operatorname{gr}(f \cdot g) = n + m = \operatorname{gr}(f) + \operatorname{gr}(g).$$

(b) Es una aplicación inmediata de (a).

(c) Asumiremos que $\operatorname{gr}(f) \neq \operatorname{gr}(g)$. Demostraremos que $f+g \neq 0$ y $\operatorname{gr}(f+g) = \operatorname{máx}\{\operatorname{gr}(f), \operatorname{gr}(g)\}$. Supongamos que $n < m$ y que

$$\begin{aligned} f &= \sum_{i=0}^{n} a_i \cdot X^i, \quad a_n \neq 0, \\ g &= \sum_{j=0}^{m} b_j \cdot X^j, \quad b_m \neq 0. \end{aligned}$$

Ahora

$$\begin{aligned} f + g &= \sum_{i=0}^{n} a_i \cdot X^i + \sum_{i=0}^{m} b_i \cdot X^i \\ &= \sum_{i=0}^{n} a_i \cdot X^i + \sum_{i=0}^{n} b_i \cdot X^i + \sum_{i=n+1}^{m} b_i \cdot X^i \\ &= \sum_{i=0}^{n} (a_i + b_i) \cdot X^i + \sum_{i=n+1}^{m} b_i \cdot X^i \end{aligned}$$

Notar que el coeficiente principal de $f+g$ es b_m, lo que implica que $f+g \neq 0$ y $\operatorname{gr}(f+g) = m = \operatorname{gr}(g) = \operatorname{máx}\{\operatorname{gr}(f), \operatorname{gr}(g)\}$. Análogamente se puede probar la propiedad cuando $n > m$.

(d) Supongamos que $f+g \neq 0$. Demostraremos que $\operatorname{gr}(f+g) \leqslant \operatorname{máx}\{\operatorname{gr}(f), \operatorname{gr}(g)\}$.

Por (c) se tiene que si $\operatorname{gr}(f) \neq \operatorname{gr}(g)$ entonces se da la igualdad. Supongamos entonces que $\operatorname{gr}(f) = \operatorname{gr}(g)$. Si

$$\begin{aligned} f &= \sum_{i=0}^{n} a_i \cdot X^i, \quad a_n \neq 0, \\ g &= \sum_{j=0}^{n} b_j \cdot X^j, \quad b_n \neq 0. \end{aligned}$$

Ahora

$$\begin{aligned} f+g &= \sum_{i=0}^{n} a_i \cdot X^i + \sum_{i=0}^{n} b_i \cdot X^i \\ &= \sum_{i=0}^{n} (a_i + b_i) \cdot X^i. \end{aligned}$$

Por hipótesis estamos asumiendo que $f+g \neq 0$, por lo que existe un $j \in \{1, \ldots, n\}$ tal que $a_j + b_j \neq 0$. Luego $\operatorname{gr}(f+g) \leqslant n = \operatorname{máx}\{\operatorname{gr}(f), \operatorname{gr}(g)\}$. Notar que la igualdad se dará únicamente en el caso que $a_n + b_n \neq 0$. ■

Ejemplo 9.2

(a) Hallar todos los elementos $f \in \mathbb{C}[X]$ tal que $X \cdot f^2 - X^3 = (2 \cdot X - 1) \cdot f + 1$.

Notemos que f debe ser no nulo, pues de otro modo tendriamos que $-X^3 = 1$ lo cual es falso.

Como f es no nulo, el grado de f está definido. Llamemos $n = \operatorname{gr}(f)$.

Si ocurriera que $n > 1$ se tiene:

$$\begin{aligned} \operatorname{gr}\left(X \cdot f^2\right) &= \operatorname{gr}(X) + 2 \cdot \operatorname{gr}(f) \text{ por Proposición 9.3-(a) y 9.3-(b)} \\ &= 1 + 2 \cdot n \\ &> 1 + 2 \cdot 1 \text{ pues } n > 1 \\ &= 3. \end{aligned}$$

Luego $X \cdot f^2 - X^3 \neq 0$ y $\operatorname{gr}(X \cdot f^2 - X^3) = 1 + 2 \cdot n$ por Proposición 9.3-(c).

Análogamente,

$$\begin{aligned} \operatorname{gr}((2 \cdot X - 1) \cdot f) &= \operatorname{gr}(2 \cdot X - 1) + \operatorname{gr}(f) \text{ por Proposición 9.3-(a)} \\ &= 1 + n \\ &> 1 + 1 \text{ pues } n > 1 \\ &= 2. \end{aligned}$$

Luego $(2 \cdot X - 1) \cdot f + 1 \neq 0$ y $\operatorname{gr}((2 \cdot X - 1) \cdot f + 1) = 1 + n$ por Proposición 9.3-(c).

Por lo tanto:

$$\operatorname{gr}\left(X \cdot f^2 - X^3\right) = \operatorname{gr}((2 \cdot X - 1) \cdot f + 1) \quad \Rightarrow \quad 1 + 2 \cdot n = 1 + n$$

$$\begin{aligned} &\Rightarrow \quad 2 \cdot n = n \\ &\Rightarrow \quad n = 0, \end{aligned}$$

lo cual es una contradicción.

La única posibilidad que nos queda es que $n \leqslant 1$, es decir, $f = a \cdot X + b$, con $a, b \in \mathbb{C}$. Ahora:

$$\begin{aligned} X \cdot (a \cdot X + b)^2 - X^3 &= (2 \cdot X - 1) \cdot (a \cdot X + b) + 1 \Leftrightarrow \\ X \cdot \left(a^2 \cdot X^2 + 2 \cdot a \cdot b \cdot X + b^2\right) - X^3 &= (2 \cdot X - 1) \cdot (a \cdot X + b) + 1 \Leftrightarrow \\ a^2 \cdot X^3 + 2 \cdot a \cdot b \cdot X^2 + b^2 \cdot X - X^3 &= 2 \cdot a \cdot X^2 + 2 \cdot b \cdot X - a \cdot X - b + 1 \Leftrightarrow \\ \left(a^2 - 1\right) \cdot X^3 + 2 \cdot a \cdot b \cdot X^2 + b^2 \cdot X &= 2 \cdot a \cdot X^2 + (2 \cdot b - a) \cdot X - b + 1 \end{aligned}$$

Luego debe cumplirse que

$$\begin{aligned} a^2 - 1 &= 0, \\ 2 \cdot a \cdot b &= 2 \cdot a, \\ b^2 &= 2 \cdot b - a, \\ -b + 1 &= 0. \end{aligned}$$

De la última ecuación se ve que $b = 1$. Esto hace cumplir la segunda ecuación de manera inmediata. De la tercera ecuación se deduce que $a = 1$, lo que hace que se satisfaga la primera ecuación. Por lo tanto $f = X + 1$.

A continuación veremos la relación que existe entre los elementos inversibles de un anillo y su anillo de polinomios.

Proposición 9.4
Sea A un anillo conmutativo con identidad que es dominio de integridad ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$). Entonces los elementos inversibles de A (con respecto al producto de A) coinciden con los elementos inversibles de $A[X]$ (con respecto al producto de $A[X]$).

Demostración.
Sea $a \in A$ inversible. Esto significa que existe $b \in A$ tal que $a \cdot b = 1$. Como $A \subset A[X]$ (ver Proposición 9.1-(a)) se tiene que a es un elemento inversible de $A[X]$.

Sea $f \in A[X]$ inversible. Esto significa que existe $g \in A[X]$ tal que $f \cdot g = 1$. Como A es un dominio de integridad, la Proposición 9.2 asegura que $A[X]$ es un dominio de integridad. Luego se tiene que $f \neq 0$ y $g \neq 0$.

Ahora tenemos que

$$\begin{aligned} 1 = f \cdot g \quad &\Rightarrow \quad \operatorname{gr}(1) = \operatorname{gr}(f \cdot g) \\ &\Rightarrow \quad 0 = \operatorname{gr}(f) + \operatorname{gr}(g) \quad \text{por Proposición 9.3-(a)} \\ &\Rightarrow \quad \operatorname{gr}(f) = 0 \text{ y } \operatorname{gr}(g) = 0 \\ &\Rightarrow \quad f, g \in A \end{aligned}$$

Por lo tanto $f \in A$. Como el producto de $A[X]$ entre elementos de A coincide con el producto de A se tiene que f es un elemento inversible en A. ■

Ejemplo 9.3

(a) Los elementos inversibles de $\mathbb{Z}[X]$ son -1 y 1 (ver Observación 6.2).

(b) Si K es un cuerpo ($\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$) los elementos inversibles de $K[X]$ son exactamente los elementos de $K - \{0\}$.

9.3. Divisibilidad

Definición 9.3
Sea K un cuerpo ($\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$), y sean $f, g \in K[X]$ con $f \neq 0$. Diremos que f divide a g (y se denota $f \mid g$) si existe $h \in K[X]$ tal que $g = f \cdot h$.

Ahora veremos una serie de propiedades análogas a la divisibilidad en $\mathbb{Z}$.

Proposición 9.5 (Propiedades de divisibilidad)
Sea K un cuerpo ($\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$). Entonces:

(a) $c \cdot f \mid f, \quad \forall f \in K[X] - \{0\}$ *y* $\forall c \in K - \{0\}$.

(b) Si $f \mid g$ *y* $g \mid h$ *entonces* $f \mid h$, *donde* $f, g \in K[X] - \{0\}$ *y* $h \in K[X]$.

(c) Si $f \mid g$ *entonces* $f \mid g \cdot h$, *donde* $f \in K[X] - \{0\}$ *y* $g, h \in K[X]$.

(d) Si $f \mid g$ *y* $f \mid h$ *entonces* $f \mid g + h$, *donde* $f \in K[X] - \{0\}$ *y* $g, h \in K[X]$.

(e) $c \mid f, \quad \forall c \in K - \{0\}$ *y* $\forall f \in K[X]$.

(f) Sean $f \in K[X] - \{0\}$ *y* $c \in K - \{0\}$. *Si* $f \mid c$ *entonces* $f \in K - \{0\}$.

(g) $f \mid 0, \quad \forall f \in K[X] - \{0\}$.

(h) Sean $f, g \in K[X] - \{0\}$. *Si* $f \mid g$ *entonces* $\operatorname{gr}(f) \leqslant \operatorname{gr}(g)$.

(i) Sean $f, g \in K[X] - \{0\}$. *Si* $f \mid g$ *y* $g \mid f$ *entonces existe* $c \in K - \{0\}$ *tal que* $f = c \cdot g$.

(j) $f \mid g \Leftrightarrow c \cdot f \mid g \Leftrightarrow f \mid d \cdot g \Leftrightarrow c \cdot f \mid d \cdot g$, *donde* $c, d \in K - \{0\}$, $f, g \in K[X]$ *y* $f \neq 0$.

Demostración.
(a) Vamos a probar que $c \cdot f \mid f$ cuando $f \in K[X] - \{0\}$ y $c \in K - \{0\}$.
Notemos que

$$f = \frac{1}{c} \cdot (c \cdot f), \quad \text{con } \frac{1}{c} \in K[X].$$

Esto significa que $c \cdot f \mid f$.

(b) Supongamos que $f, g \in K[X] - \{0\}$ y $h \in K[X]$. Demostraremos que si $f \mid g$ y $g \mid h$ entonces $f \mid h$. Luego:

$$\begin{aligned} f \mid g &\Rightarrow \exists p \in K[X] : g = f \cdot p, \\ g \mid h &\Rightarrow \exists q \in K[X] : h = g \cdot q. \end{aligned}$$

Ahora:

$$h = g \cdot q = (f \cdot p) \cdot q = f \cdot (p \cdot q),$$

por lo que $f \mid h$.

(c) Asumamos que $f \in K[X] - \{0\}$ y $g, h \in K[X]$. Veremos que si $f \mid g$ entonces $f \mid g \cdot h$.
Como $f \mid g$ entonces existe $p \in K[X]$ tal que $g = f \cdot p$. Luego

$$g \cdot h = f \cdot (p \cdot h),$$

por lo que $f \mid g \cdot h$.

(d) Consideremos que $f \in K[X] - \{0\}$ y $g, h \in K[X]$. Probaremos que si $f \mid g$ y $f \mid h$ entonces $f \mid g + h$. Veamos:

$$\begin{aligned} f \mid g &\Rightarrow \exists p \in K[X] : g = f \cdot p, \\ f \mid h &\Rightarrow \exists q \in K[X] : h = f \cdot q. \end{aligned}$$

Ahora tenemos que:

$$g + h = f \cdot p + f \cdot q = f \cdot (p + q),$$

por lo que $f \mid g + h$.

(e) Supongamos que $c \in K - \{0\}$ y $f \in K[X]$. Vamos a demostrar que $c \mid f$.
Se puede escribir:

$$f = c \cdot \left(\frac{1}{c} \cdot f \right), \quad \text{donde } \frac{1}{c} \cdot f \in K[X],$$

por lo que $c \mid f$.

(f) Consideremos que $f \in K[X] - \{0\}$ y $c \in K - \{0\}$. Probaremos que si $f \mid c$ entonces $f \in K - \{0\}$.
Como $f \mid c$ entonces existe $p \in K[X]$ tal que $c = f \cdot p$. Debido a la Proposición 9.2, como $c \neq 0$ debe ocurrir necesariamente que $p \neq 0$. Tomando grado en ambos miembros tenemos que

$$0 = \operatorname{gr}(c) = \operatorname{gr}(f \cdot p) = \operatorname{gr}(f) + \operatorname{gr}(p),$$

debido a la Proposición 9.3-(a). Por lo tanto se obtiene que $\operatorname{gr}(f) = \operatorname{gr}(p) = 0$, de lo cual deducimos que $f \in K - \{0\}$.

(g) Supongamos que $f \in K[X] - \{0\}$. Vamos a probar que $f \mid 0$.
De la definición de producto en $K[X]$ es claro que $f \cdot 0 = 0$, lo cual significa que $f \mid 0$.

(h) Asumamos que $f, g \in K[X] - \{0\}$. Demostraremos que si $f \mid g$ entonces $\operatorname{gr}(f) \leqslant \operatorname{gr}(g)$.
Como $f \mid g$ entonces existe $p \in K[X]$ tal que $g = f \cdot p$. Debido a la Proposición 9.2, como $g \neq 0$ debe ocurrir necesariamente que $p \neq 0$. Luego,

$$\begin{aligned} \operatorname{gr}(f) &\leqslant \operatorname{gr}(f) + \operatorname{gr}(p) \\ &= \operatorname{gr}(f \cdot p) \text{ por Proposición 9.3-(a)} \\ &= \operatorname{gr}(g). \end{aligned}$$

(i) Sean $f, g \in K[X] - \{0\}$. Vamos a probar que si $f \mid g$ y $g \mid f$ entonces existe $c \in K - \{0\}$ tal que $f = c \cdot g$. Comencemos:

$$\begin{aligned} f \mid g &\Rightarrow \exists p \in K[X] : g = f \cdot p, \\ g \mid f &\Rightarrow \exists c \in K[X] : f = g \cdot c. \end{aligned}$$

En virtud de la Proposición 9.2 y el hecho que $f, g \in K[X] - \{0\}$ obtenemos que $p \neq 0$ y $c \neq 0$.
Ahora $g = f \cdot p = g \cdot c \cdot p$. Tomando grado se tiene que:

$$\operatorname{gr}(g) = \operatorname{gr}(g) + \operatorname{gr}(c) + \operatorname{gr}(p),$$

con lo cual se tiene que $\operatorname{gr}(c) + \operatorname{gr}(p) = 0$, y esto implica que $\operatorname{gr}(c) = 0$. Es decir, $c \in K - \{0\}$. Por lo tanto f es igual a g multipicado por un elemento no nulo del cuerpo K.

(j) Considerando que $c, d \in K - \{0\}$, $f, g \in K[X]$ y $f \neq 0$ vamos a probar las siguientes equivalencias: $f \mid g \Leftrightarrow c \cdot f \mid g \Leftrightarrow f \mid d \cdot g \Leftrightarrow c \cdot f \mid d \cdot g$.

Asumamos primero que $f \mid g$. Entonces existe $h \in K[X]$ tal que $g = f \cdot h$. Como

$$g = f \cdot h = (c \cdot f) \cdot \left(\frac{1}{c} \cdot h\right),$$

se tiene que $c \cdot f \mid g$.

Asumamos ahora que $c \cdot f \mid g$. Entonces existe $h \in K[X]$ tal que $g = (c \cdot f) \cdot h$. Multiplicando ambos miembros por d:

$$d \cdot g = d \cdot [(c \cdot f) \cdot h] = f \cdot (c \cdot d \cdot h),$$

se tiene que $f \mid d \cdot g$.

Asumamos ahora que $f \mid d \cdot g$. Entonces existe $h \in K[X]$ tal que $d \cdot g = f \cdot h$. Como

$$d \cdot g = f \cdot h = (c \cdot f) \cdot \left(\frac{1}{c} \cdot h\right),$$

se tiene que $c \cdot f \mid d \cdot g$.

Asumamos ahora que $c \cdot f \mid d \cdot g$. Entonces existe $h \in K[X]$ tal que $d \cdot g = (c \cdot f) \cdot h$. Como

$$g = \frac{1}{d} \cdot (c \cdot f) \cdot h = f \cdot \left(\frac{c}{d} \cdot h\right),$$

se tiene que $f \mid g$. ■

9.4. Algoritmo de la división

Ahora enunciaremos un teorema análogo al algoritmo de la división en $\mathbb{Z}$. Para determinar cuándo se detiene el algoritmo de la división usaremos el grado del divisor.

Teorema 9.1 (Algoritmo de la división)
Sea K un cuerpo ($\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$) y $f, g \in K[X]$ con $g \neq 0$. Entonces existen únicos $q, r \in K[X]$ tales que $f = g \cdot q + r$ donde $r = 0$ o $\operatorname{gr}(r) < \operatorname{gr}(g)$.

Demostración.

Veamos primero la existencia. Si $g \mid f$ entonces existe $h \in K[X]$ tal que $f = g \cdot h$. En este caso basta tomar $q = h$ y $r = 0$. Supongamos ahora que $g \nmid f$. Esto significa que $f - g \cdot h \neq 0$ para todo $h \in K[X]$. Por lo tanto el siguiente conjunto está bien definido:

$$S = \{\operatorname{gr}(f - g \cdot h) : h \in K[X]\}.$$

Notar que $S \subset \mathbb{N} \cup \{0\}$ y $S \neq \varnothing$. Por Proposición 6.3 se tiene que el conjunto S posee elemento minimal que llamaremos n. Es decir, existe $q \in K[X]$ tal que $n = \operatorname{gr}(f - g \cdot q)$. Definamos $r \in K[X]$ dado por $r = f - g \cdot q$ (recordar que resulta $r \neq 0$). Luego $\operatorname{gr}(r) = n$ y $f = g \cdot q + r$. Veamos ahora que $n < \operatorname{gr}(g)$. Llamando $m = \operatorname{gr}(g)$ se tiene que:

$$\begin{aligned} r &= a_n \cdot X^n + \ldots + a_0, \quad a_n \neq 0, \\ g &= b_m \cdot X^m + \ldots + b_0, \quad b_m \neq 0. \end{aligned}$$

Si ocurriera que $n \geqslant m$ entonces $n - m \geqslant 0$. Definimos ahora:

$$s = r - a_n \cdot b_m^{-1} \cdot X^{n-m} \cdot g.$$

Luego,

$$\begin{aligned}
s &= r - a_n \cdot b_m^{-1} \cdot X^{n-m} \cdot g \\
&= \left(\sum_{i=0}^{n} a_i \cdot X^i\right) - a_n \cdot b_m^{-1} \cdot X^{n-m} \cdot \left(\sum_{i=0}^{m} b_i \cdot X^i\right) \\
&= \left(\sum_{i=0}^{n} a_i \cdot X^i\right) - \left(\sum_{i=0}^{m} a_n \cdot b_m^{-1} \cdot b_i \cdot X^{i+n-m}\right) \\
&= \left(\sum_{i=0}^{n} a_i \cdot X^i\right) - \left(\sum_{i=n-m}^{n} a_n \cdot b_m^{-1} \cdot b_{i-(n-m)} \cdot X^i\right) \\
&= a_n \cdot X^n - a_n \cdot b_m^{-1} \cdot b_m \cdot X^n + \left(\sum_{i=0}^{n-1} a_i \cdot X^i\right) - \left(\sum_{i=n-m}^{n-1} a_n \cdot b_m^{-1} \cdot b_{i-(n-m)} \cdot X^i\right) \\
&= \left(\sum_{i=0}^{n-1} a_i \cdot X^i\right) - \left(\sum_{i=n-m}^{n-1} a_n \cdot b_m^{-1} \cdot b_{i-(n-m)} \cdot X^i\right).
\end{aligned}$$

Notar que el polinomio s es no nulo pues:

$$\begin{aligned}
s &= r - a_n \cdot b_m^{-1} \cdot X^{n-m} \cdot g \\
&= f - g \cdot q - a_n \cdot b_m^{-1} \cdot X^{n-m} \cdot g \\
&= f - g \cdot \left(q + a_n \cdot b_m^{-1} \cdot X^{n-m}\right) \\
&\neq 0.
\end{aligned}$$

Por Proposición 9.3-(d) obtenemos que $\operatorname{gr}(s) \leqslant n-1 < n$. Pero por otro lado se tiene que $\operatorname{gr}(s) \in S$, lo cual es una contradicción pues n era el elemento minimal de S. Esto nos dice que $n < m$, es decir, $\operatorname{gr}(r) < \operatorname{gr}(g)$.

Veamos ahora la unicidad. Supongamos que existen $q_1, r_1, q_2, r_2 \in K[X]$ tal que

$$\begin{aligned}
f &= g \cdot q_1 + r_1, \quad \text{donde } r_1 = 0 \text{ o } \operatorname{gr}(r_1) < \operatorname{gr}(g), \\
f &= g \cdot q_2 + r_2, \quad \text{donde } r_2 = 0 \text{ o } \operatorname{gr}(r_2) < \operatorname{gr}(g).
\end{aligned}$$

Comprobemos que $r_1 = r_2$ y $q_1 = q_2$.

Si ocurriera que $r_1 = r_2$ se tiene que $g \cdot (q_1 - q_2) = 0$. Como $g \neq 0$ y $K[X]$ es un dominio de integridad, obtenemos que $q_1 = q_2$.

Si ocurriera que $r_1 \neq r_2$ tenemos que $g \cdot (q_1 - q_2) = r_2 - r_1 \neq 0$ de lo cual se deduce que $q_1 - q_2 \neq 0$. Tomando grado a la igualdad resulta que:

$$\begin{aligned}
\operatorname{gr}(g) &\leqslant \operatorname{gr}(g) + \operatorname{gr}(q_1 - q_2) \\
&= \operatorname{gr}(g \cdot (q_1 - q_2)) \\
&= \operatorname{gr}(r_2 - r_1)
\end{aligned}$$

Pueden ocurrir tres casos:

- $r_1 = 0$ y $r_2 \neq 0$: en este caso tenemos que:

$$\operatorname{gr}(g) \leqslant \operatorname{gr}(r_2 - r_1) = \operatorname{gr}(r_2) < \operatorname{gr}(g).$$

- $r_1 \neq 0$ y $r_2 = 0$: en este caso tenemos que:

$$\operatorname{gr}(g) \leqslant \operatorname{gr}(r_2 - r_1) = \operatorname{gr}(-r_1) = \operatorname{gr}(r_1) < \operatorname{gr}(g).$$

- $r_1 \neq 0$ y $r_2 \neq 0$: en este caso tenemos que:

$$\operatorname{gr}(g) \leqslant \operatorname{gr}(r_2 - r_1) \leqslant \operatorname{máx}\{\operatorname{gr}(r_1), \operatorname{gr}(r_2)\} < \operatorname{gr}(g).$$

En cualquiera de los tres casos llegamos a una contradicción. ■

Observación 9.1
Notar que el algoritmo de la división está demostrado en un anillo de polinomios sobre un cuerpo. En el caso que tengamos $f, g \in \mathbb{Z}[X]$ con $g \neq 0$, en particular ambos polinomios están en $\mathbb{Q}[X]$ y allí podemos aplicar el algoritmo de la división. Luego el cociente y el resto resultan polinomios con coeficientes en $\mathbb{Q}$ (y no necesariamente en $\mathbb{Z}$).

A través de ejemplos, y basándonos en el Teorema 9.1, veremos cómo dividir polinomios de manera muy sencilla (con un procedimiento similar a la división en $\mathbb{Z}$).

Ejemplo 9.4

(a) Consideremos $f, g \in \mathbb{R}[X]$ dados por $f = 2 \cdot X^4 + 3 \cdot X^2 - X + 5$ y $g = X^3 + X^2 + 1$. Escribimos el dividendo completando las potencias faltantes. Ver Figura 9.1.

$$\begin{array}{rrrrrrrrrrr}
 & 2\cdot X^4 & + & 0\cdot X^3 & + & 3\cdot X^2 & - & 1\cdot X & + & 5 & \\
- & 2\cdot X^4 & + & 2\cdot X^3 & & & + & 2\cdot X & & & \\
\hline
 & & - & 2\cdot X^3 & + & 3\cdot X^2 & - & 3\cdot X & + & 5 & \\
- & & - & 2\cdot X^3 & - & 2\cdot X^2 & & & - & 2 & \\
\hline
 & & & & & 5\cdot X^2 & - & 3\cdot X & + & 7 & \text{resto}
\end{array}
\qquad
\begin{array}{r|l}
 & X^3 + X^2 + 1 \\
\hline
2\cdot X - 2 & \\
\text{cociente} &
\end{array}$$

Figura 9.1: Ejemplo de división de polinomios.

(b) Consideremos $f, g \in \mathbb{R}[X]$ dados por $f = 2 \cdot X^4 + 3 \cdot X^3 + 2 \cdot X + 4$ y $g = 3 \cdot X^2 + 5$. Escribimos el dividendo completando las potencias faltantes. Ver Figura 9.2.

$$\begin{array}{rrrrrrrrrrr}
 & 2\cdot X^4 & + & 3\cdot X^3 & + & 0\cdot X^2 & + & 2\cdot X & + & 4 & \\
- & 2\cdot X^4 & & & + & \frac{10}{3}\cdot X^2 & & & & & \\
\hline
 & & & 3\cdot X^3 & - & \frac{10}{3}\cdot X^2 & + & 2\cdot X & + & 4 & \\
- & & & 3\cdot X^3 & & & + & 5\cdot X & & & \\
\hline
 & & & & - & \frac{10}{3}\cdot X^2 & - & 3\cdot X & + & 4 & \\
- & & & & - & \frac{10}{3}\cdot X^2 & & & - & \frac{50}{9} & \\
\hline
 & & & & & & - & 3\cdot X & + & \frac{86}{9} & \text{resto}
\end{array}
\qquad
\begin{array}{r|l}
 & 3\cdot X^2 + 5 \\
\hline
\frac{2}{3}\cdot X^2 + X - \frac{10}{9} & \\
\text{cociente} &
\end{array}$$

Figura 9.2: Ejemplo de división de polinomios.

(c) Consideremos $f, g \in \mathbb{R}[X]$ dados por $f = 3 \cdot X^4 + 2 \cdot X^2 - 2 \cdot X + 4$ y $g = X - 2$. Escribimos el dividendo completando las potencias faltantes. Ver Figura 9.3.

Cuando el divisor es de la forma $X - a$ entonces podemos aplicar la Regla de Ruffini, que es una simplificación del procedimiento descripto en los ejemplos anteriores. Veamos los siguientes ejemplos.

$$
\begin{array}{rrrrrrrrrrr}
 & 3\cdot X^4 & + & 0\cdot X^3 & + & 2\cdot X^2 & - & 2\cdot X & + & 4 & \llcorner\ X - 2 \\
- & 3\cdot X^4 & - & 6\cdot X^3 & & & & & & & \hline \\
 & & & 6\cdot X^3 & + & 2\cdot X^2 & - & 2\cdot X & + & 4 & 3\cdot X^3 + 6\cdot X^2 + 14\cdot X + 26 \\
 & & - & 6\cdot X^3 & - & 12\cdot X^2 & & & & & \text{cociente} \\
 & & & & & 14\cdot X^2 & - & 2\cdot X & + & 4 & \\
 & & & & - & 14\cdot X^2 & - & 28\cdot X & & & \\
 & & & & & & & 26\cdot X & + & 4 & \\
 & & & & & & - & 26\cdot X & - & 52 & \\
 & & & & & & & & & 56 & \text{resto}
\end{array}
$$

Figura 9.3: Ejemplo de división de polinomios.

$$
\begin{array}{r|ccccc}
 & 3 & 0 & 2 & -2 & 4 \\
2 & & 6 & 12 & 28 & 52 \\
\hline
 & 3 & 6 & 14 & 26 & 56 \quad \text{resto} \\
 & \multicolumn{4}{c}{\text{coeficientes del cociente}} & \\
 & X^3 & X^2 & X^1 & X^0 & R
\end{array}
$$

Figura 9.4: Ejemplo de uso de la Regla de Ruffini.

Ejemplo 9.5

(a) Consideremos $f, g \in \mathbb{R}[X]$ dados por $f = 3\cdot X^4 + 2\cdot X^2 - 2\cdot X + 4$ y $g = X - 2$. Escribimos los coeficientes del dividendo completando las potencias faltantes. Ver Figura 9.4. El cociente es $3\cdot X^3 + 6\cdot X^2 + 14\cdot X + 26$ y el resto es 56.

(b) Consideremos $f, g \in \mathbb{R}[X]$ dados por $f = 6\cdot X^5 - 50\cdot X^3 + 11\cdot X^2 - 1$ y $g = X + 3$. Escribimos los coeficientes del dividendo completando las potencias faltantes. Ver Figura 9.5. El cociente es $6\cdot X^4 - 18\cdot X^3 + 4\cdot X^2 - X + 3$ y el resto es -10.

$$
\begin{array}{r|cccccc}
 & 6 & 0 & -50 & 11 & 0 & -1 \\
-3 & & -18 & 54 & -12 & 3 & -9 \\
\hline
 & 6 & -18 & 4 & -1 & 3 & -10 \quad \text{resto} \\
 & \multicolumn{5}{c}{\text{coeficientes del cociente}} & \\
 & X^4 & X^3 & X^2 & X^1 & X^0 & R
\end{array}
$$

Figura 9.5: Ejemplo de uso de la Regla de Ruffini.

9.5. Polinomios irreducibles

Dado que el conjunto de los polinomios se comporta como el anillo de los números enteros, es natural preguntarse si en los anillos de polinomios vale alguna versión del Teorema Fundamental de la Aritmética 6.9. Esto requeriría definir algo parecido a los números primos. A continuación

comenzaremos a definir los fundamentos para llegar a los análogos de los números primos en el conjunto de los polinomios.

Definición 9.4
Sea K un cuerpo ($\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$). Diremos que dos polinomios $f, g \in K[X]$ son asociados si existe $c \in K - \{0\}$ tal que $f = c \cdot g$.

Observación 9.2
Sea K un cuerpo ($\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$) y $f, g \in K[X]$ no nulos. Los polinomios f y g son asociados si y sólo si $f \mid g$ y $g \mid f$.

Demostración.
Supongamos que f y g son asociados. Entonces existe $c \in K - \{0\}$ tal que $f = c \cdot g$. En particular esto dice que $g \mid f$. Luego se tiene que $g = c^{-1} \cdot f$. En particular esto dice que $f \mid g$.

Supongamos ahora que $f \mid g$ y $g \mid f$. Por Proposición 9.5-(i) se tiene que existe $c \in K - \{0\}$ tal que $f = c \cdot g$, lo cual dice que f y g son asociados. ■

Debido a la Proposición 9.5-(a) y 9.5-(e) se tiene que todo polinomio no nulo en el anillo $K[X]$ es divisible por sus asociados y por los elementos inversibles de K. Esto es análogo a lo que sucedía con los números enteros, pues todo entero no nulo a era divisible por 1, -1, a y $-a$.

Definición 9.5
Sea K cuerpo ($\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$) y $f \in K[X]$. Diremos que f es irreducible si:

- *$f \neq 0$.*
- *f no es un elemento inversible de K (o de $K[X]$ debido a la Proposición 9.4).*
- *f es divisible sólo por elementos inversibles de K o asociados a f.*

Notemos que la noción de irreducibilidad en $K[X]$ es análoga a la noción de número primo en $\mathbb{Z}$.

Proposición 9.6
Sea K un cuerpo ($\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$) y $f \in K[X]$ con $f \neq 0$. Si $\operatorname{gr}(f) = 1$ entonces f es irreducible.

Demostración.
Sabemos que $f \neq 0$ por hipótesis. Por otro lado, la Proposición 9.4 nos asegura que f no es un elemento inversible en K pues $\operatorname{gr}(f) = 1$. Veamos ahora quiénes son los divisores de f. Sea $g \in K[X] - \{0\}$ tal que $g \mid f$. Esto significa que $f = g \cdot h$ para algún $h \in K[X]$. En virtud de la Proposición 9.2, como $f \neq 0$, debe ocurrir necesariamente que $h \neq 0$. Tomando grado se tiene que

$$1 = \operatorname{gr}(f) = \operatorname{gr}(g \cdot h) = \operatorname{gr}(g) + \operatorname{gr}(h).$$

Luego se tiene que $\operatorname{gr}(g) = 0$ o $\operatorname{gr}(g) = 1$. Si $\operatorname{gr}(g) = 0$ entonces g es un elemento inversible de K. Si $\operatorname{gr}(g) = 1$ entonces $\operatorname{gr}(h) = 0$ y h resulta un elemento inversible de K, lo cual dice que f y g son asociados. ■

A continuación veamos una caracterización de los polinomios irreducibles en términos del grado.

Observación 9.3
Sea K un cuerpo ($\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$) y $f \in K[X]$. Entonces f es irreducible si y sólo si:

- *$f \neq 0$ y $\operatorname{gr}(f) \geqslant 1$.*
- *Dado $g \in K[X] - \{0\}$ tal que $g \mid f$ entonces $\operatorname{gr}(g) = 0$ o $\operatorname{gr}(g) = \operatorname{gr}(f)$.*

Demostración.

Asumamos primero que f es irreducible. Luego por Definición 9.5 se tiene que $f \neq 0$. Debido a la Proposición 9.4 y a la Definición 9.5 se tiene que $\text{gr}(f) > 0$, es decir, $\text{gr}(f) \geqslant 1$. Sea ahora $g \in K[X]$ un divisor de f. Luego existe $h \in K[X]$ tal que $f = g \cdot h$. Por la Proposición 9.2 se tiene que $h \neq 0$. Tomando grado se tiene:

$$\text{gr}(f) = \text{gr}(g) + \text{gr}(h).$$

utilizando la Proposición 9.3-(a). Por la Definición 9.5 g es un elemento inversible de K (o sea, $\text{gr}(g) = 0$) o g está asociado a f (o sea, $\text{gr}(g) = \text{gr}(f)$).

Asumamos ahora que se satisfacen las condiciones del enunciado. Una de esas hipótesis es que $f \neq 0$. Como $\text{gr}(f) \geqslant 1$ se tiene que f no es un elemento inversible de K. Supongamos ahora que $g \in K[X] - \{0\}$ es un divisor de f, es decir, existe $h \in K[X]$ tal que $f = g \cdot h$. Por la Proposición 9.2 se tiene que $h \neq 0$. Por hipótesis se tiene que $\text{gr}(g) = 0$ o $\text{gr}(g) = \text{gr}(f)$. Si $\text{gr}(g) = 0$ entonces g es un elemento inversible de K. Si $\text{gr}(g) = \text{gr}(f)$ entonces $\text{gr}(h) = 0$, lo que significa que f y g son asociados. Por lo tanto f resulta irreducible. ■

Ahora presentaremos un análogo del Teorema 6.2.

Proposición 9.7
Sea K un cuerpo ($\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$) y $f \in K[X]$ tal que $f \neq 0$ y $\text{gr}(f) > 0$ (es decir, $f \neq 0$ y f no es inversible en K). Entonces existe $h \in K[X]$ irreducible tal que $h \mid f$.

Demostración.

Definamos el siguiente conjunto:

$$A = \{\text{gr}(g) : g \in K[X] - \{0\}, g \mid f, \text{gr}(g) \geqslant 1\}.$$

Notemos que $A \subset \mathbb{N}$ y $A \neq \varnothing$ pues $\text{gr}(f) \in A$. Como $\mathbb{N}$ es bien ordenado, se tiene que A posee elemento minimal que llamaremos n. Es decir, existe $h \in K[X] - \{0\}$, $h \mid f$ y $\text{gr}(h) = n \geqslant 1$. Veamos que h satisface las condiciones de la Observación 9.3:

- Por definición del conjunto A tenemos que $h \neq 0$ y $\text{gr}(h) \geqslant 1$.
- Sea $g \in K[X]$ tal que $g \mid h$. Si $\text{gr}(g) = 0$ listo. Si $\text{gr}(g) \neq 0$ entonces $\text{gr}(g) \geqslant 1$. Como $g \mid h$ y $h \mid f$ entonces $g \mid f$ debido a la Proposición 9.5-(b). Luego $\text{gr}(g) \in A$. Debido a que $\text{gr}(h)$ es elemento minimal obtenemos que $\text{gr}(h) \leqslant \text{gr}(g)$. Por otro lado, como $g \mid h$ obtenemos que $\text{gr}(g) \leqslant \text{gr}(h)$ por Proposición 9.5-(h). Por lo tanto concluimos que $\text{gr}(h) = \text{gr}(g)$.

Esto concluye la proposición. ■

También hay un análogo del Teorema 6.6 que se presenta a continuación.

Proposición 9.8
Sea K un cuerpo ($\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$) y $f \in K[X]$ irreducible. Si $g, h \in K[X]$ tal que $f \mid g \cdot h$ entonces $f \mid g$ o $f \mid h$.

Demostración.

Supongamos que $f \nmid g$ y que $f \nmid h$. Esto implica que $g \neq 0$ pues si ocurriese que $g = 0$ entonces $f \mid g$ y esto contradice nuestra suposición.

Llamamos

$$H = \{\text{gr}(p) : p \in K[X] - \{0\}, f \mid p \cdot h, f \nmid p, f \nmid h\}.$$

Como $\text{gr}(g) \in H$ entonces $H \neq \varnothing$.

Además $H \subset \mathbb{N} \cup \{0\}$, aunque en realidad $H \subset \mathbb{N}$, pues si $0 \in H$ entonces existe $p \in K[X]$ tal que $p \neq 0$ y $\text{gr}(p) = 0$. Como $f \mid p \cdot h$ entonces $f \mid h$ por Proposición 9.5-(j), y esto es una contradicción.

Como $\mathbb{N}$ es bien ordenado, existe elemento minimal en H que llamaremos n. Luego existe $a \in K[X]$ tal que

$$f \mid a \cdot h, \quad f \nmid a, \quad f \nmid h, \quad \operatorname{gr}(a) = n \geqslant 1.$$

Por el algoritmo de la división (ver Teorema 9.1), existen $s, t \in K[X]$ tal que

$$a = f \cdot s + t, \quad \text{donde } t = 0 \text{ o } \operatorname{gr}(t) < \operatorname{gr}(f).$$

Se puede ver que $t \neq 0$, pues de otro modo $f \mid a$ lo cual es una contradicción. Además, debido a que $f \mid f \cdot s$ ocurre que $f \nmid t$, pues de otro modo tendríamos que $f \mid a$ lo cual es una contradicción nuevamente.

Multiplicamos por h quedando

$$a \cdot h = f \cdot s \cdot h + t \cdot h.$$

Como $f \mid a \cdot h$ y $f \mid f \cdot s \cdot h$ entonces $f \mid t \cdot h$. Juntando todo tenemos que $\operatorname{gr}(t) \in H$. Como $\operatorname{gr}(a)$ es el elemento minimal de H se tiene que:

$$\operatorname{gr}(a) \leqslant \operatorname{gr}(t) < \operatorname{gr}(f).$$

Utilizando el algoritmo de la división nuevamente, existen únicos $y, d \in K[X]$ tal que

$$f = a \cdot y + d, \quad \text{donde } d = 0 \text{ o } \operatorname{gr}(d) < \operatorname{gr}(a).$$

Si ocurriese que $d = 0$ entonces $a \mid f$. Como sabemos que $\operatorname{gr}(a) < \operatorname{gr}(f)$ y que f es irreducible, la Observación 9.3 nos dice que $\operatorname{gr}(a) = 0$, lo cual es una contradicción. Por lo tanto ocurre que $d \neq 0$ y $\operatorname{gr}(d) < \operatorname{gr}(a)$.

Multiplicando por h tenemos que

$$f \cdot h = a \cdot h \cdot y + d \cdot h.$$

Como $f \mid f \cdot h$ y $f \mid a \cdot h$ resulta que $f \mid d \cdot h$.

Juntando todo tenemos que $d \in K[X] - \{0\}$, $f \mid d \cdot h$, $f \nmid d$ (pues $\operatorname{gr}(d) < \operatorname{gr}(a) < \operatorname{gr}(f)$) y $f \nmid h$. Por lo tanto tenemos un elemento en H, a saber $\operatorname{gr}(d)$, que es menor al elemento minimal $\operatorname{gr}(a)$. Esto es una contradicción.

Finalmente debe ocurrir que $f \mid g$ o $f \mid h$. ■

9.6. Teorema fundamental de la Aritmética

El análogo del Teorema Fundamental de la Aritmética para números enteros se presenta a continuación.

Teorema 9.2 (Teorema fundamental de la Aritmética para polinomios)
Sea K un cuerpo ($\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$), $f \in K[X]$, $f \neq 0$ y $\operatorname{gr}(f) > 0$. Entonces existen $p_1, \ldots, p_r \in K[X]$ irreducibles mónicos, $c \in K - \{0\}$, $n_1, \ldots, n_r \in \mathbb{N}$ tales que

$$f = c \cdot p_1^{n_1} \cdot \ldots \cdot p_r^{n_r}.$$

Además esta escritura es única salvo el orden de los factores.

Demostración.

La demostración es similar a la demostración del Teorema 6.9. Podemos asumir sin pérdida de generalidad que f es mónico.

Analicemos primero la existencia de la descomposición. Razonemos por al absurdo y asumamos que f no admite una descomposición como dice el enunciado. Sea

$$H = \{\operatorname{gr}(p) : p \in K[X] - \{0\}, \operatorname{gr}(p) > 0, p \text{ es mónico y no admite descomposición}\}.$$

Luego $H \neq \varnothing$ pues $\operatorname{gr}(f) \in H$. Además $H \subset \mathbb{N}$. Como $\mathbb{N}$ es bien ordenado, se tiene que H tiene elemento minimal que llamaremos n. Es decir, existe $q \in K[X] - \{0\}$, $\operatorname{gr}(q) = n > 0$ tal que q es mónico y no admite descomposición.

Notemos que q no puede ser irreducible, pues de otro modo él sería su misma descomposición. Por Proposición 9.7 existe $p_1 \in K[X]$ irreducible tal que $p_1 \mid q$. Por Proposición 9.5-(j) podemos elegir que p_1 sea mónico. Luego existe $h_1 \in K[X]$ tal que $q = p_1 \cdot h_1$. Notemos que debe ocurrir que $h_1 \neq 0$ y mónico. Por Observación 9.3 debe ocurrir que $0 < \operatorname{gr}(p_1) < \operatorname{gr}(q)$ y $0 < \operatorname{gr}(h_1) < \operatorname{gr}(q)$. Como $0 < \operatorname{gr}(h_1) < \operatorname{gr}(q)$ se tiene que $\operatorname{gr}(h_1) \notin H$, por lo que h_1 admite una descomposición. Esto significa que q admite una descomposición, lo cual es una contradicción.

Ahora analicemos la unicidad de la descomposición. Supongamos que:

$$\begin{aligned} f &= c \cdot p_1 \cdot \ldots \cdot p_k, \quad \text{donde } c \in K - \{0\} \text{ y } p_1, \ldots, p_k \text{ irreducibles mónicos} \\ f &= d \cdot q_1 \cdot \ldots \cdot q_t, \quad \text{donde } d \in K - \{0\} \text{ y } q_1, \ldots, q_t \text{ irreducibles mónicos} \end{aligned}$$

Notemos que es claro que $c = d$. Probaremos que la descomposición es única utilizando inducción en k.

Si $k = 1$ entonces $t = 1$, pues de otro modo, p_1 no sería irreducible (ver Observación 9.3). Luego la unicidad queda probada. Supongamos que la unicidad está garantizada para k y vamos a probar para $k+1$. Tenemos entonces:

$$p_1 \cdot \ldots \cdot p_k \cdot p_{k+1} = q_1 \cdot \ldots \cdot q_t.$$

Luego tenemos que $p_1 \mid q_1 \cdot \ldots \cdot q_t$. Por Proposición 9.8 ocurre que $p_1 \mid q_j$ para algún $j = 1, \ldots, t$. Por Definición 9.5 debe ocurrir que p_1 es asociado a q_j. Como ambos son mónicos sucede que $p_1 = q_j$. Debido a que $K[X]$ es un dominio de integridad obtenemos que:

$$p_2 \cdot \ldots \cdot p_{k+1} = q_1 \cdot \ldots \cdot \widehat{q_j} \cdot \ldots \cdot q_t,$$

donde $\widehat{q_j}$ indica que el término j debe excluirse. Ahora usamos la hipótesis inductiva (pues en el lado izquierdo aparecen k polinomios irreducibles mónicos) para deducir que $k = t - 1$, con lo que $t = k + 1$ (esto significa que la cantidad de polinomios mónicos irreducibles de la factorización es la misma en ambos lados de la igualdad) y los polinomios irreducibles coinciden salvo el orden en que ellos aparecen. De esta manera queda demostrada la unicidad. ■

9.7. Especialización

Definición 9.6 (Especialización)
Sea A un anillo conmutativo con identidad ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$), $f \in A[X]$ definido por $\sum_{i=0}^{n} a_i \cdot X^i$ y $c \in A$. Llamaremos especialización de f en c al elemento de A definido por:

$$f(c) = \sum_{i=0}^{n} a_i \cdot c^i.$$

Proposición 9.9 (Propiedades de la especialización)
Sea A un anillo conmutativo con identidad ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$), $f, g \in A[X]$ y $c \in A$. Entonces

(a) $(f+g)(c) = f(c) + g(c)$.

(b) $(f \cdot g)(c) = f(c) \cdot g(c)$.

Demostración.

Asumamos que $f = \sum_{i=0}^{n} a_i \cdot X^i$ y $g = \sum_{i=0}^{n} b_i \cdot X^i$ (podemos asumir sin pérdida de generalidad que f y g poseen igual cantidad de sumandos, completando con coeficientes nulos si es necesario).

(a) Vamos a probar que $(f+g)(c) = f(c) + g(c)$.

$$\begin{aligned}
(f+g)(c) &= \left(\sum_{i=0}^{n} a_i \cdot X^i + \sum_{i=0}^{n} b_i \cdot X^i\right)(c) \\
&= \left(\sum_{i=0}^{n} (a_i + b_i) \cdot X^i\right)(c) \\
&= \sum_{i=0}^{n} (a_i + b_i) \cdot c^i \\
&= \sum_{i=0}^{n} \left(a_i \cdot c^i + b_i \cdot c^i\right) \\
&= \sum_{i=0}^{n} a_i \cdot c^i + \sum_{i=0}^{n} b_i \cdot c^i \\
&= f(c) + g(c).
\end{aligned}$$

(b) Vamos a demostrar que $(f \cdot g)(c) = f(c) \cdot g(c)$.

$$\begin{aligned}
(f \cdot g)(c) &= \left[\left(\sum_{i=0}^{n} a_i \cdot X^i\right) \cdot \left(\sum_{j=0}^{n} b_j \cdot X^j\right)\right](c) \\
&= \left(\sum_{k=0}^{n+n} \left(\sum_{i+j=k} a_i \cdot b_j\right) \cdot X^k\right)(c) \\
&= \sum_{k=0}^{n+n} \left(\sum_{i+j=k} a_i \cdot b_j\right) \cdot c^k \\
&= \left(\sum_{i=0}^{n} a_i \cdot c^i\right) \cdot \left(\sum_{j=0}^{n} b_j \cdot c^j\right) \\
&= f(c) \cdot g(c)
\end{aligned}$$

Esto concluye la demostración. ■

Definición 9.7 (Raíz de un polinomio)
Sea A un anillo conmutativo con identidad ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$), $f \in A[X]$, $a \in A$. Diremos que a es una raíz de f si $f(a) = 0$.

9.8. Teorema del resto y consecuencias

Teorema 9.3 (Teorema del resto)
Sea K un cuerpo ($\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$), $f \in K[X]$ y $a \in K$. Entonces el resto de la división de f por $X - a$ es $f(a)$.

Demostración.
Por el Teorema 9.1 existen únicos $q, r \in K[X]$ tales que

$$f = (X - a) \cdot q + r,$$

donde $r = 0$ o $\operatorname{gr}(r) < \operatorname{gr}(X-a) = 1$. Especializamos f en a, y debido a la Proposición 9.9, obtenemos:

$$\begin{aligned} f(a) &= (a-a)\cdot q(a) + r(a) \\ &= 0 \cdot q(a) + r(a), \\ &= 0 + r(a) \\ &= r(a), \end{aligned}$$

Ya sea que $r = 0$ o que $\operatorname{gr}(r) < 1$ se tiene que $r \in K$. Luego $r = r(a) = f(a)$. ■

Ejemplo 9.6

(a) Consideremos $f, g \in \mathbb{R}[X]$ dados por $f = 3 \cdot X^4 + 2 \cdot X^2 - 2 \cdot X + 4$ y $g = X - 2$. El Teorema 9.3 nos dice que el resto de dividir f por g está dado por:

$$\begin{aligned} f(2) &= 3 \cdot 2^4 + 2 \cdot 2^2 - 2 \cdot 2 + 4 \\ &= 3 \cdot 16 + 2 \cdot 4 - 2 \cdot 2 + 4 \\ &= 48 + 8 - 4 + 4 \\ &= 56. \end{aligned}$$

Ver Figura 9.4.

(b) Consideremos $f, g \in \mathbb{R}[X]$ dados por $f = 6 \cdot X^5 - 50 \cdot X^3 + 11 \cdot X^2 - 1$ y $g = X + 3$. El Teorema 9.3 nos dice que el resto de dividir f por g está dado por:

$$\begin{aligned} f(-3) &= 6 \cdot (-3)^5 - 50 \cdot (-3)^3 + 11 \cdot (-3)^2 - 1 \\ &= 6 \cdot (-243) - 50 \cdot (-27) + 11 \cdot 9 - 1 \\ &= -1458 + 1350 + 99 - 1 \\ &= -10. \end{aligned}$$

Ver Figura 9.5.

Teorema 9.4

Sea K un cuerpo ($\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$), $a \in K$ y $f \in K[X]$. Entonces a es raíz de f si y sólo si $X - a \mid f$.

Demostración.

Por el algoritmo de la división se tiene que existen $q, r \in K[X]$ tal que

$$f = (X-a)\cdot q + r, \quad r \in K.$$

Especializando los polinomios usando la Proposición 9.9 tenemos que:

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

Por lo tanto a es raíz de f si y sólo si $r = 0$ (o sea $X - a \mid f$). ■

9.9. Máximo común divisor

Teorema 9.5

Sea K un cuerpo ($\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$), $f, g \in K[X]$ tales que $f \neq 0$ o $g \neq 0$. Entonces existe un único $d \in K[X]$ mónico que satisface

(a) $d \mid f$ y $d \mid g$.

(b) Existen $u, v \in K[X]$ tales que $d = u \cdot f + v \cdot g$.

Demostración.

Sin pérdida de generalidad, podemos asumir que $g \neq 0$. De otro modo se pueden intercambiar los roles de f y g.

Analizaremos primero la existencia.

Haremos la prueba por inducción en $\operatorname{gr}(g)$. Sea la siguiente función proposicional en $\mathbb{N} \cup \{0\}$:

$$P(n): \quad \forall f, g \in K[X] \text{ tal que } g \neq 0 \text{ y } \operatorname{gr}(g) = n, \exists d \in K[X] : \begin{cases} d \text{ es mónico,} \\ d \mid f \text{ y } d \mid g, \\ \exists u, v \in K[X] : d = u \cdot f + v \cdot g. \end{cases}$$

Observemos que $P(0)$ es V. Para ello tomemos $f, g \in K[X]$ donde $g \neq 0$ y $\operatorname{gr}(g) = 0$ (esto último significa que $g \in K - \{0\}$). Tomar $d = 1$ (notar que $d \in K[X]$ y es mónico). Luego:

$1 \mid f$ y $1 \mid g$ por Proposición 9.5-(e)

Sean $u = 0 \in K[X]$ y $v = g^{-1} \in K[X]$. Luego $u \cdot f + v \cdot g = 0 \cdot f + g^{-1} \cdot g = 1$.

Asumamos ahora que

$$\forall n \in \mathbb{N} \cup \{0\}, n > 0, \quad P(k) \text{ es } V \text{ para todo } k < n.$$

Veamos que $P(n)$ es V. Sean $f, g \in K[X]$ con $g \neq 0$ y $\operatorname{gr}(g) = n$. Luego existen únicos $g', r \in K[X]$ tales que

$$f = g' \cdot g + r, \quad \text{donde } r = 0 \text{ o } \operatorname{gr}(r) < \operatorname{gr}(g).$$

debido al algoritmo de la división (Teorema 9.1).

Ahora tenemos dos opciones.

- Si $r = 0$:

  $g \mid f$ pues $f = g' \cdot g$

  $g \mid g$ por Proposición 9.5-(a)

  Tomar d el polinomio asociado a g de modo que d sea mónico (o sea, $g = c \cdot d$ donde c es el coeficiente principal de g). Luego notar que:

  $d \mid f$ pues d y g son asociados

  $d \mid g$ pues d y g son asociados

  Sean $u = 0 \in K[X], v = c^{-1} \in K[X]$. Luego $u \cdot f + v \cdot g = 0 \cdot f + c^{-1} \cdot g = d$.

- Si $r \neq 0$, entonces $\operatorname{gr}(r) < \operatorname{gr}(g) = n$. Como $P(\operatorname{gr}(r))$ es V por hipótesis, existe $d \in K[X]$ mónico tal que

  $$\begin{aligned} &d \mid g \text{ y } d \mid r, \\ &\exists z, w \in K[X] : d = z \cdot g + w \cdot r. \end{aligned}$$

  Además,

  $$\left.\begin{array}{l} d \mid g \Rightarrow d \mid g' \cdot g \\ d \mid r \end{array}\right\} \Rightarrow \quad d \mid g' \cdot g + r \Rightarrow d \mid f$$

Finalmente

$$\begin{aligned} d &= z \cdot g + w \cdot r = z \cdot g + w \cdot (f - g' \cdot g) \\ &= z \cdot g - w \cdot g' \cdot g + w \cdot f \\ &= w \cdot f + (z - w \cdot g') \cdot g. \end{aligned}$$

Juntando todo tenemos que:

$$\begin{aligned} &d \mid f \text{ y } d \mid g, \\ &\text{Sean } u = w \in K[X], v = z - w \cdot g' \in K[X] \text{ donde } d = u \cdot f + v \cdot g. \end{aligned}$$

Esto nos dice que $P(n)$ es V. Luego la proposición $\forall n \in \mathbb{N} \cup \{0\}, P(n)$ es V debido al Criterio 5.2.

Analizaremos ahora la unicidad.

Supongamos que existe $d' \in K[X]$ mónico tal que

$$\begin{aligned} &d' \mid f \text{ y } d' \mid g, \\ &\exists u', v' \in K[X] : d' = u' \cdot f + v' \cdot g. \end{aligned}$$

Ahora

$$\left.\begin{array}{rcl} d \mid f & \Rightarrow & d \mid u' \cdot f \\ d \mid g & \Rightarrow & d \mid v' \cdot g \end{array}\right\} \Rightarrow d \mid u' \cdot f + v' \cdot g \Rightarrow d \mid d'$$

Análogamente

$$\left.\begin{array}{rcl} d' \mid f & \Rightarrow & d' \mid u \cdot f \\ d' \mid g & \Rightarrow & d' \mid v \cdot g \end{array}\right\} \Rightarrow d' \mid u \cdot f + v \cdot g \Rightarrow d' \mid d$$

Debido a la Proposición 9.5-(i) se tiene que d y d' son asociados. Como ambos son mónicos se deduce que $d = d'$. ■

Al único d que nos da el Teorema 9.5 se lo denomina el máximo común divisor entre f y g, y se denota por (f, g). Al igual que ocurría en los números enteros, se tiene que $(f, g) = (g, f)$.

La demostración del Teorema 9.5 nos sugiere una forma de encontrar el máximo común divisor.

Ejemplo 9.7

(a) Hallar $d = (X^4 + X^3 - 2 \cdot X - 2, X^3 + X^2 + X + 1)$.

Primero usamos el algoritmo de la división:

$$X^4 + X^3 - 2 \cdot X - 2 = \left(X^3 + X^2 + X + 1\right) \cdot X + \left(-X^2 - 3 \cdot X - 2\right).$$

De acuerdo a la demostración hay que hallar el máximo común divisor entre $X^3 + X^2 + X + 1$ y $-X^2 - 3 \cdot X - 2$. Usamos otra vez el algoritmo de la división:

$$X^3 + X^2 + X + 1 = \left(-X^2 - 3 \cdot X - 2\right) \cdot (-X + 2) + (5 \cdot X + 5).$$

De acuerdo a la demostración hay que hallar el máximo común divisor entre $-X^2 - 3 \cdot X - 2$ y $5 \cdot X + 5$. Usamos otra vez el algoritmo de la división:

$$-X^2 - 3 \cdot X - 2 = (5 \cdot X + 5) \cdot \left(-\frac{1}{5} \cdot X - \frac{2}{5}\right).$$

Como el resto es 0, el máximo común divisor es el polinomio mónico asociado a $5 \cdot X + 5$, es decir,

$$d = X + 1.$$

(b) Hallar $d = (X^3 - 2, X^2 + 1)$.

Primero usamos el algoritmo de la división:

$$X^3 - 2 = \left(X^2 + 1\right) \cdot X + (-X - 2)\,.$$

De acuerdo a la demostración hay que hallar el máximo común divisor entre $X^2 + 1$ y $-X - 2$. Usamos otra vez el algoritmo de la división:

$$X^2 + 1 = (-X - 2) \cdot (-X + 2) + 5.$$

De acuerdo a la demostración hay que hallar el máximo común divisor entre $-X - 2$ y 5. Usamos otra vez el algoritmo de la división:

$$-X - 2 = 5 \cdot \left(-\frac{1}{5} \cdot X - \frac{2}{5}\right).$$

Como el resto es 0, el máximo común divisor es el polinomio mónico asociado a 5, es decir,

$$d = 1.$$

(c) Si $a, b \in K$, $a \neq b$, K cuerpo ($\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$), entonces $d = (X - a, X - b) = 1$.

Primero usamos el algoritmo de la división:

$$X - a = (X - b) \cdot 1 + (b - a)\,.$$

De acuerdo a la demostración hay que hallar el máximo común divisor entre $X - b$ y $b - a$. Usamos otra vez el algoritmo de la división:

$$X - b = (b - a) \cdot \left[(b - a)^{-1} \cdot (X - b)\right].$$

Como el resto es 0, el máximo común divisor es el polinomio mónico asociado a $b - a$, es decir,

$$d = 1.$$

Al igual que ocurría con los números enteros, la siguiente propiedad nos muestra que todo divisor simultáneo de dos polinomios debe necesariamente dividir a su máximo común divisor (ver Proposición 6.8).

Corolario 9.1
Sea K un cuerpo ($\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$), $f, g, h \in K[X]$, $h \neq 0$, y f y g no simultáneamente nulos. Si $h \mid f$ y $h \mid g$, entonces $h \mid (f, g)$.

Demostración.
Por Teorema 9.5 se sigue que existen $u, v \in K[X]$ tal que $(f, g) = u \cdot f + v \cdot g$. Ahora:

$$\left.\begin{array}{rcl} h \mid f & \Rightarrow & h \mid u \cdot f \\ h \mid g & \Rightarrow & h \mid v \cdot g \end{array}\right\} \Rightarrow h \mid u \cdot f + v \cdot g \Rightarrow h \mid (f, g)$$

Esto concluye la demostración. ■

Definición 9.8
Sea K un cuerpo ($\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$) y $f, g \in K[X]$ no simultáneamente nulos. Diremos que f y g son coprimos si $(f, g) = 1$.

A continuación mostramos el equivalente al Teorema 6.7 pero en el anillo de polinomios.

Teorema 9.6
Sea K cuerpo ($\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$) y $f, g, h \in K[X]$. Entonces:

(a) Si $(f, g) = 1$, $f \mid h$ y $g \mid h$, entonces $f \cdot g \mid h$.

(b) Si $(f, h) = 1$ y $f \mid g \cdot h$, entonces $f \mid g$.

Demostración.
(a) Como $(f, g) = 1$ tenemos que existen $u, v \in K[X]$ tales que:

$$1 = u \cdot f + v \cdot g.$$

Multiplicando por h ambos miembros tenemos que:

$$h = u \cdot h \cdot f + v \cdot h \cdot g.$$

Como $f \mid h$ entonces existe $f' \in K[X]$ tal que $h = f' \cdot f$.
Como $g \mid h$ entonces existe $g' \in K[X]$ tal que $h = g' \cdot g$.
Reemplazando obtenemos que:

$$\begin{aligned} h &= u \cdot g' \cdot g \cdot f + v \cdot f' \cdot f \cdot g \\ &= (u \cdot g' + v \cdot f') \cdot f \cdot g. \end{aligned}$$

Esto último dice que $f \cdot g \mid h$.

(b) Como $(f, h) = 1$ existen $u, v \in K[X]$ tales que

$$1 = u \cdot f + v \cdot h.$$

Multiplicando por g a ambos miembros:

$$g = u \cdot f \cdot g + v \cdot h \cdot g.$$

Ahora:

$$\left.\begin{array}{rcl} f \mid f & \Rightarrow & f \mid u \cdot f \cdot g \\ f \mid g \cdot h & \Rightarrow & f \mid v \cdot h \cdot g \end{array}\right\} \Rightarrow f \mid u \cdot f \cdot g + v \cdot h \cdot g$$
$$\Rightarrow f \mid g.$$

■

Ejemplo 9.8
(a) El Teorema 9.6-(a) podría ser falso en caso de que $(f, g) \neq 1$.

Sean $f, g, h \in \mathbb{R}[X]$ definidos por:

$$\begin{aligned} f &= x, \\ g &= x^2 - x, \\ h &= x^2 - x. \end{aligned}$$

Ahora como $x^2 - x = x \cdot (x - 1)$ entonces $f \mid h$ y $f \mid g$ (lo cual dice también que $(f, g) = f \neq 1$).
Por otro lado, como $g = h$ tenemos que $g \mid h$. Ahora:

$$f \cdot g = x \cdot \left(x^2 - x\right) = x^3 - x^2.$$

Si $f \cdot g \mid h$ entonces $\operatorname{gr}(f \cdot g) \leqslant \operatorname{gr}(h)$ debido a la Proposición 9.5-(h), pero esto diría que $3 \leqslant 2$ lo cual es una contradicción.

(b) El Teorema 9.6-(b) podría ser falso en caso de que $(f,h) \neq 1$.

Sean $f, g, h \in \mathbb{R}[X]$ definidos por:

$$\begin{aligned} f &= x^2, \\ g &= x, \\ h &= x. \end{aligned}$$

Notemos que $(f,h) = h \neq 1$ pues $h \mid f$. Es claro que $f \mid g \cdot h$, pero ni $f \nmid g$ ni $f \nmid h$ debido a la Proposición 9.5-(h).

Proposición 9.10
Sea K un cuerpo ($\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$) y $f, g \in K[X]$ no simultáneamente nulos. Entonces f y g no son coprimos si y sólo si existe $p \in K[X]$ irreducible tal que $p \mid f$ y $p \mid g$.

Demostración.

Llamemos $d = (f,g)$.

Asumamos primero que f y g no son coprimos, es decir, $d \neq 1$ (y por lo tanto $\operatorname{gr}(d) > 0$). Por Proposición 9.7 existe $p \in K[X]$ irreducible tal que $p \mid d$. Ahora:

$$\begin{aligned} p \mid d \text{ y } d \mid f &\Rightarrow p \mid f \\ p \mid d \text{ y } d \mid g &\Rightarrow p \mid g. \end{aligned}$$

Ahora asumamos que existe $p \in K[X]$ irreducible tal que $p \mid f$ y $p \mid g$. Como p es irreducible se tiene que $\operatorname{gr}(p) \geqslant 1$ por Observación 9.3. Por otro lado, el Corolario 9.1 nos dice que $p \mid d$. Por Proposición 9.5-(h) tenemos que $\operatorname{gr}(d) \geqslant 1$. Esto dice que $d \neq 1$, es decir, f y g no son coprimos. ■

9.10. Criterios para las raíces

El siguiente teorema nos muestra cuáles son los candidatos a raíces racionales de un polinomio con coeficientes enteros.

Teorema 9.7 (Criterio de Gauss)
Sea $f \in \mathbb{Z}[X]$, $f = \sum_{i=0}^{n} a_i \cdot X^i$. Si $\frac{p}{q}$ (con p y q enteros no nulos coprimos) es una raíz de f, entonces $p \mid a_0$ y $q \mid a_n$.

Demostración.

Como $\dfrac{p}{q}$ es una raíz de f se tiene que

$$0 = f\left(\frac{p}{q}\right) = \sum_{i=0}^{n} a_i \cdot \frac{p^i}{q^i}.$$

Multiplicando por q^n obtenemos que:

$$\sum_{i=0}^{n} a_i \cdot p^i \cdot q^{n-i} = 0.$$

Luego

$$0 = a_0 \cdot q^n + \sum_{i=1}^{n} a_i \cdot p^i \cdot q^{n-i} = a_0 \cdot q^n + p \cdot \sum_{i=1}^{n} a_i \cdot p^{i-1} \cdot q^{n-i}$$

Por lo tanto,

$$a_0 \cdot q^n = p \cdot \underbrace{\left(-\sum_{i=1}^{n} a_i \cdot p^{i-1} \cdot q^{n-i} \right)}_{s \in \mathbb{Z}} = p \cdot s.$$

Luego, $p \mid a_0 \cdot q^n$. Como $(p, q) = 1$ entonces $p \mid a_0$ por Teorema 6.7-(b).

Análogamente, tenemos que:

$$0 = \sum_{i=0}^{n-1} a_i \cdot p^i \cdot q^{n-i} + a_n \cdot p^n = q \cdot \sum_{i=0}^{n-1} a_i \cdot p^i \cdot q^{n-i-1} + a_n \cdot p^n.$$

Por lo tanto,

$$a_n \cdot p^n = q \cdot \underbrace{\left(-\sum_{i=0}^{n-1} a_i \cdot p^i \cdot q^{n-i-1} \right)}_{t \in \mathbb{Z}} = q \cdot t.$$

Luego, $q \mid a_n \cdot p^n$. Como $(p, q) = 1$ entonces $q \mid a_n$ por Teorema 6.7-(b). ■

Ejemplo 9.9

(a) Determinar las raíces racionales de $f = 8 \cdot X^3 + 10 \cdot X^2 - 11 \cdot X + 2$.

Si $\frac{p}{q}$ es una raíz de f (con p y q enteros no nulos coprimos), el criterio de Gauss nos dice que $p \mid 2$ y $q \mid 8$.

Los candidatos para p son: 1, 2, -1, -2.

Los candidatos para q son: 1, 2, 4, 8, -1, -2, -4, -8.

Por lo tanto, las posibles raíces racionales son:

$$1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, -1, -\frac{1}{2}, -\frac{1}{4}, -\frac{1}{8}, 2, -2.$$

Para confirmar o descartar las raíces especializamos f:

$$f(1) = 9, \quad f\left(\frac{1}{2}\right) = 0, \quad f\left(\frac{1}{4}\right) = 0, \quad f\left(\frac{1}{8}\right) = \frac{51}{64}, \quad f(-1) = 15,$$

$$f\left(-\frac{1}{2}\right) = 9, \quad f\left(-\frac{1}{4}\right) = \frac{21}{4}, \quad f\left(-\frac{1}{8}\right) = \frac{225}{64}, \quad f(2) = 84, \quad f(-2) = 0.$$

Por lo tanto las raíces racionales de f son: -2, $\frac{1}{2}$, $\frac{1}{4}$.

(b) Determinar las raíces racionales de $f = X^4 - 15 \cdot X^2 + 10 \cdot X + 24$.

Si $\frac{p}{q}$ es una raíz de f (con p y q enteros no nulos coprimos), el criterio de Gauss nos dice que $p \mid 24$ y $q \mid 1$.

Los candidatos para p son: 1, 2, 3, 4, 6, 8, 12, 24, -1, -2, -3, -4, -6, -8, -12, -24.

Los candidatos para q son: 1, -1.

Por lo tanto, las posibles raíces racionales son:

$$1, 2, 3, 4, 6, 8, 12, 24, -1, -2, -3, -4, -6, -8, -12, -24.$$

Para confirmar o descartar las raíces especializamos f:

$$\begin{array}{rclrclrclrcl} f(1) &=& 20, & f(2) &=& 0, & f(3) &=& 0, & f(4) &=& 80, \\ f(6) &=& 840, & f(8) &=& 3240, & f(12) &=& 18720, & f(24) &=& 323400, \\ f(-1) &=& 0, & f(-2) &=& -40, & f(-3) &=& -60, & f(-4) &=& 0, \\ f(-6) &=& 720, & f(-8) &=& 3080, & f(-12) &=& 18480, & f(-24) &=& 322920. \end{array}$$

Por lo tanto las raíces racionales de f son: 2, 3, -1 y -4.

Corolario 9.2
Sea $f \in \mathbb{Z}[X]$ mónico. Entonces las raíces racionales de f son enteras.

Demostración.
Si $\frac{p}{q}$ es una raíz de f (con p y q enteros no nulos coprimos), el Teorema 9.7 nos dice que $q \mid 1$. Por lo tanto $\frac{p}{q} \in \mathbb{Z}$. Si 0 fuera una raíz, también resultaría entera. ■

A continuación veremos que las raíces complejas en polinomios con coeficientes reales vienen de a pares.

Proposición 9.11
Sean $f \in \mathbb{R}[X]$ y $z \in \mathbb{C}$. Entonces z es raíz de f si y sólo si $\overline{z}$ es raíz de f.

Demostración.
Como $f \in \mathbb{R}[X]$ entonces $f = \sum_{i=0}^{n} a_i \cdot X^i$ donde $a_i \in \mathbb{R}$ para $i = 0, \ldots, n$. Luego

$$\begin{aligned} f(z) = 0 &\Leftrightarrow \sum_{i=0}^{n} a_i \cdot z^i = 0 \\ &\Leftrightarrow \overline{\sum_{i=0}^{n} a_i \cdot z^i} = 0 \\ &\Leftrightarrow \sum_{i=0}^{n} \overline{a_i \cdot z^i} = 0 \\ &\Leftrightarrow \sum_{i=0}^{n} \overline{a_i} \cdot \overline{z^i} = 0 \\ &\Leftrightarrow \sum_{i=0}^{n} a_i \cdot \overline{z^i} = 0 \\ &\Leftrightarrow \sum_{i=0}^{n} a_i \cdot \overline{z}^i = 0 \\ &\Leftrightarrow f(\overline{z}) = 0. \end{aligned}$$

■

Teorema 9.8 (Teorema Fundamental del Álgebra)
Sea $f \in \mathbb{C}[X]$. Si $\operatorname{gr}(f) \geqslant 1$ entonces f tiene al menos una raíz en $\mathbb{C}$.

La demostración del Teorema 9.8 excede los alcances de este curso puesto que no se dispone de las herramientas necesarias para demostrarlo.

Corolario 9.3
Sea K un cuerpo ($\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$) y $f \in K[X]$ no nulo de grado $n \geqslant 1$. Entonces f tiene a lo sumo n raíces distintas en K.

Demostración.

Sean $a_1, \ldots, a_m$ las raíces distintas de f en K. Entonces, por el Teorema 9.4 se tiene que $X - a_i \mid f$ para $i = 1, \ldots m$. Como $(X - a_i, X - a_j) = 1$ para $i \neq j$ (ver Ejemplo 9.7-(c)), entonces el Teorema 9.6-(a) nos dice que:

$$(X - a_1) \cdot \ldots \cdot (X - a_m) \mid f.$$

Luego la Proposición 9.5-(h) dice que:

$$m = \operatorname{gr}((X - a_1) \cdot \ldots \cdot (X - a_m)) \leqslant \operatorname{gr}(f) = n.$$

Esto concluye la prueba. ■

El siguiente resultado caracteriza los polinomios irreducibles de $\mathbb{C}$.

Corolario 9.4
Sea $f \in \mathbb{C}[X]$. Entonces f es irreducible en $\mathbb{C}[X]$ si y sólo si $\operatorname{gr}(f) = 1$.

Demostración.

Asumamos primero que $\operatorname{gr}(f) = 1$. Por Proposición 9.6 se tiene que f es irreducible.

Asumamos ahora que f es irreducible. Por Observación 9.3 se tiene que $\operatorname{gr}(f) \geqslant 1$. Si suponemos que $\operatorname{gr}(f) > 1$, el Teorema 9.8 nos dice que al menos existe una raíz $a \in \mathbb{C}$. Ahora el Teorema 9.4 nos dice que $X - a \mid f$. Ahora:

$$\operatorname{gr}(X - a) = 1 < \operatorname{gr}(f),$$

lo cual es una contradicción en virtud de la Observación 9.3. Por lo tanto, $\operatorname{gr}(f) = 1$. ■

Corolario 9.5
Sea $f \in \mathbb{C}[X]$ tal que $\operatorname{gr}(f) \geqslant 1$. Entonces la factorización de f en $\mathbb{C}[X]$ es de la forma

$$f = c \cdot (X - a_1) \cdot \ldots \cdot (X - a_n),$$

donde $a_1, \ldots, a_n \in \mathbb{C}$ (no necesariamente distintos) y $c \in \mathbb{C}$ con $c \neq 0$.

Demostración.

Por el Teorema 9.2 existen $p_1, \ldots, p_n \in \mathbb{C}[X]$ irreducibles mónicos (no necesariamente distintos) y $c \in \mathbb{C} - \{0\}$ tal que:

$$f = c \cdot p_1 \cdot \ldots \cdot p_n.$$

Por Corolario 9.4 se tiene que $\operatorname{gr}(p_i) = 1$ y por lo tanto $p_i = X - a_i$ donde $a_i \in \mathbb{C}$, para cada $i = 1, \ldots, n$. ■

Los polinomios de grado impar con coeficientes reales siempre tienen al menos una raíz real, como lo expresa el siguiente resultado.

Corolario 9.6
Sea $f \in \mathbb{R}[X]$. Si $\operatorname{gr}(f)$ es impar, entonces f tiene al menos una raíz en $\mathbb{R}$.

Demostración.

Por Corolario 9.5 se tiene que:

$$f = c \cdot (X - a_1) \cdot \ldots \cdot (X - a_{2 \cdot s - 1}), \quad s \in \mathbb{N},$$

donde $a_1, \ldots, a_{2\cdot s-1} \in \mathbb{C}$ (no necesariamente distintos) y $c \in \mathbb{C}$ con $c \neq 0$. Notar que $a_1, \ldots, a_{2\cdot s-1}$ son las raíces de f.

Probemos el resultado por inducción en s. Si $s = 1$ entonces

$$f = c \cdot (X - a_1) = c \cdot X - c \cdot a_1,$$

Como $f \in \mathbb{R}[X]$ tenemos que $c \in \mathbb{R}$ y $c \cdot a_1 \in \mathbb{R}$, con lo que se deduce que $a_1 \in \mathbb{R}$.

Asumamos que el resultado vale para s y veamos qué ocurre para $s + 1$. Ahora:

$$f = c \cdot (X - a_1) \cdot \ldots \cdot (X - a_{2\cdot s+1}).$$

Si $a_1 \in \mathbb{R}$ listo. Si ocurre que $a_1 \notin \mathbb{R}$ sucede que $\overline{a_1}$ es raíz (ver Proposición 9.11). Además $a_1 \neq \overline{a_1}$ (ver Proposición 8.2-(e)). Notar que $X - a_1 \mid f$ y $X - \overline{a_1} \mid f$ por Teorema 9.4. Luego, debido a que $(X - a_1, X - \overline{a_1}) = 1$ por el Ejemplo 9.7-(c), tenemos que $(X - a_1) \cdot (X - \overline{a_1}) \mid f$ por Teorema 9.6-(a), es decir, $X^2 - (a_1 + \overline{a_1}) \cdot X + a_1 \cdot \overline{a_1} \mid f$. Notar que $X^2 - (a_1 + \overline{a_1}) \cdot X + a_1 \cdot \overline{a_1} \in \mathbb{R}[X]$ (ver Proposición 8.2-(d) y 8.2-(i)). Luego existe $h \in \mathbb{R}[X]$ tal que

$$f = \left[X^2 - (a_1 + \overline{a_1}) \cdot X + a_1 \cdot \overline{a_1}\right] \cdot h,$$

donde $\operatorname{gr}(h) = 2 \cdot s - 1$. Por hipótesis inductiva se tiene que h tiene al menos una raíz real, o sea, que a su vez es también raíz de f. Esto concluye la demostración. ■

El siguiente resultado nos muestra una característica de los polinomios irreducibles en relación con sus raíces.

Corolario 9.7
Sea K un cuerpo ($\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$) y $f \in K[X]$ donde $\operatorname{gr}(f) \geqslant 2$. Si f es irreducible en $K[X]$ entonces f no tiene raíces en K.

Demostración.

Supongamos que f tiene una raíz a en K. Por Teorema 9.4 se tiene que $X - a \mid f$, lo que significa que existe $h \in K[X]$ tal que $f = (X - a) \cdot h$. Luego, por la Proposición 9.3-(a) tenemos que:

$$2 \leqslant \operatorname{gr}(f) = \operatorname{gr}(X - a) + \operatorname{gr}(h) = 1 + \operatorname{gr}(h),$$

de lo que se deduce que $1 \leqslant \operatorname{gr}(h) < \operatorname{gr}(f)$. En virtud de la Observación 9.3 concluimos que f no es irreducible, lo cual es una contradicción. ■

Veamos el siguiente ejemplo para ver que no vale la recíproca del Corolario 9.7.

Ejemplo 9.10

(a) El polinomio $f = (X^2 + 1) \cdot (X^2 + 1) \in \mathbb{R}[X]$ no tiene raíces en $\mathbb{R}$ y no es irreducible en $\mathbb{R}[X]$.

Las raíces de f son $i, i, -i, -i$.

El siguiente resultado nos da una caracterización de irreducibilidad en términos de sus raíces para polinomios de grado 2 o 3.

Proposición 9.12
Sea K un cuerpo ($\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$) y $f \in K[X]$ donde $\operatorname{gr}(f)$ es igual a 2 o 3. Entonces f es irreducible en $K[X]$ si y sólo si f no tiene raíces en K.

Demostración.

Supongamos primero que f es irreducible. El Corolario 9.7 nos asegura que f no tiene raíces en K.

Asumamos ahora que f no posee raíces en K y que f no es irreducible en $K[X]$.

Supongamos primero que $\operatorname{gr}(f) = 2$. La Definición 9.5 nos dice que existe $g \in K[X]$ tal que $g \mid f$ y $0 < \operatorname{gr}(g) < \operatorname{gr}(f) = 2$. Es decir, $\operatorname{gr}(g) = 1$, o sea,

$$g = a \cdot X + b, \quad a, b \in K \text{ y } a \neq 0.$$

Pero g tiene una raíz en $-a^{-1} \cdot b \in K$. Luego $-a^{-1} \cdot b$ es también una raíz de f en K, lo cual es una contradicción.

Supongamos ahora que $\operatorname{gr}(f) = 3$. La Definición 9.5 nos dice que existe $g \in K[X]$ tal que $g \mid f$ y $0 < \operatorname{gr}(g) < \operatorname{gr}(f) = 3$. Es decir, $\operatorname{gr}(g) = 1$ o $\operatorname{gr}(g) = 2$. Como $g \mid f$ entonces existe $h \in K[X]$ tal que $f = g \cdot h$. Notar que como $f \neq 0$ tenemos que $h \neq 0$.

Si $\operatorname{gr}(g) = 1$ entonces, al igual que antes,

$$g = a \cdot X + b, \quad a, b \in K \text{ y } a \neq 0.$$

Pero $-a^{-1} \cdot b \in K$ sería una raíz de g, y por lo tanto resulta raíz de f en K, lo cual es una contradicción.

Si $\operatorname{gr}(g) = 2$ entonces $\operatorname{gr}(h) = 1$, y tendríamos que:

$$h = a \cdot X + b, \quad a, b \in K \text{ y } a \neq 0.$$

Pero $-a^{-1} \cdot b \in K$ sería una raíz de h, y por lo tanto resulta una raíz de f en K, lo cual es una contradicción. ■

El siguiente resultado nos da una caracterización de irreducibilidad para polinomios con coeficientes reales.

Corolario 9.8
Sea $f \in \mathbb{R}[X]$. Entonces f es irreducible en $\mathbb{R}[X]$ si y sólo si $\operatorname{gr}(f) = 1$, o $\operatorname{gr}(f) = 2$ y f no tiene raíces reales.

Demostración.

Asumamos primero que $\operatorname{gr}(f) = 1$ o $\operatorname{gr}(f) = 2$ y f no tiene raíces reales. Si ocurriese que $\operatorname{gr}(f) = 1$ entonces f es irreducible en $\mathbb{R}[X]$ por la Proposición 9.6. Por otro lado si $\operatorname{gr}(f) = 2$ y f no tuviese raíces reales, la Proposición 9.12 nos asegura que f es irreducible en $\mathbb{R}[X]$.

Asumamos ahora que f es irreducible en $\mathbb{R}[X]$. Por Observación 9.3 se tiene que $\operatorname{gr}(f) > 0$. Si ocurriese que $\operatorname{gr}(f) > 2$, el Corolario 9.5 nos dice

$$f = c \cdot (X - a_1) \cdot \ldots \cdot (X - a_n), \quad n \geqslant 3,$$

donde $a_1, \ldots, a_n \in \mathbb{C}$ (no necesariamente distintos) y $c \in \mathbb{R}$ (pues $f \in \mathbb{R}[X]$) con $c \neq 0$. Si $a_1 \in \mathbb{R}$ entonces $X - a_1 \mid f$ y $X - a_1 \in \mathbb{R}[X]$, lo cual es una contradicción de acuerdo a la Definición 9.5. Luego no queda otra opción que $a_1 \in \mathbb{C}$, pero esto nos dice que a_1 y $\overline{a_1}$ son raíces de f. Con un razonamiento similar a la demostración del Corolario 9.6 se tiene que $X^2 - (a_1 + \overline{a_1}) \cdot X + a_1 \cdot \overline{a_1} \mid f$. Esto es una contradicción debido a la Definición 9.5. Luego se tiene que $\operatorname{gr}(f) = 1$ o $\operatorname{gr}(f) = 2$. Si $\operatorname{gr}(f) = 1$ listo. Si $\operatorname{gr}(f) = 2$, la Proposición 9.12 nos dice que f no puede tener raíces reales. ■