Contenidos

Prefacio

El presente trabajo es fruto de varios años de experiencia, impartiendo los primeros niveles de la carrera de Enseñanza de la Matemática, en la Universidad de Costa Rica. En el año 1999, la Escuela de Matemática comenzó un proceso de reestructuración de esta carrera, con la consigna de transmitir a los nuevos estudiantes, un conocimiento más acorde con su condición de futuro docente de la enseñanza media. Se elaboaron programas, y comenzamos a editar unos apuntes informales, que han ido tomando forma a través de los años.

El trabajo nace de la necesidad de dotar al futuro docente, de una herramienta de vital importancia para su desempeño académico y profesional. Se ha preparado pensando no solo en estudiantes de Enseñanza de la Matemática, sino también en aquellos docentes ya consagrados que sientan la necesidad de refrescar un poco su memoria, o simplemente disfrutar de la lectura.

Uno de los objetivos del trabajo es enfatizar la intuición como herramienta básica en la construcción del conocimiento matemático, sin perder de vista la rigurosidad. Por ejemplo, en el primer capítulo no hemos querido ahondar mucho en la axiomática de la teoría de conjuntos, menos aún hacer un estudio minucioso de las últimas corrientes de ideas en este tema. Pero sí lo hemos concebido como un apoyo valioso para el lector interesado en aprender los fundamentos de la teoría de conjuntos, y foguearse un poco en las técnicas básicas de demostración así como en la utilización de esta teoría en la resolución de problemas de matemática elemental.

Aunque a lo largo del trabajo se hacen constantes invitaciones al lector para que verifique o demuestre ciertas afirmaciones, queremos insistir en que la idea es sentirse libre de usar la intuición y no dejarse abrumar por el rigor. En temas como los tratados aquí, un dibujo siempre ayuda a entender conceptos y a deducir resultados que, de otra manera, aparecerían como construcciones antojadizas carentes de todo significado.

Parte I

Conjuntos, Relaciones y Funciones

Capítulo 1

Un poco sobre Teoría de Conjuntos

1.1 Introducción histórica

La teoría de conjuntos como se conoce hoy en día, comienza a desarrollarse a partir de los trabajos de Georg Cantor[1] $(1845-1918)$, realizados a finales del siglo XIX. Su estudio de las series trigonométricas lo llevó a la necesidad de comparar cardinalidades de conjuntos infinitos, y a establecer así la noción de equipotencia de conjuntos. El concepto de potencia para conjuntos infinitos lo llevó a generalizar los números naturales, obteniendo así los cardinales infinitos, y a desarrollar la teoría y aritmética de números transfinitos.

Los trabajos de Cantor motivaron que otros matemáticos se involucraran en intentos por presentar la teoría de conjuntos como un sistema de principios lógicos. Quizá el esfuerzo más evidente en esta dirección, está representado por los dos volúmenes de la obra de Gottlob Frege[2], en la que indicaba cómo la matemática podía ser desarrollada a partir de una serie de principios que él consideraba principios lógicos. Pero no había aparecido aún el segundo volumen, cuando Bertrand Russell apuntó la existencia de una paradoja que se derivaba de esos principios, y que parecía destruir toda posibilidad de fundamentar la matemática en los principios de Frege.

[1] Georg Ferdinand Ludwig Phillipp Cantor, nació el 3 de marzo de 1845. Descendiente de judíos y nacido en Rusia, vivió en Alemania desde los once años, adoptando finalmente esta nacionalidad. A su traslado a Alemania, asistió a varias escuelas privadas de Francfort y Damstandt, e ingresó en el Instituto de Wiesbaden en 1860.Comenzó sus estudios universitarios en Zurich, en 1862, y al siguiente año pasó a la Universidad de Berlín, donde se especializó en Matemáticas, Filosofía y Física. Entre sus profesores de Matemática, se cuentan Kummer, Weierstrass, y Kronecker. En 1874 aparece su primer trabajo revolucionario sobre la teoría de conjuntos, en el que demuestra que no existe una biyección entre el conjunto de los números reales y el conjunto de los números naturales. A partir de 1879 publica una serie de trabajos estableciendo los conceptos generales de conjuntos abstractos y números transfinitos. Su trabajo fue bien recibido por grandes matemáticos de la época, entre ellos Richard Dedekind, no así por otros como Kronecker, quien atacó duramente su trato con los conjuntos infinitos en la misma forma como si fueran finitos. Cantor murió el 6 de enero de 1918 en Hale, Alemania. A la fecha ya su obra había sido reconocida, y le habían otorgados múltiples honores.

[2] Friedrich Ludwig Gottlob Frege, nació el 8 de noviembre de 1848, y murió el 26 de julio de 1925. Fue un matemático, lógico y filósofo alemán fundador de la moderna lógica matemática y la filosofía analítica.

La primera axiomatización de la teoría de conjuntos fue publicada por Ernst Zermelo[3] en 1908, y en 1922 Abraham Fraenkel[4] y otros propusieron un axioma más (axioma de reemplazo), que completó lo que hoy en día se conoce como la teoría de Zermelo-Fraenkel (ZF). Una axiomatización alternativa fue iniciada por John von Neumann[5] en 1925, y completada por Paul Bernays[6] a partir de 1937, y por Kurt Gödel[7] en 1940. Este enfoque se conoce como la teoría de von Neumann-Bernays, o también Gödel-Bernays.

En la actualidad podría decirse que la teoría de conjuntos ha alcanzado su madurez, aunque siguen apareciendo nuevas teorías que amplían las existentes y sugieren nuevas formas de conceptualizar ideas que han sido manejadas de una manera intuitiva por varias generaciones. En este sentido conviene mencionar la teoría axiomática del *análisis no estándar,* donde nuevos axiomas se unen a los axiomas clásicos de Zermelo-Fraenkel para dar origen a nuevos elementos de la recta real que escapan a nuestra intuición geométrica clásica.

1.1.1 Un poco de terminología

Generalmente, en una teoría matemática, los términos que denotan las nociones primarias de esa teoría no se pueden definir. Así por ejemplo, en geometría resulta difícil dar una definición de términos como "punto", "recta" y "plano". Usualmente, para estas nociones primarias, se dan algunos axiomas que sirven para "fijar las reglas del juego" en su utilización. Siguiendo con el ejemplo de la geometría, recordemos una serie de axiomas como: "dos puntos distintos determinan una recta"; "tres puntos no colineales determinan un plano"; "una recta conteniendo dos puntos comunes con un plano está enteramente contenida en ese plano"; etc. En el caso de la teoría de conjuntos sucede algo similar.

Primeramente, y de acuerdo con lo que acabamos de explicar, un conjunto es una noción primaria que no definiremos. Todos los conjuntos, salvo desde luego el conjunto vacío (denotado por $\emptyset$), están formados por elementos. Para indicar que un elemento pertenece a un conjunto, utilizamos el símbolo de pertenencia " $\in$ ". Así, si a es un elemento del conjunto A, escribimos $a \in A$, que se lee: "a pertenece a A" o "a es elemento de A". Para indicar que a no es un elemento del conjunto A, se utiliza la negación del símbolo de pertenencia " $\notin$ ". Es decir, si a no es un elemento de A, escribimos $a \notin A$.

Ejemplo 1.1.1 *Si A es el conjunto vacío, tenemos $x \notin A$ para cualquier x.*

[3] Ernst Friedrich Ferdinand Zermelo, matemático y filósofo alemán. Nació en Berlín el 27 de julio de 1871, y murió el 21 de mayo de 1953.

[4] Adolf Abraham Halevi Fraenkel, matemático alemán de origen judío, nacido en Munich el 17 de febrero de 1891, murió en Jerusalén, Israel, el 15 de octubre de 1965.

[5] John Von Neumann (Neumann János Lajos), matemático húngaro-estadounidense, de ascendencia judía,. Nació el 28 de diciembre de 1903, y murió el 8 de febrero de 1957).

[6] Paul Bernays, matemático suizo, nació el 17 de octubre de 1888, y murió el 18 de setiembre de 1977. Jugó un papel crucial en el desarrollo de la lógica matemática del siglo XX.

[7] Kurt Freidrich Gödel lógico y matemático, nació el 28 de de abril de 1906 en Brünn, Moravia (Austria-Hungría, hoy República Checa), murió el 14 de enero de 1978.

Si A y B son dos conjuntos, diremos que son iguales si tienen exactamente los mismos elementos y escribimos $A = B$. Esto, en la teoría axiomática, es conocido como el *axioma de extensión*. Como quiera que se vea, este hecho corresponde con la idea intuitiva de que los conjuntos consisten de elementos y nada más; esto es, conocer un conjunto es conocer sus elementos.

Nota: Cuando decimos que "dos conjuntos A y B son iguales", realmente queremos decir que "los símbolos A y B representan el mismo conjunto".

Ejemplo 1.1.2 *Si A es el conjunto formado por todos los números naturales menores que* 0, *entonces $A = \emptyset$.*

Si A y B son dos conjuntos, diremos que A es subconjunto de B si todo elemento de A es también elemento de B. Para indicar que A es subconjunto de B, utilizamos el símbolo de inclusión " $\subseteq$ "; escribimos $A \subseteq B$. Si $A \subseteq B$, también se dice que A está contenido en B, o que B contiene a A.

Ejemplo 1.1.3 *El conjunto de los números naturales está contenido en el conjunto de los números enteros: $\mathbb{N} \subseteq \mathbb{Z}$. Además $\mathbb{Z} \subseteq \mathbb{Q}$ y $\mathbb{Q} \subseteq \mathbb{R}$.*

Ahora, ¿qué significa que A no sea subconjunto de B?. Si A no es subconjunto de B, no se cumple la afirmación "todo elemento de A es también elemento de B", y debe existir entonces por lo menos un elemento de A que no sea elemento de B. Simbólicamente se escribe $A \nsubseteq B$.

Ejemplo 1.1.4 *Note que $\mathbb{Z} \nsubseteq \mathbb{N}$, pues existen enteros x que no son naturales. Basta con observar que $-1 \in \mathbb{Z}$ y $-1 \notin \mathbb{N}$.*

Ejemplo 1.1.5 *El conjunto vacío es subconjunto de cualquier conjunto.*
En efecto, sea A un conjunto cualquiera. Si fuera falso que $\emptyset \subseteq A$, debería existir al menos un $x \in \emptyset$ tal que $x \notin A$, y como no existe ningún $x \in \emptyset$, esto es imposible. Aquí aplicamos un argumento de demostración por contradicción.

Recordemos que los conjuntos están formados por elementos. Si queremos definir un conjunto particular, es necesario precisar los elementos que lo forman. Para esto se procede de dos maneras:

- Por enumeración de todos sus elementos (extensión).

Ejemplo 1.1.6 *El conjunto formado por las letras a, e, i, o, u.*

- Enunciando una propiedad característica de sus elementos (comprensión).

Ejemplo 1.1.7 *El conjunto de los números enteros múltiplos de 3.*

Para denotar los conjuntos utilizaremos los símbolos $\{\quad\}$, así :

- $\{a, e, i, o, u\}$ se leerá "el conjunto formado por las letras a, e, i, o, u ".
- $\{x : x$ es entero múltiplo de 3 $\}$ se leerá "el conjunto de los enteros x que son múltiplos de 3".

Ejemplo 1.1.8 $\left\{x : x \text{ es entero y } x^2 + 3x + 2 = 0\right\} = \{-1, -2\}$

Ejemplo 1.1.9 $\left\{x : x \text{ es entero y } x^2 = 2\right\} = \emptyset$

En teoría de conjuntos, la utilización de algunos símbolos facilita la escritura. Dos de esos símbolos son los llamados cuantificadores:

$\forall$: que se lee "para todo", y se denomina cuantificador universal,

$\exists$: que se lee "existe", y se denomina cuantificador existencial.

Estos nos permiten escribir de manera abreviada las definiciones dadas anteriormente.

Por ejemplo:

- $A \subseteq B$ lo escribimos : $\forall x \in A$ se tiene $x \in B$ (para todo x elemento de A se tiene que x es elemento de B). En algunos contextos se suele abreviar más, escribiendo $(\forall x \in A)\,(x \in B)$.
- $A \nsubseteq B$ lo escribimos: $\exists\ x \in A$ tal que $x \notin B$ (existe un x elemento de A que no es elemento de B). Más abreviadamente, $(\exists x \in A)\,(x \notin B)$.

La relación de inclusión, nos permite dar una definición alternativa de igualdad entre conjuntos. Recordemos que $A = B$ si tienen exactamente los mismos elementos, lo que es equivalente a decir que $A \subseteq B$ y $B \subseteq A$. Claramente, para que A sea distinto de B ($A \neq B$), debe ocurrir que $A \nsubseteq B$ o $B \nsubseteq A$. Dicho de otro modo, $A \neq B$ si ocurre alguno de los siguientes casos:

1. existe al menos un elemento $a \in A$ tal que $a \notin B$, o
2. existe al menos un elemento $b \in B$ tal que $b \notin A$.

1.1.2 Sobre las negaciones de los cuantificadores

En general, si $p(x)$ representa cierta afirmación sobre el elemento x, podemos formar nuevas afirmaciones

$(\forall x \in A)\, p(x)$ "para todo x en A se cumple $p(x)$"

$(\exists x \in A)\, p(x)$ "existe x en A tal que se cumple $p(x)$"

Por ejemplo, si $p(x)$ es la proposición $x^2+1=0$, y si $A=\mathbb{R}$, entonces podemos formar la nueva proposición

$$(\exists x \in \mathbb{R})\left(x^2+1=0\right),$$

la cual es falsa. Su negación está dada por:

$$(\forall x \in \mathbb{R})\left(x^2+1\neq 0\right),$$

la cual es verdadera. En general, la negación de $(\forall x \in A)\, p(x)$ está dada por

$$(\exists x \in A)\left(\neg p(x)\right),$$

donde $\neg p(x)$ es la negación de $p(x)$. La negación de $(\exists x \in A)\, p(x)$ está dada por

$$(\forall x \in A)\left(\neg p(x)\right).$$

En matemática, a veces se utiliza un conjunto de referencia E (que contiene a todos los conjuntos con los que se está trabajando). Se entiende entonces que todo elemento en el contexto pertenece a E, así que no es necesario escribir "$x \in E$". Por ejemplo, la proposición: $(\forall x \in E)\ \ p(x)$ se escribiría abreviadamente como: $(\forall x) p(x)$.
Bajo esa convención, la definición de subconjunto se puede reescribir así:

$$A \subseteq B \Leftrightarrow (\forall x \in A)\,(x \in B),$$

o también:

$$A \subseteq B \Leftrightarrow (\forall x)\,(x \in A \Rightarrow x \in B).$$

La igualdad estaría dada por:

$$A = B \Leftrightarrow (\forall x)\,(x \in A \Leftrightarrow x \in B).$$

Finalmente, utilizaremos la notación

$$\{x \in E : p\,(x)\}$$

para denotar al conjunto de elementos de E que satisfacen la propiedad $p\,(x)$. Si no hay ambigüedad, se escribe simplemente $\{x : p\,(x)\}$.

1.1.3 Algunas reglas importantes

Dado un elemento a y un conjunto E, entre las dos relaciones $a \in E$ y $a \notin E$, una y solo una es verdadera. Aquí se aplica el **"principio del tercero excluido"**. El **"principio de no contradicción"** permite concluir que las dos proposiciones no son ciertas simultáneamente. Finalmente, decimos que un conjunto E está bien definido si para todo elemento a siempre es posible decidir si pertenece o no al conjunto E.

Por mucho tiempo se acostumbró definir un conjunto con solo dar cierta condición sobre sus elementos. Sin embargo, al aparecer ciertas paradojas de la teoría de conjuntos, debió pensarse en una teoría axiomática que evitara ese tipo de situaciones. Por ejemplo:

- No podemos hablar del conjunto de todos los conjuntos.
- Un conjunto no puede ser considerado como elemento de sí mismo.

Supongamos, por ejemplo, que podemos hablar del conjunto de todos los conjuntos, al cual denotamos por X. Tenemos entonces dos categorías de conjuntos: los que son elementos de sí mismos y los que no lo son. Sea F el conjunto de todos los conjuntos de la segunda categoría, es decir

$$F = \{A \in X : A \notin A\}.$$

La pregunta siguiente es: ¿En cuál categoría podemos ubicar al conjunto F ?.
Si $F \in F$ entonces, puesto que los elementos de F son los conjuntos que no son elementos de sí mismos, tenemos $F \notin F$. Obtenemos una contradicción, y por lo tanto es falso que $F \in F$. Pero entonces $F \notin F$, y por definición de F se sigue que $F \in F$, llegando nuevamente a una contradicción. Esto demuestra que X no puede ser considerado como conjunto.

1.1.4 Ejemplos de inclusión e igualdad de conjuntos

Ejemplo 1.1.10 *Considere los conjuntos*

$$A = \{x \in \mathbb{Z} : x \text{ es par y } 0 < x < 15\}, \quad B = \{2, 4, 6, 8, 10, 12, 14\}.$$

Entonces $A = B$.

Ejemplo 1.1.11 *Considere los conjuntos* $A = \{x \in \mathbb{Z} : x \text{ es múltiplo de } 3\}$, *y* $B = \{9, 12, 27\}$. *Entonces tenemos* $B \subseteq A$, *pero* $A \nsubseteq B$, *dado que por ejemplo* $6 \in A$ *y* $6 \notin B$. *Consecuentemente se tiene también* $A \neq B$.

Ejemplo 1.1.12 *Sean* $A = \{1, 2, 3, 4, 6\}$ *y* $B = \{3, 5, 6, 10, 12\}$. *Entonces* $A \nsubseteq B$, *pues* $4 \in A$ *y* $4 \notin B$. *Por otro lado,* $B \nsubseteq A$ *pues* $12 \in B$ *y* $12 \notin A$.

Ejemplo 1.1.13 *Sea* $A = \{n \in \mathbb{N} : n \text{ es impar}\}$, *y sea* $B = \{n \in \mathbb{N} : n \text{ es primo}\}$. *Entonces se tiene* $A \neq B$, *pues por ejemplo* $9 \in A$, *pero* $9 \notin B$. *En particular no se tiene* $A \subseteq B$ *(esto es* $A \nsubseteq B$*). Tampoco se tiene* $B \subseteq A$, *pues* $2 \in B$ *y* $2 \notin A$.

Ejemplo 1.1.14 *Sea* $A = \left\{n \in \mathbb{N} : 3 < n^2 < 30\right\}$ *y sea* $B = \{2, 3, 4, 5\}$. *Entonces* $A = B$. *Para ver esto tenemos que demostrar que* $A \subseteq B$ *y* $B \subseteq A$. *Para demostrar que* $B \subseteq A$ *nada más hay que observar que el cuadrado de cada elemento de* B *es un número natural entre* 3 *y* 30, *lo cual es evidente. Para ver que* $A \subseteq B$, *tomemos un elemento* n *de* A. *Entonces debe tenerse* $2 \leq n \leq 5$, *y como* $n \in \mathbb{N}$ *se concluye que* $n \in B$.

1.1.5 Propiedades de la inclusión y la igualdad de conjuntos

Es bastante evidente que la igualdad de conjuntos satisface las siguientes propiedades:

- Reflexividad: Para todo conjunto A se tiene $A = A$
- Simetría: Si $A = B$ entonces $B = A$
- Transitividad: Si $A = B$ y $B = C$, se sigue que $A = C$.

En efecto, estos son axiomas lógicos de igualdad, válidos en cualquier contexto de matemática clásica. En el capítulo siguiente estudiaremos las relaciones de equivalencia, que son simplemente una abstracción del concepto de igualdad, en el sentido que satisfacen estas tres propiedades.

La inclusión satisface las siguientes propiedades:

- Reflexividad: Para todo conjunto A se tiene $A \subseteq A$.
- Antisimetría: Si $A \subseteq B$ y $B \subseteq A$ entonces $A = B$.
- Transitividad: Si $A \subseteq B$ y $B \subseteq C$, se sigue que $A \subseteq C$.

Las relaciones que cumplen estas propiedades se llaman *relaciones de orden,* de acuerdo con lo que estudiaremos en el capítulo siguiente.

Ejemplo 1.1.15 *El conjunto $A = \{n \in \mathbb{N} : n \text{ es par}\}$ es subconjunto de $\mathbb{Z}$. En efecto, dado que $A \subseteq \mathbb{N}$ y $\mathbb{N} \subseteq \mathbb{Z}$, el resultado se obtiene de la transitividad.*

1.2 Conjunto potencia

Antes de dar una definición formal del conjunto potencia o conjunto de partes de un conjunto, veamos un ejemplo.

Ejemplo 1.2.1 *Si $E = \{a, b, c\}$, los subconjuntos de E son los conjuntos: E, $\emptyset$, $\{a\}$, $\{b\}$, $\{c\}$, $\{a, b\}$, $\{a, c\}$, $\{b, c\}$. Al conjunto*

$$\mathcal{P}(E) = \{E, \emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}\}$$

se le llama el conjunto potencia de E o el conjunto de partes de E.

Definición 1.2.1 *Dado E un conjunto cualquiera, el conjunto de todos los subconjuntos de E se llama Conjunto Potencia de E, o Conjunto de Partes de E, y se denota por $\mathcal{P}(E)$. Simbólicamente se tiene*

$$\mathcal{P}(E) = \{X : X \subseteq E\}.$$

De acuerdo con la definición de inclusión, E es subconjunto de sí mismo para cualquier conjunto E. Por lo tanto $E \in \mathcal{P}(E)$, e igualmente $\emptyset \in \mathcal{P}(E)$. Como consecuencia se tiene $\mathcal{P}(E) \neq \emptyset$.

Ejemplo 1.2.2 *Si* $E = \emptyset$, *se tiene que* $\mathcal{P}(E) = \{\emptyset\}$. *Tenga presente que* $\emptyset \neq \{\emptyset\}$.

Ejemplo 1.2.3 *Sea* $E = \{x \in \mathbb{Z} : x \text{ es múltiplo de } 3 \text{ y } 9 \leq x < 18\} = \{9, 12, 15\}$. *Entonces*

$$\mathcal{P}(E) = \{\emptyset, \{9, 12, 15\}, \{9\}, \{12\}, \{15\}, \{9, 12\}, \{9, 15\}, \{12, 15\}\}.$$

Ejemplo 1.2.4 *Si* $E = \{3, 4\}$, *entonces* $\mathcal{P}(E) = \{\emptyset, \{3, 4\}, \{3\}, \{4\}\}$.

Observe que para el caso $E = \emptyset$ se tiene $\mathcal{P}(E) = \{\emptyset\}$. En este caso E tiene cero elementos y $\mathcal{P}(E)$ tiene un elemento (o sea 2^0 elementos). Para el caso $E = \{3, 4\}$, E consta de dos elementos y $\mathcal{P}(E) = \{\emptyset, \{3, 4\}, \{3\}, \{4\}\}$ consta de cuatro elementos (2^2 elementos). Finalmente, el conjunto $E = \{9, 12, 15\}$ está formado por tres elementos, mientras que $\mathcal{P}(E)$ está formado por ocho elementos (2^3 elementos).
De manera general, se puede demostrar usando un argumento inductivo que: si E es un conjunto formado por n elementos, entonces el conjunto $\mathcal{P}(E)$ está formado por 2^n elementos. Esto se puede intuir del hecho que, para $A \subseteq E$, cada elemento de E tiene dos posibilidades: pertenecer a A o no pertenecer a A. Como E tiene n elementos, en total hay $2 \cdot 2 \cdot \cdots \cdot 2 = 2^n$ posibilidades de escoger el conjunto A.

1.2.1 Algunas cosas que conviene tener presentes

- Si A es un elemento de $\mathcal{P}(E)$ y si $B \subseteq A$, entonces B también es un elemento de $\mathcal{P}(E)$. En efecto, note que $A \in \mathcal{P}(E)$ significa que $A \subseteq E$. Así, se tiene que $B \subseteq A$ y $A \subseteq E$, y consecuentemente $B \subseteq E$. Es decir, $B \in \mathcal{P}(E)$.

- Para cualquier conjunto E se tiene: $\mathcal{P}(E) \neq \emptyset$ y $\mathcal{P}(E) \neq E$. En efecto, $E \subseteq E$ y por lo tanto $E \in \mathcal{P}(E)$ con lo cual resulta que $\mathcal{P}(E) \neq \emptyset$. Además, del hecho que $E \notin E$ y $E \in \mathcal{P}(E)$, resulta $E \neq \mathcal{P}(E)$.

- El conjunto $\mathcal{P}(E)$ está formado por elementos que son a su vez conjuntos: todos los subconjuntos de E.

1.2.2 Unas palabras sobre los símbolos " $\Rightarrow$ " y " $\Leftrightarrow$ "

El símbolo " $\Rightarrow$ " se lee "implica" y se utiliza para sustituir la frase: "si... entonces...". Por ejemplo, en lugar de: "Si $E = \emptyset$ entonces $\mathcal{P}(E) = \{\emptyset\}$ ", podemos escribir:

$$E = \emptyset \Rightarrow \mathcal{P}(E) = \{\emptyset\}.$$

Para escribir: "si $A \subseteq B$ entonces $\mathcal{P}(A) \subseteq \mathcal{P}(B)$ ", podemos hacerlo así:

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

En algunos casos, se puede demostrar que un cierto "implica" es válido y que también es válida la otra dirección. Por ejemplo, se puede probar que si $A \subseteq B$ entonces $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, pero también se puede demostrar que si $\mathcal{P}(A) \subseteq \mathcal{P}(B)$ entonces $A \subseteq B$. En este caso se escribe

$$A \subseteq B \Leftrightarrow \mathcal{P}(A) \subseteq \mathcal{P}(B),$$

y decimos que las proposiciones "$A \subseteq B$" y "$\mathcal{P}(A) \subseteq \mathcal{P}(B)$ " son equivalentes.

El símbolo " $\Leftrightarrow$ " se lee "si y solo si", y a veces se abrevia "sii".

Seguidamente, vamos a considerar un conjunto de referencia E, y sobre $\mathcal{P}(E)$ definiremos una serie de operaciones.

1.3 Intersección de conjuntos

Dados dos conjuntos A y B, se llama "intersección de A y B" al conjunto formado por los elementos que pertenecen simultáneamente al conjunto A y al conjunto B. Tal conjunto se denota por $A \cap B$. Simbólicamente

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

Note que si los conjuntos A y B son elementos de $\mathcal{P}(E)$, la intersección nos permite crear un tercer conjunto que también pertenece a $\mathcal{P}(E)$.

Ejemplo 1.3.1 *Sea E el conjunto de los números naturales, y considere los conjuntos:*

$$\begin{aligned} A &= \{x \in E : x \text{ es divisor de } 18\} \\ B &= \{x \in E : x \text{ es divisor de } 45\} \end{aligned}$$

Por extensión tenemos:

$$A = \{1, 2, 3, 6, 9, 18\}, \quad B = \{1, 3, 5, 9, 15, 45\}.$$

Luego $A \cap B = \{1, 3, 9\}$. Observe que los elementos de $A \cap B$ resultan ser los divisores comunes de 18 y 45.

Ejemplo 1.3.2 *Sea E el conjunto de los naturales, y sean*

$$\begin{aligned} A &= \{x \in E : x \text{ es múltiplo de } 4\} \\ B &= \{x \in E : x \text{ es impar}\} \end{aligned}$$

Note que $A = \{4, 8, 12, 16, 20, ...\}$ y $B = \{1, 3, 5, 7, 9, 11, ...\}$. Entones $A \cap B = \emptyset$. En casos como este se dice que A y B son disjuntos.

1.3.1 Propiedades básicas de la intersección

1. Para todo par de conjuntos A y B en $\mathcal{P}(E)$ se cumple:

$$A \cap B \subseteq A, \qquad A \cap B \subseteq B, \qquad A \cap B \in \mathcal{P}(E).$$

   En efecto, $A \cap B \subseteq A$ puesto que todo elemento común de A y B es elemento de A. De manera análoga $A \cap B \subseteq B$. Por otro lado, como $A \in \mathcal{P}(E)$ tenemos $A \subseteq E$, y como $A \cap B \subseteq A$, se concluye que $A \cap B \subseteq E$, esto es $A \cap B \in \mathcal{P}(E)$.

2. La intersección de conjuntos es conmutativa: $A \cap B = B \cap A$.

3. La intersección es asociativa: $(A \cap B) \cap C = A \cap (B \cap C)$.

4. Para todo $A \in \mathcal{P}(E)$, se cumple $A \cap A = A$.

5. Para todo $D \in \mathcal{P}(E)$ se tiene

$$D \subseteq A \text{ y } D \subseteq B \Leftrightarrow D \subseteq A \cap B.$$

Se invita al lector a convencerse de estos resultados, y a intentar una demostración de cada uno de ellos.

1.3.2 Sobre el uso de diagramas o pinturas

A veces es conveniente utilizar diagramas para darse una idea geométrica de lo que significa una operación entre conjuntos, o cierta identidad. En dichos diagramas los conjuntos se pintan como "regiones" o figuras geométricas en un plano, por lo que debe tenerse cuidado y recordar que estas pinturas son una creación didáctica, y no sustituyen en absoluto el concepto. La representación gráfica de la intersección, se presenta a manera de ejemplo en la figura 1.1.

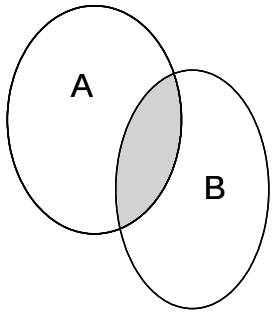


Figura 1.1: La parte sombreada representa $A \cap B$.

Debe insistirse en que la forma que tengan las figuras, o la ubicación que les demos con respecto a las otras, en general no tienen nada que ver con los conjuntos en sí.

Una buena práctica para el lector es convencerse de las propiedades enunciadas arriba, mediante el uso de diagramas.

1.4 Unión de conjuntos

Dados dos conjuntos A y B, se llama "unión de A y B" al conjunto formado por los elementos que pertenecen al menos a uno de ellos. Lo denotamos por $A \cup B$. Simbólicamente:

$$A \cup B = \{x : x \in A \text{ o } x \in B\}$$

La unión de conjuntos se representa gráficamente en la figura 1.2.

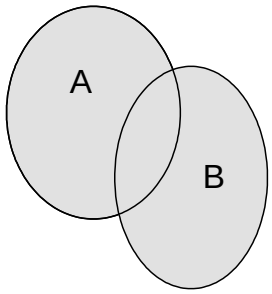


Figura 1.2: La parte sombreada representa $A \cup B$.

Ejemplo 1.4.1 *Sea* $E = \mathbb{N}$*, y sean*

$$\begin{aligned} A &= \{x \in E : x \text{ es divisor de } 20\} \\ B &= \{x \in E : x \text{ es divisor de } 16\}. \end{aligned}$$

Tenemos $A = \{1, 2, 4, 5, 10, 20\}$ *y* $B = \{1, 2, 4, 8, 16\}$*. Luego*

$$A \cup B = \{1, 2, 4, 5, 8, 10, 16, 20\}.$$

1.4.1 Propiedades básicas de la unión

1. Para cualesquiera dos conjuntos A y B en $\mathcal{P}(E)$ se tiene:

$$A \subseteq A \cup B, \quad B \subseteq A \cup B, \quad A \cup B \in \mathcal{P}(E)$$

2. La unión de conjuntos es una operación conmutativa: $A \cup B = B \cup A$.

3. La unión de conjuntos es una operación asociativa: $(A \cup B) \cup C = A \cup (B \cup C)$.

4. Para todo conjunto A, se cumple $A \cup A = A$.

5. Para todo $D \in \mathcal{P}(E)$ se tiene:

$$(A \subseteq D \text{ y } B \subseteq D) \Leftrightarrow A \cup B \subseteq D.$$

Las primeras cuatro propiedades se dejan como ejercicio. Para demostrar la propiedad **5,** primero suponemos que $A \subseteq D$ y $B \subseteq D$; entonces dado $x \in A \cup B$ se tiene $x \in A$ o $x \in B$, y como ambos son subconjuntos de D, se concluye que $x \in D$. Recíprocamente, suponga que $A \cup B \subseteq D$; entonces como $A \subseteq A \cup B$ (por la propiedad 1) se sigue de la transitividad que $A \subseteq D$, y similarmente $B \subseteq D$. $\square$

1.4.2 La doble distributividad de las operaciones booleanas

1. La unión es distributiva con respecto a la intersección

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

2. La intersección distribuye con respecto a la unión

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

La primera de estas identidades se puede visualizar geométricamente en las pinturas de la figura 1.3. En la primera se sombreó $A \cup (B \cap C)$, en la segunda se sombreó $A \cup B$ y en la tercera $A \cup C$. La identidad dice que la parte sombreada de la primera pintura, es la intersección de las partes sombreadas en las otras dos.

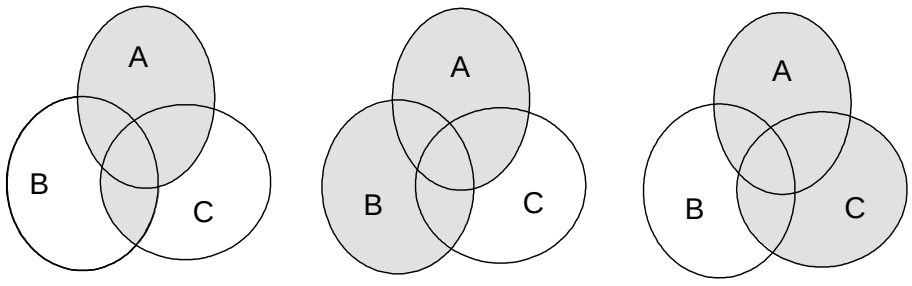


Figura 1.3: Distributividad de la unión con respecto a la intersección.

En los ejercicios se le pide al lector demostrar estas dos propiedades.

1.5 Complemento y diferencia de conjuntos

Dados dos conjuntos A y B, la diferencia $B - A$ se define como el conjunto formado por los elementos de B que no están en A. Más precisamente se tiene

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

Note que aquí no se asume ninguna relación entre A y B. En caso que A sea subconjunto de un conjunto E, al conjunto $E - A$ también se le llama *complemento de A con respecto a E*, y se denota $\complement_E A$. Así, se tiene que

$$\complement_E A = E - A = \{x \in E : x \notin A\}.$$

Es muy importante tener presente que $\complement_E A$ es un subconjunto de E $\left(\complement_E A \in \mathcal{P}(E)\right)$, y que el conjunto de referencia E es fundamental pues $\complement_E A$ varía cada vez que varía E. Cuando en el contexto no hay ambigüedad sobre quién es E, se suele escribir simplemente $\complement A$, y también se denota $A^c = \complement A = \complement_E A$. La diferencia de conjuntos se representa gráficamente en la figura 1.4.

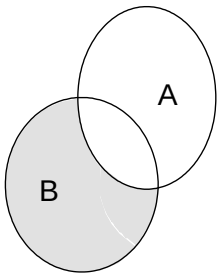


Figura 1.4: La parte sombreada representa $B - A$.

El complemento de A en E se puede representar como se muestra en la figura 1.5.

Ejemplo 1.5.1 *Si $A = [-5, \pi]$ y $B = \{1, 2, 3, 4, 5\}$, tenemos $B - A = \{4, 5\}$.*

Ejemplo 1.5.2 *Sea $E = \mathbb{R}$ y sea $A = \{x \in \mathbb{R} : x < 2\}$. Entonces*

$$\complement_E A = \{x \in \mathbb{R} : x \geq 2\}.$$

Ejemplo 1.5.3 *Sean $A = [1, 4]$ y $B = [3, 6]$. Entonces $A \cup B = [1, 6]$, $A \cap B = [3, 4]$, y $A - B = [1, 3[$.*

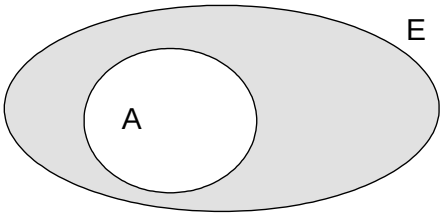


Figura 1.5: La parte sombreada representa $\complement_E A$.

1.5.1 Algunas propiedades del complemento

1. Si $A \subseteq E$, entonces $\complement_E A = E \Leftrightarrow A = \emptyset$.

   Demostración

   Recordemos que para demostrar una doble implicación o equivalencia, se debe demostrar la veracidad del "implica" en las dos direcciones.

   " $\Leftarrow$ " Supongamos que $A = \emptyset$ y probemos que $\complement_E A = E$. Por la definición, sabemos que $\complement_E \emptyset \subseteq E$ y bastaría entonces con demostrar que $E \subseteq \complement_E \emptyset$. Dado $x \in E$, como $x \notin \emptyset$ tenemos $x \in \complement_E \emptyset$. Esto demuestra el resultado.

   " $\Rightarrow$ " Supongamos que $\complement_E A = E$, debemos demostrar que $A = \emptyset$. Supongamos que $A \neq \emptyset$, entonces debe existir al menos un $x \in A$. Pero como $A \subseteq E$, se tiene $x \in E = \complement_E A$, lo que implica $x \notin A$. Como esto es contradictorio, se sigue que $A = \emptyset$. $\square$

2. Consideremos $A \subseteq E$. De acuerdo con la definición de complemento, hemos visto que $\complement_E A \subseteq E$ y por lo tanto tiene sentido hablar de $\complement_E \left(\complement_E A\right)$. Mostraremos que:

   $$\complement_E \left(\complement_E A\right) = A.$$

   Esta es conocida como la ley de involución. Para demostrarla basta con observar que, para todo $x \in E$, se tienen las equivalencias siguientes:

   $$x \in \complement_E \left(\complement_E A\right) \Leftrightarrow x \notin \complement_E A \Leftrightarrow x \in A.$$

   Se invita al lector a escribir esto con más detalle.

3. Sea $A \subseteq E$. Entonces $\complement_E A = \emptyset \Leftrightarrow A = E$.

   Demostración

   Por la propiedad **1** tenemos

   $$\complement_E A = \emptyset \Leftrightarrow \complement_E \left(\complement_E A\right) = E,$$

   y por la propiedad 2, $A = \complement_E \left(\complement_E A\right)$. Entonces $\complement_E A = \emptyset \Leftrightarrow A = E$

4. Si A y B son subconjuntos de E entonces

$$A \subseteq B \Leftrightarrow \complement_E B \subseteq \complement_E A$$

¡Haga la demostración!

5. Si A y B son subconjuntos de E se tiene

$$A - B = A \cap \complement_E B. \tag{1.1}$$

¡Haga la demostración!

1.5.2 Leyes de De Morgan

Si A y B son subconjuntos de E, entonces

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

Estas dos propiedades se conocen como las leyes De Morgan. Vamos a demostrar la primera propiedad, y para esto tomamos $x \in \complement_E(A \cup B)$. Por definición de complemento se tiene que $x \in E$ y $x \notin A \cup B$, lo cual garantiza que $x \notin A$ y $x \notin B$. Esto demuestra que $x \in \complement_E A \cap \complement_E B$, y luego $\complement_E(A \cup B) \subseteq \complement_E A \cap \complement_E B$.

Por otro lado, si $x \in \complement_E A \cap \complement_E B$ tenemos $x \in E$ y $(x \notin A$ y $x \notin B)$, y por lo tanto $x \in E$ y $x \notin A \cup B$, con lo cual $x \in \complement_E(A \cup B)$. Esto demuestra la otra inclusión, y por lo tanto la igualdad.
La demostración de la segunda ley de De Morgan, se deja como ejercicio. □

Nota: Las fórmulas de De Morgan, de manera abreviada, se enuncian como sigue:

El complemento de la unión es la intersección de los complementos,
y el complemento de la intersección, es la unión de los complementos.

En caso que A y B no estén contenidos en E, las leyes de De Morgan toman la siguiente forma:

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

La demostración es idéntica al caso de complementos.

En algunos casos, las leyes de De Morgan y la ley de involución $\left(\complement_E\left(\complement_E A\right) = A\right)$, permiten hallar fácilmente el complemento de una expresión en la que figuren uniones e intersecciones. Consideremos el siguiente ejemplo.

Ejemplo 1.5.4 *Hallar el complemento (en E) de* $\left(\left(\complement_E A\right) \cup B\right) \cap \left(C \cup \complement_E D\right)$.
Por las fórmulas De Morgan y la ley de involución se tiene:

$$\begin{aligned}
\complement_E \left\{\left(\left(\complement_E A\right) \cup B\right) \cap \left(C \cup \complement_E D\right)\right\} &= \left[\complement_E \left(\left(\complement_E A\right) \cup B\right)\right] \cup \left[\complement_E \left(C \cup \complement_E D\right)\right] \\
&= \left[\complement_E \left(\complement_E A\right) \cap \complement_E B\right] \cup \left[\left(\complement_E C\right) \cap \complement_E \left(\complement_E D\right)\right] \\
&= \left(A \cap \complement_E B\right) \cup \left(\left(\complement_E C\right) \cap D\right) \\
&= (A - B) \cup (D - C) .
\end{aligned}$$

1.6 La diferencia simétrica

Definición 1.6.1 *Dados los conjuntos A y B, se llama diferencia simétrica de A y B al conjunto* $(A - B) \cup (B - A)$.

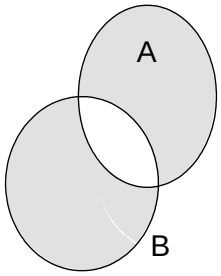


Figura 1.6: La parte sombreada representa $A\Delta B$.

La diferencia simétrica de A y B es entonces el conjunto de puntos que pertenecen a uno, y solo uno, de estos conjuntos. Se denota por $A\triangle B$, esto es

$$A\Delta B = (A - B) \cup (B - A) .$$

En algunas ocasiones, es muy útil expresar la diferencia simétrica en términos de las operaciones de unión, intersección y complemento.

Teorema 1.1 *Sean $A, B \in \mathcal{P}(E)$. Entonces*

$$\begin{aligned}
\textbf{\textit{(a)}} \qquad A\triangle B &= \left(A \cap \complement_E B\right) \cup \left(B \cap \complement_E A\right) \\
\textbf{\textit{(b)}} \qquad A\triangle B &= (A \cup B) - (A \cap B)
\end{aligned}$$

Demostración
La parte (a) es una consecuencia inmediata de las definiciones, y de la la propiedad (1.1). Demostremos la parte (b):

Por las leyes de De Morgan y de distributividad se tiene

$$\begin{aligned}(A \cup B) - (A \cap B) &= (A \cup B) \cap (A \cap B)^c \\ &= (A \cup B) \cap (A^c \cup B^c) \\ &= (A \cap A^c) \cup (A \cap B^c) \cup (B \cap A^c) \cup (B \cap B^c) \\ &= \emptyset \cup (A - B) \cup (B - A) \cup \emptyset \\ &= A \triangle B. \ \square\end{aligned}$$

1.6.1 Algunos ejemplos

Ejemplo 1.6.1 $\{1,2,3,4\} \triangle \{2,5,4,7\} = \{1,3,5,7\}$

Ejemplo 1.6.2 *Sea P el conjunto de los números naturales pares, y Q el conjunto de los primos. Entonces*

$$\begin{aligned}P \triangle Q &= (P \cup Q) - (P \cap Q) \\ &= \{x \in \mathbb{N} : x \text{ es par o primo}\} - \{2\}.\end{aligned}$$

Ejemplo 1.6.3 *Sea $A = [1,4]$ y $B = [3,6]$. Entonces $A \triangle B = [1,3[\cup]4,6]$.*

1.6.2 Algunas propiedades de la diferencia simétrica

Teorema 1.2 *Sean $A, B, C \in \mathcal{P}(E)$, entonces*

(a) $A \triangle \emptyset = A$

(b) $A \triangle A = \emptyset$

(c) $A \triangle B = B \triangle A$ *(propiedad conmutativa)*

(d) $(A \triangle B) \triangle C = A \triangle (B \triangle C)$ *(propiedad asociativa)*

(e) $(A \triangle B) \cap C = (A \cap C) \triangle (B \cap C)$ *(propiedad distributiva de la intersección con respecto a la diferencia simétrica).*

Demostración
Probaremos la parte **(d)**, la cual requiere de más cuidado. El resto se deja de ejercicio.
Primero observemos que, por el teorema 1.1,

$$(A \triangle B) \triangle C = [(A \triangle B) - C] \cup [C - (A \triangle B)].$$

Desarrollemos la primera parte del lado derecho:

$$\begin{aligned}(A\triangle B) - C &= \left[\left(A \cap \complement_E B\right) \cup \left(B \cap \complement_E A\right)\right] \cap \complement_E C \\ &= \left[\left(A \cap \complement_E B\right) \cap \complement_E C\right] \cup \left[\left(B \cap \complement_E A\right) \cap \complement_E C\right] \\ &= \left(A \cap \complement_E \left(B \cup C\right)\right) \cup \left(B \cap \complement_E \left(A \cup C\right)\right) \\ &= \left[A - (B \cup C)\right] \cup \left[B - (A \cup C)\right].\end{aligned}$$

Para la segunda parte observemos que

$$\begin{aligned}C - (A\triangle B) &= C \cap \complement_E \left(\left[A \cup B\right] \cap \complement_E \left[A \cap B\right]\right) \\ &= C \cap \left[\complement_E \left(A \cup B\right) \cup \left(A \cap B\right)\right] \\ &= \left[C \cap \complement_E \left(A \cup B\right)\right] \cup \left[C \cap \left(A \cap B\right)\right] \\ &= \left[C - (A \cup B)\right] \cup (A \cap B \cap C)\end{aligned}$$

Pegando las dos partes calculadas obtenemos

$$\begin{aligned}(A\triangle B)\triangle C &= \left[A - (B \cup C)\right] \cup \left[B - (A \cup C)\right] \\ &\qquad \cup \left[C - (A \cup B)\right] \cup \left[A \cap B \cap C\right].\end{aligned}$$

Ahora observemos que la expresión del lado derecho es simétrica en A, B y C, lo que significa que

$$(A\triangle B)\triangle C = (B\triangle C)\triangle A,$$

y finalmente, por la conmutatividad obtenemos

$$\begin{aligned}(A\triangle B)\triangle C &= (B\triangle C)\triangle A \\ &= A\triangle \left(B\triangle C\right). \ \square\end{aligned}$$

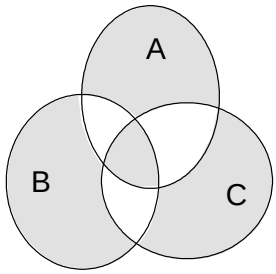


Figura 1.7: Representación gráfica de la asociatividad.

1.7 Producto cartesiano de conjuntos

Para formar el producto cartesiano de un conjunto A con un conjunto B, el cual denotamos por $A \times B$, se deben considerar los pares ordenados de elementos de A con elementos de B.

1.7.1 Unas palabras sobre los pares ordenados

Usualmente cuando hablamos de pareja ordenada o par ordenado, decimos que se toma un $x \in A$ y un $y \in B$, y que (x, y) es un par ordenado. Sin embargo, no se precisa qué significa *par ordenado*. Debemos indicar que en una definición de par ordenado, es fundamental poder distinguir entre el primer y el segundo elemento, y además poder precisar si dos parejas dadas son iguales.

Una manea de lograr esto es mediante la definición

$$(x, y) = \{\{x\}, \{x, y\}\}.$$

Vamos a verificar que, efectivamente, esta definición nos proporciona los elementos deseados. Veamos primero que esta definición nos permite distinguir entre el x y el y. En efecto, si $x \neq y$ tenemos $\{x\} \neq \{y\} \neq \{x, y\}$, así que

$$(x, y) = \{\{x\}, \{x, y\}\} \neq \{\{y\}, \{x, y\}\} = (y, x).$$

Veamos ahora que

$$(x, y) = (z, w) \Leftrightarrow x = z \text{ y } y = w.$$

"$\Leftarrow$" Observe que si $x = z$ y $y = w$, entonces

$$(x, y) = \{\{x\}, \{x, y\}\} = \{\{z\}, \{z, w\}\} = (z, w).$$

"$\Rightarrow$" Supongamos que $(x, y) = (z, w)$, y probemos que $x = z$ y $y = w$. La hipótesis nos dice que

$$\{\{x\}, \{x, y\}\} = \{\{z\}, \{z, w\}\}.$$

Tenemos entonces que $\{x\} \in \{\{z\}, \{z, w\}\}$, y por lo tanto hay dos posibilidades:

- Si $\{x\} = \{z\}$ entonces $x = z$.
- Si $\{x\} = \{z, w\}$ se sigue que $x = z = w$.

En ambos casos concluimos que $x = z$. Consecuentemente $\{x, y\} = \{z, w\}$, de donde se sigue que $y = w$. $\square$

1.7.2 Definición del producto cartesiano

Definición 1.7.1 *Sean A y B dos conjuntos. Se define el producto cartesiano de A y B por*

$$A \times B = \{(x, y) : x \in A,\ y \in B\}.$$

Ejemplo 1.7.1 *Sean $A = \{1\}$ y $B = \{3\}$. Entonces $A \times B = \{(1, 3)\}$, y $B \times A = \{(3, 1)\}$. Esto muestra que en general $A \times B \neq B \times A$.*

Ejemplo 1.7.2 *Sea $A = \{1, 2\}$ y $B = \{3, 4\}$. Entonces*

$$\begin{aligned} A \times B &= \{(1,3), (1,4), (2,3), (2,4)\}, \\ B \times A &= \{(3,1), (3,2), (4,1), (4,2)\}. \end{aligned}$$

Ejemplo 1.7.3 *Considere los intervalos*

$$\begin{aligned} A &= \{x \in \mathbb{R} : a \leq x \leq b\} = [a, b], \\ B &= \{y \in \mathbb{R} : c \leq y \leq d\} = [c, d], \end{aligned}$$

donde $a, b, c, d \in \mathbb{R}$ son tales que $a < b$ y $c < d$. Entonces

$$A \times B = \left\{(x, y) \in \mathbb{R}^2 : x \in [a, b]\ \text{y}\ y \in [c, d]\right\}$$

es un rectángulo con borde.

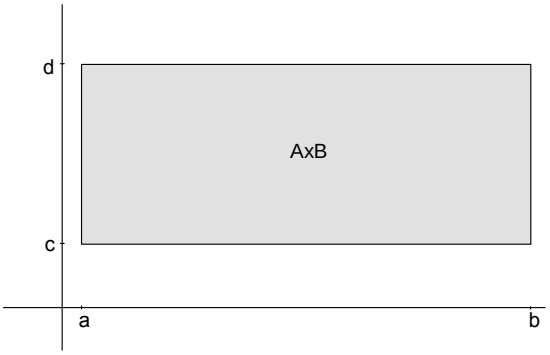


Figura 1.8: Representación gráfica del productocartesiano de intervalos.

Comentario: Sean A y B dos conjuntos no vacíos. Si $a \in A$ y $b \in B$, se tiene que

$$\{a\} \subseteq A \cup B \quad \text{y} \quad \{a, b\} \subseteq A \cup B.$$

Así resulta que

$$(a, b) = \{\{a\}, \{a, b\}\} \subseteq \mathcal{P}(A \cup B).$$

Es decir:

$$(a,b) \in \mathcal{P}\left(\mathcal{P}\left(A \cup B\right)\right).$$

Por lo tanto, una definición precisa del producto cartesiano de A y B sería:

$$A \times B = \{(a,b) \in \mathcal{P}\left(\mathcal{P}\left(A \cup B\right)\right) : a \in A \text{ y } b \in B\}$$

Conviene notar que en general

$$A \times (B \times C) \neq (A \times B) \times C$$

ya que los elementos de $A \times (B \times C)$ son pares ordenados de la forma $(a,(b,c))$, con $a \in A$ y $(b,c) \in B \times C$, mientras que los elementos de $(A \times B) \times C$ son pares ordenados de la forma $((a,b),c)$, con $(a,b) \in A \times B$ y $c \in C$.

Las siguientes propiedades merecen ser recordadas:

1. $A \times \emptyset = \emptyset$ para cualquier conjunto A.

   En efecto, si $A \times \emptyset$ tuviera algún elemento, este sería un par ordenado (a,b), con $a \in A$ y $b \in \emptyset$. Pero como no hay ningún $b \in \emptyset$, no existe tal par ordenado.

2. Si $A \neq \emptyset$ y $B \neq \emptyset$, entonces $A \times B \neq \emptyset$. En efecto, como $A \neq \emptyset$ existe $a \in A$, y como $B \neq \emptyset$ existe $b \in B$. Luego $(a,b) \in A \times B$, y por lo tanto este conjunto no es vacío.

3. La propiedad anterior se puede enunciar también así: Si $A \times B = \emptyset$, entonces $A = \emptyset$ o $B = \emptyset$

4. $A \times (B \cup C) = (A \times B) \cup (A \times C)$. Esta es la propiedad distributiva del producto cartesiano con respecto a la unión (demuéstrela).

Ejemplo 1.7.4 *Sean* $A = \{1,2\}$, $B = \{4\}$, *y* $C = \{5,6\}$. *Vamos a verificar que* $A \times (B \cup C) = (A \times B) \cup (A \times C)$ *en este caso particular:*

$$\begin{aligned} A \times (B \cup C) &= \{1,2\} \times (\{4\} \cup \{5,6\}) \\ &= \{1,2\} \times \{4,5,6\} \\ &= \{(1,4),(1,5),(1,6),(2,4),(2,5),(2,6)\} \\ &= \{(1,4),(2,4),(1,5),(1,6),(2,5),(2,6)\} \\ &= (\{1,2\} \times \{4\}) \cup (\{1,2\} \times \{5,6\}) \\ &= (A \times B) \cup (A \times C). \end{aligned}$$

1.8 Familias de conjuntos

Hemos dicho que los conjuntos se denotan con letras mayúsculas del alfabeto. Si pensamos en que cada letra del alfabeto A, B, C, $\ldots$, Z denota un conjunto, entonces tenemos una familia finita de conjuntos. Sin embargo, el usar las letras del alfabeto para denotar familias de

conjuntos tiene un problema, cual es el vernos limitados a trabajar con familias cuyo número de miembros no sobrepase el número de letras del alfabeto. Para resolver esta limitación, vamos a utilizar los subíndices. La idea es utilizar una letra cualquiera con subíndices para denotar los conjuntos de cierta familia. Por ejemplo, A_1, A_2, A_3, $A_4, \ldots$. De esta forma, podemos trabajar con familias de conjuntos sin importar el número de miembros que las compongan. Por supuesto que en algunos casos es necesario hacer una escogencia adecuada del conjunto de índices (conjunto al cual pertenecen los subíndices). Veamos algunos ejemplos:

Ejemplo 1.8.1 *Sea $\mathfrak{G}$ una familia compuesta por 2 elementos. Entonces escribimos*

$$\mathfrak{G} = \{G_1, G_2\}$$

Ejemplo 1.8.2 *Sea $\mathfrak{F}$ una familia compuesta por 535 conjuntos.*
Entonces escribimos

$$\mathfrak{F} = \{F_1, F_2, F_3, \ldots, F_{535}\}$$

1.8.1 Intersección de familias finitas

Definición 1.8.1 *Sean $E_1, E_2, E_3, \ldots, E_n$, n conjuntos dados. Se llama intersección de $E_1, E_2, E_3, \ldots, E_n$ al conjunto formado por los elementos que pertenecen simultáneamente a todos los n conjuntos dados.*

La intersección de los conjuntos $E_1, E_2, E_3, \ldots, E_n$ se denota por

$$E_1 \cap E_2 \cap \ldots \cap E_n, \text{ o también por } \bigcap_{i=1}^{n} E_i$$

De forma abreviada se puede escribir

$$\bigcap_{i=1}^{n} E_i = \{x : x \in E_i \text{ para cada } i = 1, 2, \ldots, n\}$$

Algunos ejemplos aclararán mejor este concepto.

Ejemplo 1.8.3 *Para $E_1 = \{2, 5, 8, 9\}$, $E_2 = \{5, 9, 11\}$, $E_3 = \{1, 3, 5, 8, 9\}$, $E_4 = \{10, 5, 9\}$, se tiene*

$$\bigcap_{i=1}^{4} E_i = \{5, 9\}.$$

Ejemplo 1.8.4 *Consideremos los siguientes subconjuntos de $\mathbb{N}$:*

$$E_i = \{1, \ldots, i\}, \text{ con } i = 1, 2, \ldots, n.$$

Es decir, $E_1 = \{1\}$, $E_2 = \{1, 2\}$, $E_3 = \{1, 2, 3\}$, y así sucesivamente. Se tiene entonces

$$\bigcap_{i=1}^{n} E_i = \{1\}.$$

Ejemplo 1.8.5 *En un plano dado, consideremos los siguientes conjuntos:*

A_1 : *Conjunto de todos los cuadriláteros.*

A_2 : *Conjunto de todos los polígonos con ángulos iguales.*

A_3 : *Conjunto de todos los polígonos con lados iguales.*

Entonces resulta que:

$A_1 \cap A_2 \cap A_3$ *es el conjunto de todos los cuadrados.*

Nota: Todos los resultados que hemos demostrado para la intersección de dos conjuntos, siguen siendo válidos para el caso de la intersección de n conjuntos, con obvias modificaciones. Por ejemplo, es claro que

$$\bigcap_{i=1}^{n} A_i \subseteq A_j, \text{ para cada } j = 1, \ldots, n.$$

Además, si $C \subseteq A_i$ para cada $i = 1, \ldots, n$ se sigue que

$$C \subseteq \bigcap_{i=1}^{n} A_i.$$

Invitamos al lector a ensayar una demostración de estos resultados.

1.8.2 Unión de familias finitas

Definición 1.8.2 *Sean $E_1, E_2, \ldots, E_n$ conjuntos dados. Se llama unión de estos conjuntos, al conjunto cuyos elementos pertenecen al menos a uno de ellos.*

La unión de los conjuntos $E_1, E_2, \ldots, E_n$ se denota por $E_1 \cup E_2 \cup \ldots \cup E_n$, o por

$$\bigcup_{i=1}^{n} E_i.$$

En forma abreviada podemos escribir

$$\bigcup_{i=1}^{n} E_i = \{x : x \in E_i, \text{ para algún } i = 1, 2, \ldots, n\}$$

Consideremos algunos ejemplos.

Ejemplo 1.8.6 *Si $E_1 = \{1, 2, 3\}, E_2 = \{1, 5\}, E_3 = \{2, 7, 9\}, E_4 = \{4, 5, 8\}$, se tiene*

$$\bigcup_{i=1}^{4} E_i = E_1 \cup E_2 \cup E_3 \cup E_4 = \{1, 2, 3, 4, 5, 7, 8, 9\}.$$

Ejemplo 1.8.7 *Consideremos los siguientes subconjuntos de* $\mathbb{N}$ *:* $E_i = \{1, \ldots, i\}$*, para* $i = 1, 2, \ldots, n$*. Note que* $E_1 = \{1\}$*,* $E_2 = \{1, 2\}$*, y así sucesivamente. En este caso se tiene que*

$$\bigcup_{i=1}^{n} E_i = E_n = \{1, 2, \ldots, n\}.$$

Ejemplo 1.8.8 *Sea* A *el conjunto formado por los números de cuatro cifras que tienen por lo menos un cero. Para* $i = 1, 2, 3$*, sea* A_i *el conjunto de números de cuatro cifras que tienen* i *ceros y las* $4 - i$ *cifras restantes diferentes de cero. Entonces*

$$A_1 \cup A_2 \cup A_3 = \bigcup_{i=1}^{3} A_i = A.$$

En efecto, si $x \in A$ *tiene por lo menos un cero; si tiene tres cifras diferentes de cero pertenece a* A_1*, si tiene dos cifras diferentes de cero pertenece a* A_2*, y si tiene una sola cifra distinta de cero pertenece a* A_3*. En cualquiera de los tres casos* $x \in \bigcup_{i=1}^{3} A_i$*, de donde resulta que* $A \subseteq \bigcup_{i=1}^{3} A_i$*.*

Por otro lado, si $x \in \bigcup_{i=1}^{3} A_i$ *se tiene que* $x \in A_i$ *para algún* $i = 1, 2, 3$*, y como cada* $A_i \subseteq A$*, resulta* $x \in A$*, con lo cual* $\bigcup_{i=1}^{3} A_i \subseteq A$*.*

Al igual que en el caso de la intersección, se generalizan las propiedades de unión al caso de uniones finitas:

$$A_j \subseteq \bigcup_{i=1}^{n} A_i, \text{ para cada } j = 1, \ldots, n.$$

También, si $A_i \subseteq D$ para cada $i = i, \ldots, n$ se sigue que

$$\bigcup_{i=1}^{n} A_i \subseteq D.$$

1.8.3 Generalización de las leyes de De Morgan

Las fórmulas de De Morgan se pueden generalizar al caso de n conjuntos de la manera siguiente:

$$\textbf{(a)} \quad \complement_E \left(\bigcup_{i=1}^{n} A_i \right) = \bigcap_{i=1}^{n} \complement_E A_i$$

$$\textbf{(b)} \quad \complement_E \left(\bigcap_{i=1}^{n} A_i \right) = \bigcup_{i=1}^{n} \complement_E A_i$$

Para demostrar la primera aserción, tomemos $x \in \complement_E \left(\bigcup_{i=1}^{n} A_i \right)$. Esto significa que $x \in E$ y $x \notin \bigcup_{i=1}^{n} A_i$. Pero por definición de unión, esto es equivalente a tener $x \notin A_i$ para cada i, es decir $x \in \complement_E A_i$ para cada $i = 1, \ldots, n$. Finalmente, por definición de intersección esto significa $x \in \bigcap_{i=1}^{n} \complement_E A_i$. Los pasos anteriores se pueden recorrer en la otra dirección, demostrando la igualdad deseada. □

La otra ley se deja como ejercicio.

1.8.4 Generalización de las leyes distributivas

Similarmente, las leyes distributivas se pueden generalizar al caso de uniones e intersecciones de n conjuntos.

$$\textbf{(a)} \quad A \cap \left(\bigcup_{j=1}^{n} B_j \right) = \bigcup_{j=1}^{n} (A \cap B_j)$$

$$\textbf{(b)} \quad A \cup \left(\bigcap_{j=1}^{n} B_j \right) = \bigcap_{j=1}^{n} (A \cup B_j)$$

Demostremos la segunda igualdad:

Primero, dado $x \in A \cup \left(\bigcap_{j=1}^{n} B_j \right)$, se tiene $x \in A$ ó $x \in \bigcap_{j=1}^{n} B_j$. Si $x \in A$ entonces $x \in A \cup B_j$ para cada j, con lo que $x \in \bigcap_{j=1}^{n} (A \cup B_j)$. Si $x \notin A$ entonces $x \in \bigcap_{j=1}^{n} B_j$, lo que significa que $x \in B_j$ para cada $j = 1, \ldots, n$. Luego, como $B_j \subseteq A \cup B_j$ se tiene $x \in A \cup B_j$ para cada j, y esto implica $x \in \bigcap_{j=1}^{n} (A \cup B_j)$.

Recíprocamente, si $x \in \bigcap_{j=1}^{n} (A \cup B_j)$, tenemos $x \in A \cup B_j$ para cada j. Si $x \in A$ entonces $x \in A \cup \left(\bigcap_{j=1}^{n} B_j \right)$. Si $x \notin A$, se sigue que $x \in B_j$ para cada j, y consecuentemente $x \in \bigcap_{i=1}^{n} B_j$. Luego $x \in A \cup \left(\bigcap_{i=1}^{n} B_j \right)$. □

La primera identidad se deja como ejercicio.

1.8.5 Generalización del producto cartesiano

Así como se ha definido el concepto de par ordenado, podemos definir las tripletas ordenadas, de manera que cumplan con condiciones análogas. Más precisamente, requerimos que se cumpla

$$(a, b, c) = (x, y, z) \Leftrightarrow a = x,\ b = y,\ c = z.$$

Una manera de lograr esto es mediante la definición

$$(a, b, c) = ((a, b), c).$$

Es decir, una tripleta sería un par ordenado en el que la primera componente es, a su vez, otro par ordenado. Utilizando la propiedad básica de pares ordenados se tiene:

$$(a, b, c) = (x, y, z) \Rightarrow [(a, b) = (x, y) \wedge \ c = z] \Rightarrow a = x, \ b = y, \ c = z.$$

Una vez resuelto el problema de definir tripletas ordenadas, podemos definir

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

Nótese que bajo esta definición se tiene $A \times B \times C = (A \times B) \times C$, y que este no coincide con $A \times (B \times C)$.

Ejemplo 1.8.9 *Si* $A = \{1\}$, $B = \{3, 4\}$, $C = \{1, 2\}$ *se tiene*

$$A \times B \times C = \{(1, 3, 1), (1, 3, 2), (1, 4, 1), (1, 4, 2)\}.$$

Ejemplo 1.8.10 *Si* $A = \emptyset$ *entonces* $A \times B \times C = \emptyset$. *En efecto, si existiera una tripleta* $(a, b, c) \in \emptyset \times B \times C$, *entonces se tendría* $a \in \emptyset$, *lo cual es imposible.*

Ejemplo 1.8.11 *En general,* $A \times B \times C = \emptyset$ *si y solo si al menos uno de los tres conjuntos es vacío.*

Dados $A_1, \ldots, A_n$ conjuntos, se puede definir sucesivamente el producto cartesiano de ellos, de la siguiente manera: Ya hemos definido $A_1 \times A_2 \times A_3 = (A_1 \times A_2) \times A_3$. Luego se define

$$A_1 \times A_2 \times A_3 \times A_4 = (A_1 \times A_2 \times A_3) \times A_4,$$

y así sucesivamente. Denotando

$$\prod_{i=1}^{n} A_i = A_1 \times \ldots \times A_n,$$

se tiene entonces que

$$\prod_{i=1}^{n+1} A_i = \left(\prod_{i=1}^{n} A_i \right) \times A_{n+1}.$$

Ejemplo 1.8.12 *Si* $A_i = \{i\}$ *se tiene*

$$\prod_{i=1}^{4} A_i = \prod_{i=1}^{4} \{i\} = \{(1, 2, 3, 4)\}.$$

Ejemplo 1.8.13 *Si* $A_i = \{i, i+1\}$ *entonces*

$$\begin{aligned}\prod_{i=1}^{3} A_i &= \prod_{i=1}^{3} \{i, i+1\} \\ &= \{1,2\} \times \{2,3\} \times \{3,4\} \\ &= \{(1,2,3), (1,2,4), (1,3,3), (1,3,4), (2,2,3), (2,2,4), (2,3,3), (2,3,4)\}.\end{aligned}$$

Ejemplo 1.8.14 *Si* $A_i = \left\{1, \frac{1+(-1)^n}{2}\right\}$, *se tiene*

$$\begin{aligned}\prod_{i=1}^{4} A_i &= \{0,1\} \times \{1\} \times \{0,1\} \times \{1\} \\ &= \{(0,1,0,1), (0,1,1,1), (1,1,0,1), (1,1,1,1)\}.\end{aligned}$$

Ejemplo 1.8.15 *Si* $A_1 = \mathbb{R}$, $A_2 = \ldots = A_5 = \{1\}$, *entonces*

$$\prod_{i=1}^{5} A_i = \mathbb{R} \times \{1\} \times \{1\} \times \{1\} \times \{1\} = \{(x,1,1,1,1) : x \in \mathbb{R}\}.$$

Ejemplo 1.8.16 *Si* $A_1 = \ldots = A_n = \mathbb{R}$ *se tiene*

$$\prod_{i=1}^{n} A_i = \mathbb{R} \times \ldots \times \mathbb{R} = \mathbb{R}^n = \{(x_1, \ldots, x_n) : x_i \in \mathbb{R},\ \forall i = 1, \ldots, n\}.$$

Ejemplo 1.8.17 *Si* $A_i = \emptyset$ *para algún* $i \in \{1, \ldots, n\}$ *entonces*

$$\prod_{i=1}^{n} A_i = \emptyset.$$

1.8.6 Familias indexadas por $\mathbb{N}$

En muchos casos se hace necesario trabajar con familias que no son finitas, como lo muestran los siguientes ejemplos.

Ejemplo 1.8.18 *Consideremos el conjunto* $\mathbb{N}$ *de los números naturales y definamos:*

$$B_n = \{n, n+1\},\ \textit{con}\ n \in \mathbb{N}.$$

La familia $\mathfrak{B} = \{B_1, B_2, \ldots, B_n, \ldots\}$ *es una familia infinita de conjuntos, indexada por* $\mathbb{N}$. *Se denota también*

$$\mathfrak{B} = \{B_n : n \in \mathbb{N}\}.$$

Ejemplo 1.8.19 *Consideremos ahora*

$$A_n = \{x \in \mathbb{R} : -n \leq x \leq n\}.$$

Note que A_n es el intervalo $[-n, n]$. Así:

$$A_1 = [-1, 1], \quad A_2 = [-2, 2], \quad A_3 = [-3, 3], \quad etc.$$

La familia $\mathfrak{A} = \{A_1, A_2, \ldots, A_n, \ldots\}$ es una familia indexada por $\mathbb{N}$.

En general, consideraremos familias de conjuntos de la forma

$$\mathfrak{F} = \{F_1, F_2, F_3, \ldots\}, \text{ que también se denota } \mathfrak{F} = \{F_n : n \in \mathbb{N}\}.$$

Nota: Las familias indexadas por $\mathbb{N}$ también se llaman *familias contables.*

Hasta este momento, hemos definido las nociones de unión e intersección de un número finito de conjuntos. Ahora, vamos a extender estas nociones al caso de un número infinito de conjuntos.

Definición 1.8.3 *Sea $\mathfrak{F} = \{F_n : n \in \mathbb{N}\}$ una familia de conjuntos indexada por $\mathbb{N}$. Se define la intersección de la familia $\mathfrak{F}$ así:*

$$\bigcap_{n\in\mathbb{N}} F_n = \{x : x \in F_n \text{ para cada } n \in \mathbb{N}\},$$

mientras que la unión se define por

$$\bigcup_{n\in\mathbb{N}} F_n = \{x : x \in F_n \text{ para algún } n \in \mathbb{N}\}.$$

Ejemplo 1.8.20 *Consideremos la familia de conjuntos formada por*

$$\mathfrak{A} = \{A_1, A_2, \ldots\},$$

donde $A_n = [-n, n]$. En este caso se tiene

$$\begin{array}{ll} (a) & \bigcap\limits_{n\in\mathbb{N}} A_n = A_1 = [-1, 1], \\ (b) & \bigcup\limits_{n\in\mathbb{N}} A_n = \mathbb{R}. \end{array}$$

- *Probemos que $\bigcap\limits_{n\in\mathbb{N}} A_n = A_1$. En efecto, note que los elementos de la familia $\mathfrak{A}$ cumplen:*

  $$A_1 \subseteq A_2 \subseteq A_3 \subseteq \ldots \subseteq A_n \subseteq A_{n+1} \subseteq \ldots$$

  de donde resulta que $A_1 \subseteq \bigcap\limits_{n\in\mathbb{N}} A_n$. Por otro lado, considere $x \in \bigcap\limits_{n\in\mathbb{N}} A_n$. Entonces $x \in A_n$ para todo $n \in \mathbb{N}$, y en particular $x \in A_1$. Por lo tanto $\bigcap\limits_{n\in\mathbb{N}} A_n \subseteq A_1$.

- *Probemos que* $\bigcup_{n\in\mathbb{N}} A_n = \mathbb{R}$. *Sabemos que* $A_n \subseteq \mathbb{R}$ *para todo* $n \in \mathbb{N}$, *y por lo tanto* $\bigcup_{n\in\mathbb{N}} A_n \subseteq \mathbb{R}$. *Para la otra inclusión, sea* $x \in \mathbb{R}$. *Debemos demostrar que existe algún* $n \in \mathbb{N}$ *tal que* $x \in A_n$, *o equivalentemente* $-n \leq x \leq n$. *Esto se obtiene inmediatamente de la arquimedianidad de* $\mathbb{R}$. *En efecto, dado* $x \in \mathbb{R}$ *existe* $n \in \mathbb{N}$ *tal que* $|x| \leq n$, *y entonces* $x \in A_n$.

Ejemplo 1.8.21 *Definimos las familias*

$$\mathfrak{B} = \{B_1, B_2, \ldots, B_n, \ldots\},$$

con $B_n = \{n, n+1, \ldots\}$ *para cada* $n \in \mathbb{N}$, *y*

$$\mathfrak{A} = \{A_1, A_2, \ldots, A_n, \ldots\},$$

con $A_n = \{1, 2, \ldots, n\}$ *para cada* $n \in \mathbb{N}$. *Entonces:*

$$\begin{array}{rclcrcl} \bigcup\limits_{n\in\mathbb{N}} B_n & = & \mathbb{N}, & \qquad & \bigcap\limits_{n\in\mathbb{N}} B_n & = & \emptyset, \\ \bigcup\limits_{n\in\mathbb{N}} A_n & = & \mathbb{N}, & \qquad & \bigcap\limits_{n\in\mathbb{N}} A_n & = & \{1\}. \end{array}$$

¡Compruébelo!

Las leyes de De Morgan, y las leyes distributivas, se generalizan al caso de familias indexadas por $\mathbb{N}$. Veamos:

Teorema 1.3 *Sea* $\mathfrak{A} = \{A_n : n \in \mathbb{N}\}$ *una familia infinita de subconjuntos de* E, *y sea* B *cualquier conjunto. Entonces se cumplen:*

(1) Leyes de De Morgan:

$$\begin{cases} \text{(a) } \complement_E \left(\bigcup\limits_{n\in\mathbb{N}} A_n \right) = \bigcap\limits_{n\in\mathbb{N}} \complement_E A_n \\ \text{(b) } \complement_E \left(\bigcap\limits_{n\in\mathbb{N}} A_n \right) = \bigcup\limits_{n\in\mathbb{N}} \complement_E A_n \end{cases}$$

(2) La doble distributividad:

$$\begin{cases} \text{(a) } \bigcup\limits_{n\in\mathbb{N}} (B \cap A_n) = B \cap \left(\bigcup\limits_{n\in\mathbb{N}} A_n \right) \\ \text{(b) } \bigcap\limits_{n\in\mathbb{N}} (B \cup A_n) = B \cup \left(\bigcap\limits_{n\in\mathbb{N}} A_n \right) \end{cases}$$

Demostración

- Vamos a demostrar 1(b). Para demostrar que $\complement_E \left(\bigcap_{n\in\mathbb{N}} A_n \right) \subseteq \bigcup_{n\in\mathbb{N}} \complement_E A_n$ consideramos $x \in \complement_E \left(\bigcap_{n\in\mathbb{N}} A_n \right)$. Entonces $x \in E$ y $x \notin \bigcap_{n\in\mathbb{N}} A_n$, lo que significa que para algún $n \in \mathbb{N}$ se tiene $x \notin A_n$, y esto indica que $x \in \complement_E A_n$ para dicho n. Consecuentemente $x \in \bigcup_{n\in\mathbb{N}} \complement_E A_n$.

  Recíprocamente, si $x \in \bigcup_{n\in\mathbb{N}} \complement_E A_n$ entonces para algún $n \in \mathbb{N}$ se tiene $x \in \complement_E A_n$, es decir que $x \notin A_n$. Luego $x \notin \bigcap_{n\in\mathbb{N}} A_n$, y consecuentemente $x \in \complement_E \left(\bigcap_{n\in\mathbb{N}} A_n \right)$.

  El argumento anterior se puede escribir resumidamente de la siguiente manera:

$$\begin{aligned} x \in \complement_E \left(\bigcap_{n\in\mathbb{N}} A_n \right) &\Leftrightarrow x \notin \bigcap_{n\in\mathbb{N}} A_n \\ &\Leftrightarrow \exists n \in \mathbb{N} : x \notin A_n \\ &\Leftrightarrow \exists n \in \mathbb{N} : x \in \complement_E A_n \\ &\Leftrightarrow x \in \bigcup_{n\in\mathbb{N}} \complement_E A_n. \ \square \end{aligned}$$

  La proposición 1(a) se demuestra de manera análoga.

- Demostremos ahora 2(a). Vamos a demostrar primero la inclusión "$\subseteq$". Si $x \in \bigcup_{n\in\mathbb{N}} (B \cap A_n)$, entonces para algún $n \in \mathbb{N}$ se tiene $x \in B \cap A_n$, y esto significa $x \in B$ y $x \in A_n$. Así que $x \in B$ y $x \in \bigcup_{n\in\mathbb{N}} A_n$, demostrando que $x \in B \cap \left(\bigcup_{n\in\mathbb{N}} A_n \right)$.

  Recíprocamente, si $x \in B \cap \left(\bigcup_{n\in\mathbb{N}} A_n \right)$, entonces $x \in B$ y $x \in \bigcup_{n\in\mathbb{N}} A_n$. Esto quiere decir que $x \in B$ y $x \in A_n$ para algún $n \in \mathbb{N}$. Por lo tanto $x \in B \cap A_n$ para algún $n \in \mathbb{N}$, lo que significa $x \in \bigcup_{n\in\mathbb{N}} (B \cap A_n)$.

  Invitamos al lector a escribir este argumento en forma resumida. La parte 2(b) se demuestra de manera totalmente análoga. $\square$

1.9 Ejemplos relacionados con problemas de secundaria

Los siguientes ejemplos muestran como la teoría de conjuntos puede ayudar a entender mejor algunos de los problemas que se presentan en secundaria. Por ejemplo, al resolver un sistema de ecuaciones, realmente se está hallando la intersección de varios conjuntos; al analizar una ecuación con valor absoluto, se separa la recta como unión disjunta de conjuntos, en los que

el análisis es más simple, y al final se deben unir las soluciones encontradas en cada caso. Como veremos en el siguiente capítulo, algo similar pasa al encontrar dominios de funciones.

Ejemplo 1.9.1 *Sea* $A = \{x \in \mathbb{R} : |2x+1| \leq 3\}$. *Note que* A *es el conjunto solución de la inecuación* $|2x+1| \leq 3$. *Resolviendo tenemos:*

$$|2x+1| \leq 3 \Leftrightarrow -3 \leq 2x+1 \leq 3 \Leftrightarrow -4 \leq 2x \leq 2 \Leftrightarrow -2 \leq x \leq 1.$$

Entonces $A = [-2, 1]$.

Ejemplo 1.9.2 *Sea* $A = \left\{x \in \mathbb{R} : x^2 + 3x + 2 < 0\right\}$. *Note que*

$$x^2 + 3x + 2 = (x+2)(x+1)$$

es negativo cuando, y solo cuando $-2 < x < -1$. *Luego* $A =]-2, -1[$.

Ejemplo 1.9.3 *Consideremos el problema de resolver la inecuación* $|x+1| \geq 3$. *El lector posiblemente recuerda que en estos casos se analizan las dos posibilidades:* $x+1 \geq 0$ *y* $x+1 < 0$. *En el primer caso la inecuación se convierte en* $x+1 \geq 3$, *de donde* $x \geq 2$. *En el segundo caso se convierte en* $-x-1 \geq 3$, *de donde* $x \leq -4$. *Al final deben unirse las dos soluciones, obteniendo que el conjunto solución es* $A =]-\infty, -4] \cup [2, \infty[$.
Visto desde la teoría de conjuntos, lo que hacemos es tomar $A = \{x \in \mathbb{R} : |x+1| \geq 3\}$ *y* $B = [-1, \infty[$. *Entonces:*

$$A = A \cap \left(B \cup \complement B\right) = (A \cap B) \cup \left(A \cap \complement B\right),$$

donde

$$\begin{array}{rcl} A \cap B & = & \{x : x \geq -1 \ y \ |x+1| \geq 3\} \\ & = & \{x \geq -1 : x+1 \geq 3\} \\ & = & [2, \infty[, \end{array}$$

y similarmente $A \cap \complement B =]-\infty, -4]$.

Ejemplo 1.9.4 *Resolver el sistema de ecuaciones en dos variables:*

$$\left\{ \begin{array}{l} 2x + 4y = 3 \\ x - 3y = 4. \end{array} \right. \tag{1.2}$$

Se trata de hallar la intersección de los conjuntos

$$A = \left\{(x, y) \in \mathbb{R}^2 : 2x + 4y = 3\right\}, \quad B = \left\{(x, y) \in \mathbb{R}^2 : x - 3y = 4\right\}.$$

Algebraicamente, de la segunda ecuación se deduce que $y = \frac{1}{3}(x-4)$, *y al sustituir en la primera se obtiene*

$$2x + \tfrac{4}{3}(x-4) = 3 \Rightarrow 10x - 16 = 9 \Rightarrow x = \tfrac{5}{2}.$$

Luego $y = \frac{1}{3}(x-4) = -\frac{1}{2}$. *El conjunto solución es entonces* $A \cap B = \left\{\left(\frac{5}{2}, -\frac{1}{2}\right)\right\}$.
Geométricamente, lo que buscamos es la intersección de las rectas de ecuaciones dadas.

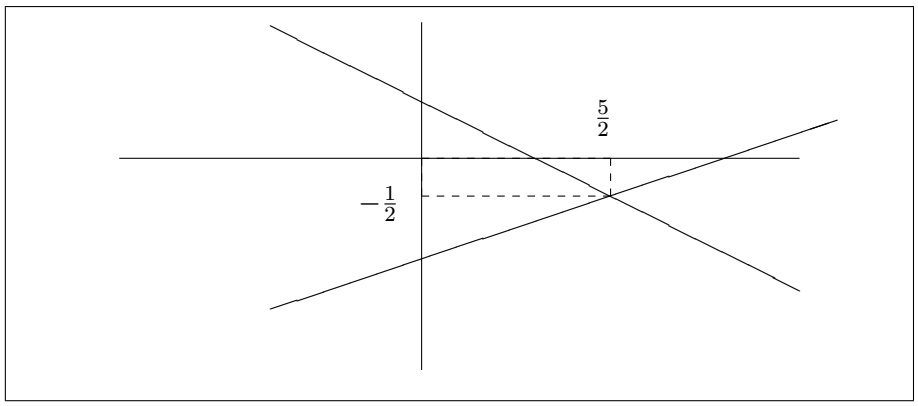


Figura 1.9: Solución gráfica del sistema de ecuaciones lineales (1.2).

1.10 Ejercicios

1. Sean $A = \{a, b, c, d, e\}$, $B = \{a, c, e, g\}$, $C = \{b, d, f\}$, donde los elementos a, b, c, d, e, f, g son todos distintos. Halle $A \cap B$, $A \cup B$, $A - B$, $A - C$, $B \cap C$, $B \cup C$, $B - A$, $C - A$, $(B \cup C) - A$, $A - (B \cap C)$, $A \triangle B$. ¿Cuántos elementos tiene $A \times B$?

2. Sean $E = \{n \in \mathbb{N} : n \text{ es par}\}$, $A = \{n \in E : n > 10\}$, $B = \{n \in E : 2n + 1 \geq 25\}$. Demuestre que $A = B$.

3. Sean $A = [1, 3] \cup \{7\}$ y $B =]0, 5[$. Halle $A \cup B$, $A \cap B$, $A - B$, $B - A$, $A \triangle B$, $\complement_{\mathbb{R}} A$ y $\complement_{\mathbb{R}} B$.

4. Sea $A = \{x \in \mathbb{R} : |x + 1| - |x - 2| \leq 2\}$. Halle $A \cap]-\infty, -1[$, $A \cap [-1, 2]$ y $A \cap]2, \infty[$. Concluya que $A = \left]-\infty, \frac{3}{2}\right]$.

5. Repita el ejercicio anterior con $A = \{x \in \mathbb{R} : |x + 1| + |x - 2| \leq 3\}$.

6. Exprese como intervalo, o unión de intervalos, cada uno de los siguientes conjuntos:

$$A = \left\{x \in \mathbb{R} : 3 + x^2 < 7\right\} \qquad E = \left\{x \in \mathbb{R} : 3 - x^2 < 3\right\}$$
$$B = \left\{x \in \mathbb{R} : x^2 + 4x + 3 \geq 0\right\} \qquad F = \left\{x \in \mathbb{R} : \left(x^2 - 4\right)\left(x^2 - 9\right) > 0\right\}$$
$$C = \left\{x \in \mathbb{R} : \frac{1}{x} + \frac{1}{1 - x} \geq 0\right\} \qquad G = \left\{x \in \mathbb{R} : (x + 1)\left(x^2 - 4\right) < 0\right\}$$
$$D = \left\{x \in \mathbb{R} : \frac{1 - x}{x + 1} \geq 0\right\} \qquad H = \{x \in \mathbb{R} : (x - 1)(x + 3)(2x + 3) > 0\}.$$

7. Resuelva cada una de las siguientes inecuaciones, explicando con detalle las operaciones

con conjuntos involucradas:

$$|x-2| \geq 5, \qquad |x+1| + |x-2| > 1,$$
$$|x+1| < 3, \qquad |x^2+3x+2| > 0,$$
$$|x^2-1| > 3, \qquad |x^2+3x+2| > 1,$$
$$|x-1| - |x+1| < 1, \qquad |x^2+3x+2| \geq \tfrac{1}{4}.$$

8. Determine cuáles de los siguientes conjuntos son vacíos.

   $A = \{x \in \mathbb{N} : x^2 = 12\}$ $\quad B = \{x \in \mathbb{R} : x^2 = 7 \text{ y } x^3 = 12\}$

   $C = \{x \in \mathbb{R} : x^2 = 2x - 1\}$ $\quad D = \{x \in \mathbb{R} : x^2 = 2x + 1\}$

   $E = \{x \in \mathbb{R} : x^2 = x - 1\}$ $\quad F = \{A \in \mathcal{P}(\mathbb{N}) : A \subsetneq \mathbb{Z}\}$

9. Halle el conjunto potencia de cada uno de los siguientes conjuntos:

   (a) $A = \{1, 2, \emptyset\}$

   (b) $B = \{1, \{1\}, \{\{1\}\}\}$

   (c) $C = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$

10. Dé ejemplos de conjuntos A tales que:

    · $\mathcal{P}(A)$ tenga 512 elementos.

    · $\mathcal{P}(\mathcal{P}(A))$ tenga 256 elementos.

    · $\mathcal{P}(\mathcal{P}(\mathcal{P}(A)))$ tenga 16 elementos.

    · $\mathcal{P}(A \cup \mathcal{P}(A))$ tenga 32 elementos.

    · $\mathcal{P}(A \cup \mathcal{P}(A) \cup \mathcal{P}(\mathcal{P}(A)))$ tenga 4 elementos.

11. ¿Será posible hallar un conjunto A tal que:

    · $\mathcal{P}(A)$ tenga 3 elementos?

    · $\mathcal{P}(A) - A$ tenga 3 elementos?

    · $\mathcal{P}(\mathcal{P}(A))$ tenga 8 elementos?

    · $\mathcal{P}(A \cup \mathcal{P}(A))$ tenga 16 elementos?

12. Si es posible halle $A \neq \emptyset$ tal que.

    (a) $A \subseteq \mathcal{P}(A)$

    (b) $A \cap (A \times A) \neq \emptyset$

    (c) $(A \times \mathcal{P}(A)) \cap A \neq \emptyset$

13. Demuestre que para cualesquiera conjuntos A, B y C se tiene

    (a) $A \cap B \subseteq A \subseteq A \cup B$
    (b) $A \cap B = B \cap A$
    (c) $A \cup B = B \cup A$
    (d) $(A \cup B) \cup C = A \cup (B \cup C)$
    (e) $(A \cap B) \cap C = A \cap (B \cap C)$
    (f) $A \cup A = A \cap A = A$

14. Demuestre las leyes distributivas:

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

15. Demuestre la segunda ley de De Morgan:

$$\complement_E (B \cap C) = \left(\complement_E A\right) \cup \left(\complement_E B\right).$$

16. Demuestre que:

    (a) Si $A \subseteq B$ y $C \subseteq D$, entonces $A \cup C \subseteq B \cup D$ y $A \cap C \subseteq B \cap D$.
    (b) Si $A \subseteq B$, entonces $A \cup B = B$ y $A \cap B = A$.
    (c) $A \subseteq B$ si y solo si $A \cup B = B$.
    (d) $A \subseteq B$ si y solo si $A - B = \emptyset$.

17. Sea E el conjunto de referencia, y denote por A^c al complemento de A en E. Demuestre que para $A, B \subseteq E$, se tiene:

    (a) $A \cup A^c = E$.
    (b) $A \cap A^c = \emptyset$.
    (c) $(A - B)^c = A^c \cup B$.

18. Si $A \subseteq C$ y $B \subseteq D$, demuestre que $A \times B \subseteq C \times D$.

19. Sean A, B y C conjuntos. Demuestre que

    (a) $(A \cap B) \times C = (A \times C) \cap (B \times C)$.
    (b) $A \times (B \cap C) = (A \times B) \cap (A \times C)$.
    (c) $(A \cup B) \times C = (A \times C) \cup (B \times C)$.
    (d) $A \times (B \cup C) = (A \times B) \cup (A \times C)$.
    (e) $(A - B) \times C = (A \times C) - (B \times C)$.

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

20. Sea $\mathcal{F}$ una familia de subconjuntos de E. Es decir, $\mathcal{F} \subseteq \mathcal{P}(E)$. Se define

$$\begin{aligned} \bigcup_{S\in\mathcal{F}} S &= \{x : x \in S \text{ para algún } S \in \mathcal{F}\} = \{x : (\exists S \in \mathcal{F}\,)\,(x \in S)\ \}, \\ \bigcap_{S\in\mathcal{F}} S &= \{x : x \in S \text{ para todo } S \in \mathcal{F}\} = \{x : (\forall S \in \mathcal{F}\,)\,(x \in S)\ \}. \end{aligned}$$

(a) Demuestre las leyes de De Morgan:

$$\complement_E\left(\bigcup_{S\in\mathcal{F}} S\right) = \bigcap_{S\in\mathcal{F}} \complement_E S, \qquad \complement_E\left(\bigcap_{S\in\mathcal{F}} S\right) = \bigcup_{S\in\mathcal{F}} \complement_E S.$$

(b) Si $A \subseteq S$, para todo $S \in \mathcal{F}$, demuestre que $A \subseteq \bigcap_{S\in\mathcal{F}} S$.

(c) Si $S \subseteq B$, para todo $S \in \mathcal{F}$, demuestre que $\bigcup_{S\in\mathcal{F}} S \subseteq B$.

21. Halle $\bigcup_{n\in\mathbb{N}} S_n$ y $\bigcap_{n\in\mathbb{N}} S_n$ para:

a. $S_n = [\frac{1}{n}, 2]$ d. $S_n =]-\frac{1}{n}, \frac{1}{n}[$

b. $S_n = [-\frac{1}{n}, 1[$ e. $S_n = [1 + (-1)^n, 3]$

c. $S_n = [\frac{n}{n+1}, \frac{n+1}{n}]$ f. $S_n = \left\{\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}\right\}$.

22. Si $\mathcal{P}(E) = \{\emptyset\}$, demuestre que $E = \emptyset$.

23. Demuestre que si A y B son conjuntos, se cumple que:

$$A \subseteq B \Leftrightarrow \mathcal{P}(A) \subseteq \mathcal{P}(B).$$

24. ¿Qué se puede afirmar de dos conjuntos A y B tales que $\mathcal{P}(\mathcal{P}(A)) = \mathcal{P}(\mathcal{P}(B))$?

25. Sean $A, B \in \mathcal{P}(E)$. Demuestre que $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.

26. Sean $A, B \in \mathcal{P}(E)$. Demuestre que $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$. ¿Será cierta la igualdad?.

27. Supongamos que $A \subseteq F$ y $A \subseteq E$. ¿Existe alguna relación general entre $\complement_F A, \complement_E A$ y $\complement_{E\cup F} A$?

28. Sean E_1, E_2, E_3, …, E_n conjuntos dados. Demuestre que para todo $j \in \{1, \ldots, n-1\}$ se cumple

$$\left(\bigcap_{i=1}^{j} E_i\right) \bigcap \left(\bigcap_{i=j+1}^{n} E_i\right) = \bigcap_{i=1}^{n} E_i.$$

29. Sean $r_1, r_2, \ldots, r_n$ números reales tales que $r_1 \leq r_2 \leq \ldots \leq r_n$. Demostrar que

$$\bigcup_{i=1}^{n-1} \{x : r_i \leq x \leq r_{i+1}\} = \{x : r_1 \leq x \leq r_n\}.$$

Es decir, demuestre que

$$\bigcup_{i=1}^{n-1} [r_i, r_{i+1}] = [r_1, r_n].$$

30. Para $E_1, \ldots, E_n$ conjuntos, demuestre que

$$\bigcup_{i=1}^{n} \mathcal{P}(E_i) \subseteq \mathcal{P}\left(\bigcup_{i=1}^{n} E_i\right).$$

Capítulo 2

Relaciones Binarias

Podría decirse que la Matemática consta de conjuntos y de relaciones entre estos. Las más simples de estas relaciones son las relaciones binarias, esto es, relaciones entre los elementos de dos conjuntos dados. Estas son usadas muchas veces de una manera inconsciente, sin hacer mención explícita de ellas. Sin embargo, si se quiere tener cierta rigurosidad al hablar de temas tan simples como por ejemplo los números enteros, es indispensable construir cierta teoría de relaciones binarias. En este capítulo abordamos este tema de una manera elemental, restringiéndonos únicamente a estudiar aquellos conceptos que son estrictamente necesarios para desarrollar los capítulos posteriores.
El concepto de relación binaria, aunque más abstracto que el de función, es de gran utilidad para darle rigor a las construcciones de los conjuntos numéricos, tarea que abordaremos en capítulos posteriores. El estudiar las relaciones binarias en su generalidad, nos permite disponer de un lenguaje mucho más apropiado a la hora de hablar de operaciones como la composición de funciones, y de conceptos como el de función inversa, por mencionar algunos.

2.1 Conceptos básicos

Dados dos conjuntos A y B, y dado $R \subseteq A \times B$, podemos pensar en R como una relación que asocia elementos de A con elementos de B. Más precisamente, podemos decir que $a \in A$ se relaciona con $b \in B$ si $(a, b) \in R$. Podríamos decir entonces que una relación de A en B es un subconjunto de $A \times B$, pero para evitar ambigüedades, vamos a dar una definición más precisa.

Definición 2.1.1 *Dados dos conjuntos A y B, una relación binaria de A en B es una tripleta $\mathcal{R} = (A, B, R)$, donde $R \subseteq A \times B$. Al conjunto A se le llama el conjunto de salida de la relación, a B se le llama el conjunto de llegada, y a R el gráfico de la misma.*

Cuando a se relaciona con b bajo la relación $\mathcal{R}$, escribimos $a\mathcal{R}b$. En caso contrario escribimos $a\not\mathcal{R}b$

Ejemplo 2.1.1 *Sean*

$$A = \{1, 2, 3\}, B = \{a, b\}, R = \{(1, a), (1, b), (2, a), (3, b)\} \subseteq A \times B.$$

Tenemos entonces que $1\mathcal{R}a$, $1\mathcal{R}b$, $2\mathcal{R}a$, $3\mathcal{R}b$. *Además* $2\not\mathcal{R}b$ *y* $3\not\mathcal{R}a$.

Ejemplo 2.1.2 *Sean* $A = B = \mathbb{N}$, $R = \{(n, 2n) : n \in \mathbb{N}\} \subseteq \mathbb{N} \times \mathbb{N}$. *Entonces* $1\mathcal{R}2$, $2\mathcal{R}4$, $3\mathcal{R}6$, *y en general* $n\mathcal{R}2n$.

Ejemplo 2.1.3 *Sea* $A = \mathbb{N}$, $B = \{0, 1\}$, $R = \{(n, 0) : n \text{ es par}\} \cup \{(n, 1) : n \text{ es impar}\}$. *Entonces* $2\mathcal{R}0$, $1\mathcal{R}1$, $3\mathcal{R}1$, $4\mathcal{R}0$, *etc.*

En la práctica se piensa una relación como una ley que asocia elementos de A con elementos de B. De hecho, la manera más común de definir una relación es dando explícitamente esa ley. Para ilustrar esto, observe que la relación del ejemplo 2.1.2 se puede describir como:

$$n\mathcal{R}m \Leftrightarrow m = 2n.$$

En el ejemplo 2.1.3 podemos definir

$$n\mathcal{R}p \Leftrightarrow n + p \text{ es par},$$

o también podemos decir que $n\mathcal{R}p$ sii p es el resto que se obtiene al dividir n por 2 (tenga presente en este ejemplo que $p \in \{0, 1\}$).

2.1.1 Relación Inversa

Antes de entrar a dar una definición precisa de relación inversa, veamos la siguiente relación $\mathcal{R}$ definida sobre $\mathbb{N}$:

$$x\mathcal{R}y \Leftrightarrow x \text{ es divisor de } y.$$

Resulta claro ver que

$$3\mathcal{R}6,\ 3\mathcal{R}27,\ 5\mathcal{R}10,\ 5\mathcal{R}25.$$

También resulta fácil ver que $6\not\mathcal{R}3$, $7\not\mathcal{R}12$. Ahora consideremos otra relación $\mathcal{P}$ sobre $\mathbb{N}$, definida de la manera siguiente:

$$u\mathcal{P}v \Leftrightarrow u \text{ es divisible por } v.$$

Comparando las relaciones $\mathcal{R}$ y $\mathcal{P}$ que acabamos de definir sobre $\mathbb{N}$, se puede observar que $v\mathcal{R}u \Leftrightarrow u\mathcal{P}v$. En este caso, decimos que $\mathcal{P}$ es la relación inversa de $\mathcal{R}$ y la denotamos por $\mathcal{P} = \mathcal{R}^{-1}$.
De manera general, a toda relación $\mathcal{R} = (A, B, R)$ le corresponde una relación inversa $\mathcal{R}^{-1}$, que definimos a continuación. Primero definimos el gráfico inverso R^{-1} así:

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

Note que $R^{-1} \subseteq B \times A$, y por lo tanto define una relación de B en A.

Definición 2.1.2 *Si $\mathcal{R} = (A, B, R)$ es una relación binaria, la relación inversa $\mathcal{R}^{-1}$ se define como*

$$\mathcal{R}^{-1} = \left(B, A, R^{-1}\right).$$

Es decir, para $a \in A$ y $b \in B$ se tiene:

$$b\mathcal{R}^{-1}a \Leftrightarrow a\mathcal{R}b.$$

Veamos algunos ejemplos:

Ejemplo 2.1.4 *Sean $A = \{1, 2, 3\}$, $B = \{a, b\}$, $R = \{(1, a), (1, b), (2, a), (3, b)\}$. Entonces $R^{-1} = \{(a, 1), (b, 1), (a, 2), (b, 3)\}$. En particular $a\mathcal{R}^{-1}1$, $b\mathcal{R}^{-1}1$, etc.*

Ejemplo 2.1.5 *Sean $A = B = \mathbb{N}$, y definamos $\mathcal{R}$ como sigue:*

$$n\mathcal{R}m \Leftrightarrow n + m \text{ es par.}$$

Entonces $\mathcal{R}^{-1} = \mathcal{R}$. En efecto, como $A = B$, $\mathcal{R}$ y $\mathcal{R}^{-1}$ tienen mismo conjunto de salida y de llegada. Además se tiene

$$\begin{aligned} m\mathcal{R}^{-1}n &\Leftrightarrow n\mathcal{R}m \\ &\Leftrightarrow n + m \text{ es par} \\ &\Leftrightarrow m + n \text{ es par} \\ &\Leftrightarrow m\mathcal{R}n. \end{aligned}$$

Se tiene entonces que $\mathcal{R}$ y $\mathcal{R}^{-1}$ tienen también mismo gráfico, así que $\mathcal{R}^{-1} = \mathcal{R}$.

Ejemplo 2.1.6 *Sean $A = \mathbb{N}$, $B = \{0, 1\}$, y definamos la relación $\mathcal{S}$ de A a B como sigue:*

$$n\mathcal{S}m \Leftrightarrow n + m \text{ es par.}$$

Esta es la misma relación del ejemplo 2.1.3, pero no es la misma del ejemplo anterior dado que difieren en el conjunto de llegada. Ahora $\mathcal{S}^{-1}$ se define igual que $\mathcal{S}$:

$$m\mathcal{S}^{-1}n \Leftrightarrow m + n \text{ es par,}$$

pero $\mathcal{S}^{-1} \neq \mathcal{S}$ dado que los conjuntos de salida y de llegada son diferentes.

2.1.2 Composición de relaciones

Considere dos relaciones $\mathcal{R} = (A, B, R)$ y $\mathcal{S} = (B, C, S)$. Para entender el concepto de composición, pensemos en la relación $\mathcal{R}$ como estableciendo puentes desde los elementos de A a los de B; la relación $\mathcal{S}$ hará lo mismo entre los elementos de B y de C. La composición de estas relaciones, relacionará todos aquellos elementos de A y de C que estén "conectados" a través de un elemento de B. Es decir, diremos que $a\mathcal{S} \circ \mathcal{R}c$ si existe $b \in B$ tal que $a\mathcal{R}b$ y $b\mathcal{S}c$. Para ser más precisos, se define el gráfico

$$S \circ R = \{(a, c) \in A \times C : \exists b \in B \text{ t.q. } (a, b) \in R \text{ y } (b, c) \in S\},$$

y luego $\mathcal{S} \circ \mathcal{R} = (A, C, S \circ R)$.

Ejemplo 2.1.7 *Consideremos las relaciones* $\mathcal{R} = (\mathbb{N}, \mathbb{Z}, R)$ *y* $\mathcal{S} = (\mathbb{Z}, \mathbb{N}, S)$, *con*

$$R = \{(|z|, z) : s \in \mathbb{Z}\}, \quad S = \{(z, |z| - z) : z \in \mathbb{Z}\}.$$

Se tiene $\mathcal{S} \circ \mathcal{R} = (\mathbb{N}, \mathbb{N}, T)$, *con*

$$T = \{(n, 0) : n \in \mathbb{N}\} \cup \{(n, 2n) : n \in \mathbb{N}\}.$$

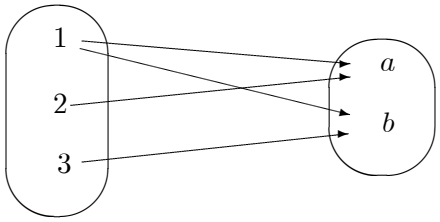
El lector puede convencerse de esto.

2.1.3 Representaciones gráficas de relaciones

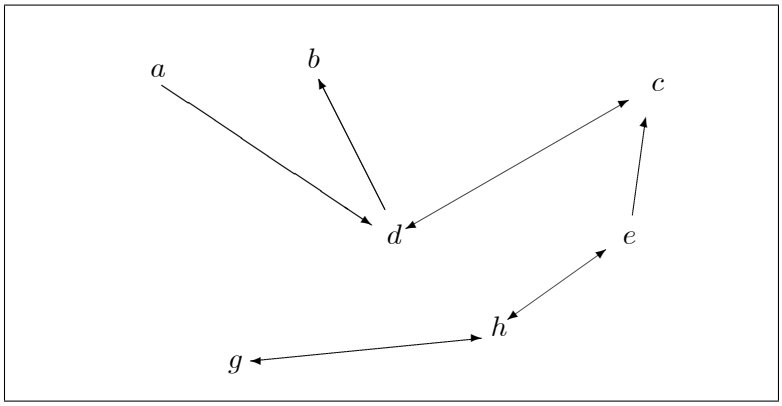
Existen varias maneras de representar relaciones binarias, dependiendo de su naturaleza. La más común parece ser la que se usa en secundaria, mediante el uso de diagramas de flechas. En el caso que los conjuntos A y B sean finitos, o si al menos se pueden numerar de cierta manera, se pueden representar sus elementos en regiones de un plano, donde la relación de dos elementos se simboliza con una flecha que sale del primero y llega al segundo. En el caso del ejemplo 2.1.1 se tiene

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

La relación se puede representar mediante la siguiente figura:



En caso de relaciones definidas de un conjunto en sí mismo, se pueden pintar los elementos en una misma región, y unir por flechas aquellos que se relacionan. Por ejemplo, la figura



puede representar la relación $\mathcal{R} = (E, E, R)$, donde $E = \{a, b, c, d, e, g, h\}$, y

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

2.2 Tipos de relaciones

En esta sección consideramos únicamente relaciones binarias de la forma $\mathcal{R} = (E, E, R)$, esto es, relaciones definidas de un conjunto E en sí mismo. Como iremos dándonos cuenta, los tipos de relaciones que describiremos a continuación, son de gran importancia en matemática.

Definición 2.2.1 *Se dice que:*

- $\mathcal{R}$ *es* ***reflexiva*** *si* $a\mathcal{R}a$, $\forall a \in E$. *Esto es, todo elemento de* E *se relaciona consigo mismo.*
- $\mathcal{R}$ *es* ***simétrica*** *si* $\forall a, b \in E,\ a\mathcal{R}b \Rightarrow b\mathcal{R}a$.
- $\mathcal{R}$ *es* ***transitiva*** *si* $a\mathcal{R}b \wedge b\mathcal{R}c \Rightarrow a\mathcal{R}c$.
- $\mathcal{R}$ *es* ***antisimétrica*** *si para* $a \neq b$ *se tiene que* $a\mathcal{R}b \Rightarrow b\not\mathcal{R}a$. *Equivalentemente, si para todo* $a, b \in E$ *se tiene* $(a\mathcal{R}b \wedge b\mathcal{R}a) \Rightarrow a = b$.

Veamos algunos ejemplos:

Ejemplo 2.2.1 *Sean* $E = \{1, 2, 3\}$ *y* $R = \{(1, 1), (1, 2), (2, 2), (2, 3), (3, 3)\}$. *Entonces*
$\mathcal{R}$ *es reflexiva pues* $1\mathcal{R}1$, $2\mathcal{R}2$, $3\mathcal{R}3$.
$\mathcal{R}$ *no es simétrica pues* $1\mathcal{R}2$ *pero* $2\not\mathcal{R}1$.
$\mathcal{R}$ *no es transitiva pues* $1\mathcal{R}2$, $2\mathcal{R}3$, *pero* $1\not\mathcal{R}3$.
$\mathcal{R}$ *es antisimétrica, pues* $2\not\mathcal{R}1$, $3\not\mathcal{R}2$.

Ejemplo 2.2.2 *Si* $E = \{1, 2, 3\}$, *y* $R = \{(1, 1), (1, 2), (2, 1), (1, 3), (2, 3)\}$, *tenemos*
$\mathcal{R}$ *no es reflexiva pues* $2\not\mathcal{R}2$.
$\mathcal{R}$ *no es simétrica pues* $1\mathcal{R}3$ *y* $3\not\mathcal{R}1$.
$\mathcal{R}$ *no es transitiva pues* $2\mathcal{R}1$ *y* $1\mathcal{R}2$, *pero* $2\not\mathcal{R}2$.
$\mathcal{R}$ *no es antisimétrica pues* $1\mathcal{R}2$ *y* $2\mathcal{R}1$, *siendo* $1 \neq 2$.

Ejemplo 2.2.3 *Si* $E = \{1, 2, 3\}$, $R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3)\}$. *Es fácil verificar que* $\mathcal{R}$ *es reflexiva, simétrica y transitiva, pero no es antisimétrica.*

Ejemplo 2.2.4 *Sea* E *cualquier conjunto,* $R = \{(a, a) : a \in E\}$. *Esto es,* $a\mathcal{R}b$ *si y solo si* $a = b$. *Entonces* $\mathcal{R}$ *es reflexiva, simétrica, transitiva y antisimétrica. De hecho, es la única relación que posee las cuatro propiedades.*

Ejemplo 2.2.5 *Sea* $E = \mathbb{N}$, *y defina* $n\mathcal{R}m$ *sii* $n \leq m$. *Entonces* $\mathcal{R}$ *es reflexiva, antisimétrica y transitiva. No es simétrica.*

Ejemplo 2.2.6 *Con* $E = \mathbb{N}$ *otra vez, defina* $n\mathcal{R}m$ *sii* $n < m$. *Entonces* $\mathcal{R}$ *no es reflexiva ni simétrica. Sí es transitiva y antisimétrica, esto último pues es imposible tener* $n < m$ *y* $m < n$ *a la vez.*

Ejemplo 2.2.7 *En* $E = \mathbb{N}$, *se define la relación* $x\mathcal{R}y \Leftrightarrow x = y^2$. *Esta relación no es reflexiva, pues* $m \neq m^2$ *excepto para* $m = 1$. *Además no es simétrica ni transitiva. ¿Será antisimétrica?*

2.2.1 Relaciones de orden

Una relación $\mathcal{R} = (E, E, R)$ se llama relación de orden si es reflexiva, antisimétrica y transitiva. Por ejemplo, ya vimos en el ejemplo 2.2.5 que " $\leq$ " es una relación de orden en $\mathbb{N}$. Podría decirse que este es el ejemplo típico de una relación de orden. Veamos otros ejemplos:

Ejemplo 2.2.8 *Para $E = \mathbb{N}^*$ se define $\mathcal{R}$ por*

$$n\mathcal{R}m \text{ sii } n \text{ es divisor de } m.$$

Esta relación es claramente reflexiva. Además es antisimétrica, pues en particular si n es divisor de m debe tenerse $n \leq m$. Ahora, si n es divisor de m tenemos $m = nk$, para algún $k \in \mathbb{N}$. Si además m es divisor de p, tenemos $p = ml$, para algún $l \in \mathbb{N}$, y luego $p = ml = n(kl)$, lo que demuestra que n es divisor de p. Entonces $\mathcal{R}$ es también transitiva, y por lo tanto de orden. Note que esta relación es una "subrelación" de "$\leq$", en el sentido que el gráfico de la primera está contenido en el de la segunda. Más precisamente:

$$\{(n, m) : n \text{ es divisor de } m\} \subseteq \{(n, m) : n \leq m\}.$$

Ejemplo 2.2.9 *Sea X un conjunto, y sea $E = \mathcal{P}(X)$. Se define en E la relación*

$$A\mathcal{R}B \text{ sii } A \subseteq B.$$

Como los elementos de E son conjuntos, preferimos usar $A, B, etc.$ en vez de $x, y, etc.$ Como siempre ocurre $A \subseteq A$, tenemos que $\mathcal{R}$ es reflexiva. Además, por "definición" de igualdad tenemos que $A \subseteq B$ y $B \subseteq A$ implica $A = B$. Finalmente, sabemos que $A \subseteq B$ y $B \subseteq C$ siempre implica $A \subseteq C$. La relación "$\subseteq$" es entones una relación de orden en E.

Cuando se estudian las relaciones de orden, se distinguen las relaciones de orden total y las relaciones de orden parcial.

Definición 2.2.2 *Una relación de orden $\mathcal{R}$, sobre un conjunto E, se llama un orden total sobre E si, para todo par de elementos $x, y \in E$, se tiene $x\mathcal{R}y$ o $y\mathcal{R}x$. Si $\mathcal{R}$ es un orden total sobre E, el par ordenado $(E, \mathcal{R})$ se llama un conjunto totalmente ordenado.*

El ejemplo clásico de una relación de orden total es la realción " $\leq$ " sobre el conjunto de los naturales.

Definición 2.2.3 *Una relación de orden $\mathcal{R}$ sobre E, se llama orden parcial si $\mathcal{R}$ no es un orden total sobre E. Es decir, si existen $x, y \in E$ tales que $x\not\mathcal{R}y$ y $y\not\mathcal{R}x$. Un conjunto E dotado de un orden parcial se llama parcialmente ordenado.*

Ejemplo 2.2.10 *Para ilustrar con un ejemplo una relación de orden parcial, vamos a considerar $E = P(X)$; donde X es cualquier conjunto, y la relación de inclusión. Es decir, sobre $P(X)$ se considera la relación $A\mathcal{R}B \Leftrightarrow A \subseteq B$. Ya hemos observado que esta relación es reflexiva, antisimétrica y transitiva; o sea " $\subseteq$ " es una relación de orden sobre $P(X)$. Sin embargo, esta relación solo permite "comparar" dos conjuntos cuando uno está contenido en el otro. Por ejemplo, si $A = \{1, 2\}$ y $B = \{2, 3\}$ se tiene $A \subsetneq B$ y $B \subsetneq A$.*

Definición 2.2.4 *Sea E un conjunto dotado de una relación de orden denotada por " $\leq$ ". Para $Y \subseteq E$, un elemento $m \in E$ se llama una cota superior de Y si para cada $y \in Y$ se tiene $y \leq m$. Cuando $Y \subseteq E$ posee una cota superior, se dice que Y es acotado superiormente.*

Ejemplo 2.2.11 *Sea $E = \mathbb{N}$ con el orden usual " $\leq$ ". Considere el siguiente subconjunto*

$$Y = \{n \in \mathbb{N} : n \text{ es un entero de } 3 \text{ cifras}\}$$

Sea $m = 1635$. Es claro que

$$n \leq m, \ \forall n \in Y,$$

así que $m = 1635$ es una cota superior de Y. Note que en este caso, el número 999 es la menor cota superior.

Desde luego que en $\mathbb{N}$ se pueden encontrar muchos subconjuntos que no son acotados superiormente, es decir que no poseen una cota superior. Por ejemplo, el conjunto de los números naturales pares.
Decimos que m es el elemento máximo de un subconjunto Y de E, si m es una cota superior de Y y además $m \in Y$. Observe, entonces, que si b es otra cota superior de Y se tiene $m \leq b$, y en consecuencia un elemento máximo de Y es la menor cota superior de Y. Es inmediato darse cuenta que si Y posee un elemento máximo (un mayor elemento), entonces Y está acotado superiormente. Sin embargo, bien puede suceder que Y sea acotado superiormente y no posea un mayor elemento.

Ejemplo 2.2.12 *El conjunto $Y = \{x \in \mathbb{Q} : 0 < x < 1\}$ es un conjunto acotado superiormente en $\mathbb{R}$, pero no posee un mayor elemento.*

De manera análoga, un elemento $m \in E$ se llama una cota inferior de Y si $m \leq y$ para cada $y \in Y$. Si Y posee una cota inferior, se dice que Y es acotado inferiormente. Un elemento p es el elemento mínimo de Y si $p \in Y$ y p es cota inferior de Y.

Ejemplo 2.2.13 *Dada la relación de orden en $\mathbb{N}$ definida por*

$$n \mathcal{R} m \Leftrightarrow n \text{ es divisor de } m,$$

el conjunto

$$Y = \{n \leq 30 : n \text{ es múltiplo de } 7\},$$

tiene a $m = 7$ como mínimo y $b = 28$ como máximo. Para el conjunto $A = \{3, 5, 6, 8\}$ se tiene que $b = 120$ es una cota superior. De hecho, esta es la menor cota superior, pero A no tiene máximo. Note también que $m = 1$ es la única cota inferior de A, y que A no tiene mínimo.

2.2.2 Relaciones de Equivalencia

El concepto de relación de equivalencia generaliza el concepto de igualdad en un sentido que irá aclarándose conforme avancemos en ejemplos y aplicaciones del mismo. En matemática se utiliza mucho este concepto en diferentes contextos, para identificar objetos que, aunque diferentes, comparten una serie de propiedades que nos permiten tratarlos como iguales. Una de las primeras aplicaciones interesantes que haremos de las relaciones de equivalencia, es en la construcción de $\mathbb{Q}$ a partir de $\mathbb{Z}$, donde identificamos todas las fracciones $\frac{m}{n}$ que definen un mismo racional.

Definición 2.2.5 *Una relación $\mathcal{R} = (E, E, R)$ se llama relación de equivalencia si es reflexiva, simétrica y transitiva.*

Es muy común usar el símbolo "$\sim$" para denotar relaciones de equivalencia, en vez del símbolo $\mathcal{R}$.

Ejemplo 2.2.14 *Sean $E = \{1, 2, 3\}$, y $R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3)\}$.*
En un ejemplo previo vimos que esta relación es reflexiva, simétrica y transitiva, y por lo tanto de equivalencia.

Ejemplo 2.2.15 *Sea E cualquier conjunto, $R = \{(a, a) : a \in E\}$. Esto es, $a\mathcal{R}b$ sii $a = b$. Entonces $\mathcal{R}$ es una relación de equivalencia. De hecho, es la relación de equivalencia más simple que existe.*

Ejemplo 2.2.16 *En $E = \mathbb{N}$ defina la relación*

$$n \sim m \Leftrightarrow n + m \text{ es par.}$$

Note que si $n \sim m$ y n es par, entonces m es par, y viceversa. Esto demuestra que en este caso, $n \sim m$ sii n y m tienen la misma "paridad". Dicho de otra forma, todos los números pares se relacionan entre sí, lo mismo que todos los impares. Dejamos al lector la tarea de convencerse de que esta relación es de equivalencia.

Ejemplo 2.2.17 *En $E = \mathbb{N} \times \mathbb{N}$ defina la relación:*

$$(m, n) \sim (p, q) \Leftrightarrow m + q = n + p.$$

Veamos que esta es una relación de equivalencia:

Reflexividad: Dado que $m + n = n + m$, tenemos que $(m, n) \sim (m, n)$, para cada elemento $(m, n) \in \mathbb{N} \times \mathbb{N}$.
Simetría: Si $(m, n) \sim (p, q)$ tenemos $m + q = n + p$, o lo que es lo mismo, $p + n = q + m$. Esto significa que $(p, q) \sim (m, n)$.
Transitividad: Si $(m, n) \sim (p, q)$ y $(p, q) \sim (r, s)$, tenemos

$$m + q = n + p, \quad p + s = q + r.$$

Luego $m + q + p + s = n + p + q + r$, de donde $m + s = n + r$. Esto significa $(m, n) \sim (r, s)$.

Ejemplo 2.2.18 *En $E = \mathbb{Z}$ se define la relación*

$$m \sim n \Leftrightarrow m - n \text{ es múltiplo de } 5.$$

La reflexividad y simetría se dejan como ejercicio. Para la transitividad suponga que $m \sim n$ y $n \sim p$. Entonces $m - n = 5k$ y $n - p = 5l$, donde $k, l \in \mathbb{Z}$. Luego

$$m - p = (m - n) + (n - p) = 5(k + l),$$

y como $k + l \in \mathbb{Z}$, esto implica $m \sim p$.

Clases de equivalencia

La idea de introducir una relación de equivalencia es, como dijimos, identificar elementos que son equivalentes entre sí. Es por eso natural pensar en los conjuntos formados por esos elementos, los cuales llamaremos clases de equivalencia. Identificar elementos equivalentes significa considerar las clases como elementos de un nuevo conjunto, llamado conjunto cociente. Más precisamente, dada una relación de equivalencia sobre el conjunto E, y dado $a \in E$, definimos la clase de equivalencia de a como

$$[a] = \{x \in E : a \sim x\}.$$

La mejor manera de aclarar este concepto es mediante los ejemplos. Retomemos los ejemplos estudiados arriba.

Ejemplo 2.2.19 *Sea $E = \{1, 2, 3\}$, $R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3)\}$.*
En este caso $[1] = \{1, 2\} = [2]$, $[3] = \{3\}$.

Ejemplo 2.2.20 *Sea E cualquier conjunto, y $\mathcal{R}$ la relación de igualdad en E. Entonces $[a] = \{a\}$, para todo $a \in E$.*

Ejemplo 2.2.21 *Considere $E = \mathbb{N}$ con la relación*

$$n \sim m \Leftrightarrow n + m \text{ es par.}$$

Ahora tenemos

$$[0] = \{n \in \mathbb{N} : n \text{ es par }\} = [2] = [4] = etc.,$$

mientras que

$$[1] = \{n \in \mathbb{N} : n \text{ es impar }\} = [3] = [5] = etc.$$

En otras palabras, solo hay dos clases, la formada por los pares y la formada por los impares.

Ejemplo 2.2.22 *Para la relación definida por*

$$(m,n) \sim (p,q) \Leftrightarrow m+q = n+p,$$

en $\mathbb{N}\times\mathbb{N}$*, tenemos:*

$$\begin{aligned} [(1,0)] &= \{(p,q)\in\mathbb{N}\times\mathbb{N} : 1+q=p\} = \{(q+1,q) : q\in\mathbb{N}\}, \\ [(0,1)] &= \{(p,q)\in\mathbb{N}\times\mathbb{N} : q=p+1\} = \{(p,p+1) : p\in\mathbb{N}\}. \end{aligned}$$

En general,

$$\begin{aligned} [(m,0)] &= \{(p,q)\in\mathbb{N}\times\mathbb{N} : m+q=p\} = \{(q+m,q) : q\in\mathbb{N}\}, \\ [(0,n)] &= \{(p,q)\in\mathbb{N}\times\mathbb{N} : q=n+p\} = \{(p,p+n) : p\in\mathbb{N}\}. \end{aligned}$$

El lector puede convencerse de que éstas son todas las clases de equivalencia para esta relación.

Ejemplo 2.2.23 *Considere el conjunto E formado por todas las palabras del idioma español. Sobre E definimos la siguiente relación $\mathcal{R}$: una palabra x está relacionada con una palabra y si comienzan con la misma letra. Resulta inmediato que esta relación es de equivalencia en el conjunto E.*
Note por ejemplo que:

$$[aro] = \{x\in E : x \text{ comienza con } a\}, \quad [bola] = \{x\in E : x \text{ comienza con } b\}$$

y similarmente

$$[zorra] = \{x\in E : x \text{ comienza con } z\}.$$

Es claro que la relación $\mathcal{R}$ define 27 clases de equivalencia.

Ejemplo 2.2.24 *Para la relación definida en $E=\mathbb{Z}$ por*

$$m\sim n \Leftrightarrow m-n \text{ es múltiplo de } 5,$$

tenemos

$$\begin{aligned} [0] &= \{n\in\mathbb{Z} : n \text{ es un múltiplo de } 5\} = \{\ldots,-5,0,5,10,\ldots\}, \\ [1] &= \{n\in\mathbb{Z} : n-1 \text{ es múltiplo de } 5\} = \{\ldots,-4,1,6,11,\ldots\}, \\ [2] &= \{n\in\mathbb{Z} : n-2 \text{ es múltiplo de } 5\} = \{\ldots,-3,2,7,12,\ldots\}, \\ [3] &= \{n\in\mathbb{Z} : n-3 \text{ es múltiplo de } 5\} = \{\ldots,-2,3,8,13,\ldots\}, \\ [4] &= \{n\in\mathbb{Z} : n-4 \text{ es múltiplo de } 5\} = \{\ldots,-1,4,9,14,\ldots\}. \end{aligned}$$

Note que $[5]=[0]$, $[-1]=[4]$, *etc., así que hay exactamente cinco clases de equivalencia.*

Es importante observar que, por simetría, en la definición de clase puede escribirse también $x\sim a$ en vez de $a\sim x$. A continuación enumeramos algunas propiedades de las clases de equivalencia:

1. Para $a \in E$ tenemos $a \in [a] \subseteq E$. En particular $[a] \neq \emptyset$.

2. Si $b \in [a]$ entonces $[b] = [a]$.

   En efecto, como $b \in [a]$ tenemos que $a \sim b$. Luego, para $x \in [b]$ tenemos $a \sim b \wedge b \sim x$, y por transitividad se sigue que $a \sim x$, esto es $x \in [a]$. De la misma forma se demuestra que $x \in [a]$ implica $x \in [b]$.

   Nota: Dada una clase de equivalencia C, con $a \in C$, cuando escribimos $C = [a]$ decimos que estamos usando el elemento a como representante de dicha clase. Cualquier $b \in C$ puede usarse como representante de C, de acuerdo con la propiedad anterior.

3. Si $[a] \neq [b]$, entonces $[a] \cap [b] = \emptyset$.

   En efecto, si existiera $c \in [a] \cap [b]$, entonces por la propiedad 2 tendríamos $[a] = [c] = [b]$.

4. La unión de todas las clases de equivalencia determinadas por la relación $\sim$, es todo E. Esto es
$$\bigcup_{a \in E} [a] = E.$$
   En efecto, como $[a] \subseteq E$, para todo $a \in E$, tenemos "$\subseteq$". Por otro lado, si $b \in E$, tenemos $b \in [b]$, con lo que $b \in \bigcup_{a \in E} [a]$, y esto nos da "$\supseteq$".

Definición 2.2.6 *Un conjunto P de partes de E se llama una partición de E si:*

1. *E es la unión de los subconjuntos pertenecientes a P*

2. *Si $A \in P$, $B \in P$ y $A \neq B$ entonces $A \cap B = \varnothing$. Es decir, dos elementos distintos de P son disjuntos*

3. *$\varnothing \notin P$.*

De acuerdo con lo anterior, las clases de equivalencia de $\sim$ forman una partición del conjunto E.

Conjunto cociente

Volviendo a la idea de considerar todos los elementos de una clase como uno solo, vamos a definir el conjunto formado por todas las clases de una relación de equivalencia. A este conjunto le llamaremos el *conjunto cociente* definido por E y $\sim$, y lo denotamos $E/\sim$. Así
$$E/\sim = \{[a] : a \in E\}.$$

Retomemos los ejemplos de la sección anterior.

Ejemplo 2.2.25 *Si* $E = \{1, 2, 3\}$, $R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3)\}$, *tenemos*

$$E/\mathcal{R} = \{[1], [3]\} = \{\{1, 2\}, \{3\}\}.$$

Ejemplo 2.2.26 *Sea* E *cualquier conjunto, y* $\mathcal{R}$ *la relación de igualdad en* E. *Entonces*

$$E/\mathcal{R} = \{\{a\} : a \in E\}.$$

Ejemplo 2.2.27 *En* $E = \mathbb{N}$, *con la relación*

$$n \sim m \Leftrightarrow n + m \text{ es par},$$

se tiene $E/\sim = \{[0], [1]\} = \{P, I\}$, *donde* P *es el conjunto de los pares, e* I *es el conjunto de los impares.*

Ejemplo 2.2.28 *Para la relación definida por*

$$(m, n) \sim (p, q) \Leftrightarrow m + q = n + p,$$

en $\mathbb{N} \times \mathbb{N}$, *tenemos*

$$E/\sim = \{[(m, 0)] : m \in \mathbb{N}\} \cup \{[(0, n)] : n \in \mathbb{N}\}.$$

Para $n \neq 0$ *denotamos* $+n = [(n, 0)]$ *y* $-n = [(0, n)]$, *y también* $\mathbf{0} = [(0, 0)]$. *Así, el conjunto* $E/\sim$ *puede ser identificado con* $\mathbb{Z}$. *Esta idea puede ser usada para dar una construcción del conjunto* $\mathbb{Z}$ *de números enteros, a partir del conjunto* $\mathbb{N}$ *de números naturales.*

Ejemplo 2.2.29 *Para la relación definida en* $E = \mathbb{Z}$ *por*

$$m \sim n \Leftrightarrow m - n \text{ es múltiplo de } 5,$$

tenemos

$$E/\sim = \{[0], [1], [2], [3], [4]\}.$$

Este conjunto se denota por $\mathbb{Z}_5$.

Ejemplo 2.2.30 *En general, dado un entero* $p > 0$, *se define la relación* $\mathcal{R}$ *en* $\mathbb{Z}$ *mediante*

$$m\mathcal{R}n \Leftrightarrow m - n \text{ es múltiplo de } p.$$

Esta relación resulta de equivalencia, y el conjunto cociente $\mathbb{Z}/\mathcal{R}$ *se denota por* $\mathbb{Z}_p$.

Las ideas expresadas en estos ejemplos, pueden ser usadas para construir los conjuntos numéricos. Esto lo haremos en la segunda parte, mientras en el capítulo siguiente estudiaremos otro tipo especial de relaciones binarias, el cual posiblemente le es familiar al lector.

2.3 Ejercicios

1. En cada caso, dé un ejemplo de relación binaria con las propiedades enunciadas:

   (a) Que sea reflexiva pero no simétrica, ni transitiva ni antisimétrica.

   (b) Que sea reflexiva y simétrica, pero no transitiva.

   (c) Que sea reflexiva y transitiva, pero no simétrica.

2. ¿Qué se puede decir de una relación $\mathcal{R} = (A, A, R)$ que sea reflexiva, simétrica y antisimétrica?

3. En $\mathbb{N}$ se define la relación $\mathcal{R}$ mediante:

   $$n\mathcal{R}m \text{ sii } n \leq m \leq n+2.$$

   ¿Es esta relación de orden?, ¿de equivalencia?

4. En $\mathbb{Z}$ se define la relación $n \sim m$ sii $n-m$ es múltiplo de 7. Demuestre que esta relación es de equivalencia, y halle $\mathbb{Z}/\sim$.

5. En general, si $p \in \mathbb{N}^*$, se define la relación $\mathcal{R}$ en $\mathbb{Z}$ por:

   $$n\mathcal{R}m \Leftrightarrow n - m \text{ es múltiplo de } p.$$

   Demuestre que $\mathcal{R}$ es de equivalencia, y que $\mathbb{Z}/\mathcal{R}$ tiene exactamente p elementos.

6. En $E = \mathbb{R}$ se define la relación: $x\mathcal{R}y \Leftrightarrow x - y$ es racional. ¿Es esta relación de equivalencia? Justifique su respuesta. ¿Qué pasa si se cambia "racional" por "irracional"?

7. Sea $E = \mathbb{N} \cup \{\omega\}$, donde $\omega \notin \mathbb{N}$. En E se define la relación $\mathcal{R}$ de gráfico $R = G \cup \{(n, \omega) : n \in E\}$, donde R es el gráfico de la relación $\leq$ en $\mathbb{N}$. En otras palabras, $\preceq$ es una extensión de $\leq$, imponiendo que $n \preceq \omega$ para todo $n \in E$. Demuestre que $\preceq$ es una relación de orden total en E (satisface la ley de tricotomía).

8. En $E = \mathbb{R}$ se define la relación $\mathcal{R}$ mediante: $x\mathcal{R}y \Leftrightarrow x \cdot y > 0$. Demuestre que esta relación no es de equivalencia. Sin embargo, si se cambia $\mathbb{R}$ por $\mathbb{R}^*$, la relación resultante sí es de equivalencia. Halle $\mathbb{R}^*/\mathcal{R}$.

9. En $\mathbb{Z}$ se definae la relación $\mathcal{S}$ por:

   $$a\mathcal{S}b \Leftrightarrow a^2 - b^2 = a - b.$$

   Demuestre que esta relación es de equivalencia. ¿Cuantos elementos tiene cada clase de equivalencia?

10. Repita el ejercicio anterior, cambiando $a^2 - b^2$ por $a^3 - b^3$, y luego por $a^4 - b^4$.

11. En $\mathbb{R}^2$ se define la relación $\prec$ por:

$$(a,b) \prec (c,d) \Leftrightarrow (a \leq c \text{ y } b \leq d)\,.$$

Demuestre que esta relación es de orden. Para (a,b) dado, dibuje el conjunto de puntos (x,y) tales que $(a,b) \prec (x,y)$. ¿Es esta relación de orden total?

12. Sea $\mathcal{R} = (A, A, R)$ una relación reflexiva. Se define $\mathcal{S}$ mediante:

$$a\mathcal{S}b \text{ sii } (a\mathcal{R}b \vee b\mathcal{R}a)$$

Demuestre que $\mathcal{S}$ es reflexiva y simétrica, pero no necesariamente transitiva (aunque $\mathcal{R}$ lo sea).

13. En $\mathbb{R}$ sea $\mathcal{T}$ la relación definida por:

$$x\mathcal{T}y \Leftrightarrow x \text{ y } y \text{ tienen la misma parte entera.}$$

(a) Trace la gráfica de $\mathcal{T}$ en un plano cartesiano.

(b) ¿Es $\mathcal{T}^{-1} = \mathcal{T}$? Justifique.

(c) Calcule $\mathcal{T}^{-1} \circ \mathcal{T}$.

14. Sean $\mathcal{R} = (A, B, R)$ y $\mathcal{S} = (B, C, S)$.

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

(b) Si $\mathcal{T} = (C, D, T)$, demuestre que $(\mathcal{T} \circ \mathcal{S}) \circ \mathcal{R} = \mathcal{T} \circ (\mathcal{S} \circ \mathcal{R})$.

15. Sea $\leq$ es una relación de orden sobre E, y sea $A \subseteq E$. Se diceque $a \in A$ es un elemento maximal de A, si para cada $x \in A$ se tiene

$$a \leq x \Rightarrow a = x.$$

Es decir, no hay elementos en A que sean "mayores que a". Dé ejemplos en los que haya varios elementos maximales, pero no haya máximo.

Capítulo 3

Funciones

3.1 Introducción histórica sobre el concepto de función

La idea de relacionar cantidades es tan añeja como la matemática misma. Sin embargo, resulta de sumo interés explorar la trayectoria seguida por esta noción vaga hasta la concepción conjuntista de hoy en día. También, sería muy instructivo analizar las diferentes concepciones de la noción de función y su papel preponderante en el desarrollo del análisis matemático moderno. Sin embargo, no es el momento para dicho análisis y tan solo se harán referencias muy superficiales.

3.1.1 Los babilonios

La primera etapa en el desarrollo del concepto de función, se puede situar en la antigüedad (ver [5]). En esta época, una de las civilizaciones mesopotámicas, que conocemos como babilónica (2000 A.C-600A.C), usó fuertemente en sus cálculos tablas sexagesimales de cuadrados y raíces cuadradas, de cubos y raíces cúbicas, etc; tablas cuyo interés era ser utilizadas en astronomía y, particularmente para realizar compilaciones de fenómenos importantes relacionados con el sol, la luna y los planetas.

Los matemáticos babilonios, estudiaron problemas de variaciones tales como la luminosidad de la luna en intervalos iguales de tiempo, o los períodos de visibilidad de un planeta dependiendo del ángulo formado con el sol.

Los babilonios no utilizaron letras para representar cantidades variables, pero sí incorporaron los mismos términos longitud, área, anchura y volumen para tal fin.

No se puede asegurar que la noción general de función estuviera presente en las tablas elaboradas por los babilonios, de hecho algunos investigadores sostienen que en dichas tablas no subyacía una idea general de función y, otros, por el contrario, sostienen que había una similitud entre estas correspondencias tabulares y la idea de función, al menos en cuanto a una relación general que asocia elementos de dos conjuntos. Como dicen algunos investigadores,

había un "instinto de funcionalidad" entre los matemáticos y astrónomos babilonios aunque estaba muy distante de la noción de función.

3.1.2 Los griegos

Las ideas de cambio y de cantidad variable no eran ajenas al pensamiento griego. Los intentos, atribuidos a los pitagóricos, para establecer las leyes de la acústica son característicos de la búsqueda de interdependencia cuantitativa entre cantidades físicas. Si bien se puede afirmar que en los griegos existía una idea muy primitiva de función, también es cierto que los filósofos griegos de la época consideraban el cambio y el movimiento como algo fuera de la matemática. Probablemente, por esta razón la idea de cambio cuantitativo y la de movimiento local, ambas presentes en la Física de Aristóteles, no desembocaron en una noción más abstracta de cantidad variable, pues no fueron objeto de estudio por parte de los matemáticos griegos.

Si bien las ideas presentes en la definición de la espiral de Arquímedes o de la hélice cilíndrica de Apolonio fueron muy importantes en el desarrollo de la idea de funcionalidad, lo cierto es que la matemática griega en su conjunto con sus procedimientos de determinación y cálculo de límites particulares no condujeron a una formulación explícita de las nociones de sucesión, de variable y de "infinitamente pequeño".

Se debe admitir que en la antigüedad, no hubo una idea general de funcionalidad.

3.1.3 La edad media

Durante esta época, se dio un fuerte impulso a la búsqueda de una explicación racional de todos los fenómenos. Emerge así la matemática como un modelo de ciencia racional. Las escuelas de filosofía natural de Oxford y París, que florecen en el siglo XVI, comenzaron a considerar la matemática como un instrumento idóneo para el conocimiento de los fenómenos naturales.

Se busca cuantificar ciertas cualidades o fenómenos como el calor, la densidad, la velocidad y otros. Estos fenómenos, llamados cualidades o formas en la terminología de Aristóteles, son abordados desde la perspectiva no solo del por qué suceden los cambios, si no fundamentalmente cómo suceden.

Las cualidades o formas son fenómenos que pueden poseer muchos grados de intensidad y que, de manera general, cambian continuamente entre ciertos límites dados.
Una forma era cualquier cantidad o cualidad variable en la naturaleza. La intensidad o latitud de una forma era el valor numérico que había que asignarle, en relación con otra forma invariable que llamaban extensión o longitud.

En esta época, se rompe con la concepción estática presente en el pensamiento griego e irrumpe el movimiento como objeto de estudio de la matemática.

Nicolás Oresme (1320-1382) señalaba "toda cosa medible, excepto los números, se puede imaginar como una cantidad continua". En palabras de Luisa Ruiz Higueras (ver [13]) "A Nicolás Oresme se le ocurrió una idea brillante. ¿por qué no hacer un dibujo o una gráfica que represente el modo en que las cosas varían ?. Aquí vemos una manifestación primitiva de lo que ahora llamamos representación gráfica de funciones."

Las nociones de movimiento, de velocidad, de aceleración, de instantaneidad estaban presentes en las escuelas de Oxford y París. Pero además, algo muy importante, distinguían el movimiento local uniforme del movimiento uniformemente acelerado.

Para el caso de la velocidad, Oresme dio una demostración geométrica del siguiente resultado: *en un tiempo dado, un móvil recorre con movimiento uniformemente acelerado la misma distancia que otro móvil con velocidad constante e igual al promedio entre las velocidades extremas del primero.*

Oresme recurre a la representación gráfica, una de las primeras, de la relación funcional que liga el tiempo y la velocidad.

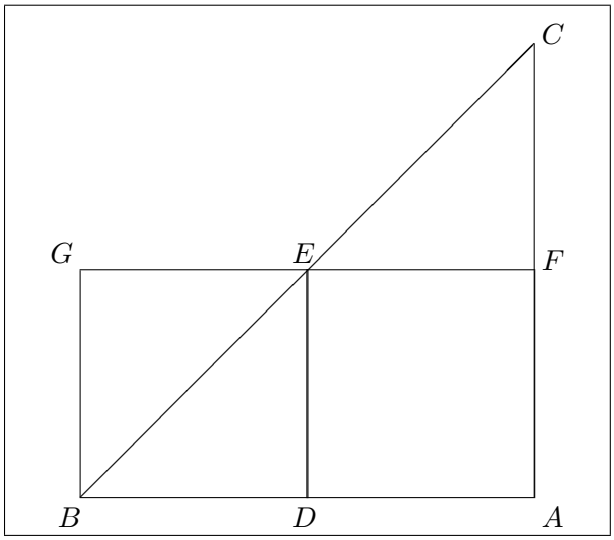


Figura 3.1: Interpretación del argumento de Oresme.

Él sitúa los tiempos sobre una línea horizontal AB y las velocidades instantáneas paralelamente a la línea perpendicular AC, encima de los puntos correspondientes de AB.

Si D es el punto medio de AB y F el punto medio de AC, el área del rectangulo AFGB mide el espacio recorrido por el segundo móvil, puesto que DE×AB es el producto de la velocidad por el tiempo. El área del triángulo BAC da la distancia recorrida por el primer móvil. Las dos áreas son iguales.

Este resulta un momento importante en el desarrollo teórico del concepto de función, pues se comienza a considerar las leyes de la naturaleza como leyes de tipo funcional y se producen intercambios entre el pensamiento matemático y las consideraciones cinemáticas.

3.1.4 Desarrollo del algebra literal y simbólica

Al parecer, los siglos XV y XVI no fueron muy prolíferos en resultados e ideas matemáticas novedosas. Dos aspectos a señalar son: la creación y desarrollo del álgebra literal y simbólica, y la consolidación de la trigonometría como una rama particular de la matemática.
Es indudable, que estos dos aspectos contribuyeron significativamente al desarrollo del concepto de función; sobre todo a los aspectos simbólicos y al estudio de las funciones trigonométricas. Este elemento permite, después de Viète (1591), una notación resumida y manejable de una expresión algebraica conteniendo cantidades desconocidas y coeficientes arbitrarios. Si bien es cierto el simbolismo de Viète sufrió enmiendas y transformaciones muy rápidamente, el mismo contribuyó a un notable avance del cálculo matemático.

Este período, se caracteriza por iniciar el paso del estudio del movimiento al estudio de las trayectorias. Aparece una concepción de las matemáticas como lenguaje que permite expresar la realidad física de la naturaleza.

En esta época, destacaron matemáticos como el alemán Müller (1436-1476), más conocido como Regiomontano, y Galileo (1564-1642). Como aporte al desarrollo del concepto de función, destaca el trabajo de Galileo orientado a la búsqueda de resultados y relaciones provenientes de la experiencia más que de la abstracción. Estudió el movimiento, la velocidad, la aceleración y la distancia recorrida y buscó ligarlos mediante leyes sustentadas en la experiencia y la observación. Galileo también estudió las trayectorias de proyectiles en movimiento.

3.1.5 Siglo XVII

A principios de este siglo, la formulación de las leyes de Kepler sobre las trayectorias elípticas de los planetas, orienta el interés matemático hacia los problemas de cálculo y el estudio de trayectorias.

La mayoría de las funciones introducidas en esta época fueron estudiadas, en un primer momento, como curvas, las cuales eran consideradas como trayectorias de puntos en movimiento.

El desarrollo del álgebra literal simbólica y la madurez del concepto de número (a finales del siglo XVI abarcaba los reales, los imaginarios y los complejos) contribuyeron de manera significativa al desarrollo de la teoría de funciones.

Unos veinte años después que John Napier (1550-1617), entre otros matemáticos de la época, introdujeran la función logaritmo, Fermat (1601-1665) y Descartes (1586-1650) aplican el álgebra simbólica a la geometría y desarrollan el método analítico para el estudio de funciones.

El objetivo de Descartes, contenido en su geometría de 1637, era reducir la solución de todos los problemas algebraicos que requerían de resolución de ecuaciones, a procedimientos estándares para construir sus raíces reales mediante las coordenadas de sus puntos de intersección de curvas planas de grado lo más bajo posible. Él distinguía curvas geométricas y curvas mecánicas y centró su atención en las primeras; es decir en aquellas curvas donde las dos coordenadas x e y están relacionadas por una ecuación algebraica $P(x, y) = 0$, y que hoy día se conocen como curvas algebraicas.

La introducción en geometría del método de las coordenadas, también conocido como la aplicación del álgebra a la geometría, y más tarde como geometría analítica, permitió la traducción de todo problema de la geometría plana en un problema equivalente de álgebra; esto debido a que los objetos y relaciones de la axiomática de Hilbert se podían interpretar como objetos y relaciones de la teoría de los números reales.

El método de coordenadas fue factor fundamental para la formulación de la noción de función y el cálculo infinitesimal.

Aquí se expone por primera vez la idea de que una ecuación en x e y es una forma de introducir una relación de dependencia funcional, entre cantidades variables, en el sentido de que una de ellas permite determinar la otra. Esta idea de introducir la funcionalidad por medio de ecuaciones significó un momento importante en el desarrollo matemático. Este método de representar funciones, muy pronto se desligó de su campo de origen, la geometría analítica, para extenderse a otras ramas de la matemática, particularmente al análisis infinitesimal.

La idea de Descartes de restringir la noción de función únicamente a las expresiones algebraicas, fue una limitación que no soportó el peso del descubrimiento de los matemáticos de la generación siguiente (Wallis, Mercator, James Gregory, Newton): el desarrollo de funciones en series de potencias.

Nicolas Mercator encuentra el área de una hipérbola reduciendo a una serie geométrica la expresión $\frac{1}{1+x}$, y luego integrándola término a término según el método de Wallis. Este método tuvo gran suceso y numerosos matemáticos trabajaron e hicieron grandes aportes apollados en el mismo. Sin embargo, más sobresaliente fue Newton quien desarrolla en serie de potencias racionales, las funciones $(1 + x)^{-1}$, $\operatorname{sen} x$, $\cos x$, y series análogas para los arcos de elipses.

La mejor definición explícita del concepto de función, hasta ese momento, fue dada por James Gregory en 1667; él define una función como una cantidad obtenida a partir de otras cantidades por una sucesión de operaciones algebraicas, o como dice él mismo, por no importa cual operación imaginable. No obstante, el contexto deja entrever que es necesario agregar a las cinco operaciones algebraicas (adición, sustracción, multiplicación, división, extracción de raíz) una sexta operación definida aproximadamente como un paso al límite.

La idea de usar procedimientos algorítmicos infinitos para la definición de función, en particular el desarrollo en series de potencias enteras, fue de incalculable valor en el trabajo de extender este concepto.

3.1.6 El papel preponderante del concepto de función

Hasta finales del siglo XVII, la noción de función sigue siendo muy vaga. Sin embargo, a partir de este momento, con matemáticos como Leibnitz y Jean Bernoulli, el concepto de función comienza a tomar un sesgo más analítico, aunque sigue siendo vago. Una precisión significativa, se logra con los trabajos de Euler (1707- 1783).

El nacimiento del cálculo infinitesimal sucitó un gran entusiasmo entre los matemáticos de la época y planteó la necesidad de clarificar y precisar una serie de conceptos, entre ellos la noción de "infinitamente pequeño".

El siglo XVIII, en cuanto a la matemática se refiere, arranca alrededor de 1730 con los primeros trabajos de Euler, considerado el gigante del siglo, los de Daniel Bernoulli (1700-1782). Comienza un momento nuevo en el desarrollo histórico de la matemática, que se ve marcado por un distanciamiento entre filósofos y matemáticos y una especialización creciente del trabajo científico.

La primera consideración de una función como expresión analítica se debe a Jean Bernoulli en 1718,: "llamamos función de una magnitud variable a una cantidad compuesta de cualquier manera que sea de esta magnitud variable y de constantes".

Euler, y otros matemáticos contemporáneos, al no contar con el concepto de límite y no poder superar los problemas generados por la utilización de los algoritmos infinitos, considera el cálculo infinitesimal como una extensión del álgebra, agregando la diferenciación y la integración. Euler se proponía estudiar las funciones elementales y sus propiedades recurriendo al cálculo algebraico. Él utiliza las manipulaciones algebraicas sobre expresiones infinitas (series, productos infinitos, fracciones continuas, etc.) de una manera puramente formal; es decir sin ninguna preocupación por aspectos de convergencia.

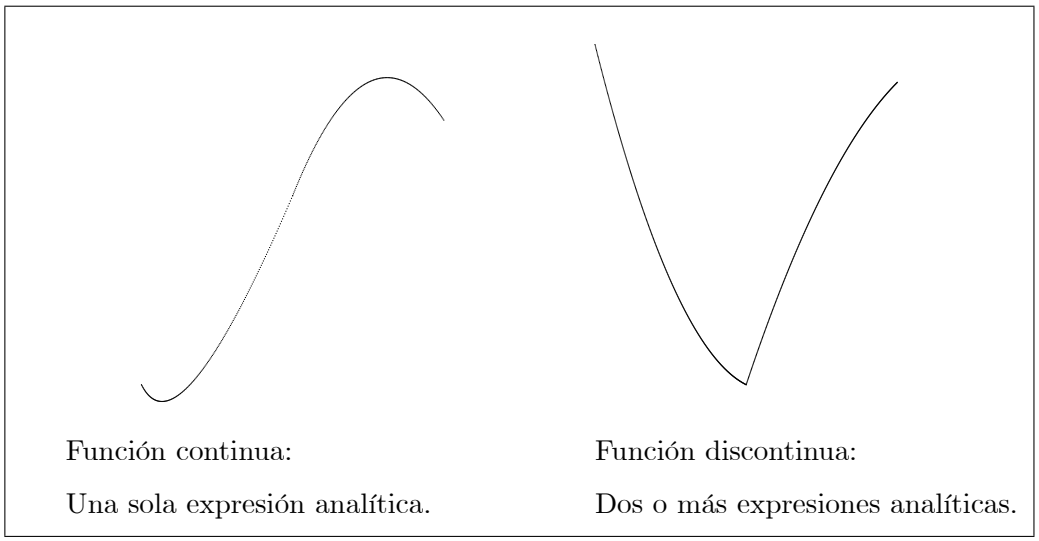
El libro escrito por Euler "Introductio in analysin infinitorum" se constituye en el primer tratado en donde el concepto de función está a la base de la construcción matemática.

Euler define una función de una cantidad variable como "una expresión analítica compuesta de una manera cualquiera de esta cantidad variable y de números o cantidades constantes". Es decir, para Euler, una función es una combinación arbitraria de operaciones tomadas del conjunto de operaciones y de modos de cálculo conocidos en su tiempo y aplicables a los números: operaciones clásicas del álgebra, exponencial, logaritmo, etc; algunas de estas operaciones pueden ser iteradas de manera ilimitada. Esta manera de construir expresiones analíticas, permite a Euler hacer una clasificación de las mismas en tres grupos principales: algebraicas-trascendentes, uniformes-multiformes, explícitas-implícitas.

Resulta importante mencionar que las funciones consideradas en la obra de Euler, es decir las definidas por una sola expresión analítica finita o infinita, son llamadas funciones continuas tanto por Euler como por los otros matemáticos del siglo XVIII.

Posteriormente, Euler desarrolló aplicaciones del concepto de función a la geometría; introduciendo así lo que él llamó funciones mixtas o irregulares y que requieren diferentes

expresiones analíticas en diferentes dominios. Así, la continuidad según Euler, expresa al carácter inmutable de la fórmula que define la función para todos los valores de la variable.



Función continua:

Una sola expresión analítica.

Función discontinua:

Dos o más expresiones analíticas.

Por otro lado, se debe señalar que el desarrollo de la teoría de ecuaciones diferenciales y del cálculo de variaciones en el siglo XVIII, constituyen un testimonio del desplazamiento del concepto de número al de función como objeto matemático central y del cual hablaba J.Hadamard.

Euler, seguido de otros matemáticos contemporáneos, rompe con el lenguaje, la escogencia y la organización de los matemáticos que le preceden, y es el concepto de función el que pasa a ser la base del edificio matemático.

Posterior a Euler, y dentro de la perspectiva formalista, aparece Lagrange con su esfuerzo por dotar a la matemática de bases rigurosas sustentadas en una sistematización de las prácticas del análisis algebraico del siglo XVIII. Esta tentativa de Lagrange se apoya sobre la teoría del desarrollo de funciones en series enteras. Lagrange maneja una noción de función que es la noción de función continua de Euler. Lagrange no tuvo éxito en su empresa, pues excluyó de partida toda consideración sobre límite dentro de su teoría. En el último decenio del siglo, un gran pesimismo sobre el futuro se apoderó de los matemáticos. Lagrange, dijo al respecto, que eran pocos los progresos que se podían lograr con el estado actual del análisis.

Muy importante de resaltar es el hecho que la concepción algebraica y formal de las funciones, que durante mucho tiempo sirvió de estímulo para el desarrollo del análisis, se convertía en un verdadero freno para la búsqueda de nuevos resultados.

El atascamiento que embargaba el análisis, se ve truncado por dos líneas de trabajo desarrolladas por matemáticos de la generación siguiente.

Por un lado, Gauss, Cauchy, Bolzano y Abel, desarrollan trabajos en donde había una preocupación especial por el rigor y los fundamentos, y que desembocan en la clasificación y presición de una serie de conceptos centrales para el análisis: el infinitamente pequeño, límite, continuidad, convergencia, etc. Por otro lado, no de manera independiente, Fourier, Lejeune, Dirichlet y Riemann toman como base de su trabajo los problemas planteados por la física y la representación de las funciones mediante series trigonométricas.

3.1.7 Siglo XIX: La noción general de función

Después de Fourier, Cauchy, Dirichlet y Riemann, se puede decir que la noción de función alcanzó su plena madurez. Por ejemplo, Dirichlet, en 1837 dio la siguiente definición: *si una variable y está relacionada con otra variable x de tal manera que siempre que se atribuya un valor numérico a x hay una regla según la cual queda determinado un único valor de y, entonces se dice que y es una función de la variable independiente x.*

Más tarde, en 1858, Riemman formuló la siguente definición: *se dirá que y es función de x si a todo valor bien determinado de x corresponde un valor bien determinado de y cualquiera que sea la forma de la relación que une a x e y.*

La profundización de las nociones de función y de continuidad, se ven acompañadas por la construcción de funciones cada vez más y más patológicas. Algunas de estas eran construidas, como contraejemplos a conjeturas que gravitaban en el quehacer matemático en ese momento. Una de estas construcciones famosas fue la de Weierstrass, quien construye una función continua en un cierto intervalo y no derivable en ningún punto de ese intervalo.

Una transición del viejo concepto de función a la versión acabada, se marca por la utilización de algoritmos infinitos para representar y aproximar funciones cada vez más generales. En el siglo XIX, las series de Taylor y las series de Fourier son los dos algoritmos más importantes.

Este rápido seguimiento al concepto de función en su desarrollo histórico, lo cerramos diciendo que el siglo XX ve aparecer el concepto de función como terna y como aspecto central de las matemáticas. Al respecto, Spivak dice: "el concepto más importante de las matemáticas es, sin duda, el de función". En casi todas las ramas de la matemática actual, la investigación se centra en el estudio de funciones. No ha de sorprender, por lo tanto, que el concepto de función haya llegado a definirse con una gran generalidad.

Hoy día una definición típica en un texto universitario es:

Sean A,B dos conjuntos no vacíos. Una función f definida en el conjunto A y con valores en B, es una ley mediante la cual se hace corresponder a cada elemento de A un único elemento de B.
La definición rigurosa será presentada a continuación, mediante el uso de relaciones binarias.

3.2 Las funciones de hoy en día

3.2.1 Definición y ejemplos

Una función f de un conjunto A en otro conjunto B, es una relación binaria $f = (A, B, G)$ que asocia a cada elemento en A, un único elemento en B. Más precisamente, la relación binaria f se llama función si:

$$\forall a \in A, \exists\, b \in B \text{ único, tal que } afb.$$

Cuando a se relaciona con b, esto es cuando afb, se dice que b es la imagen de a, y se escribe $f(a) = b$. En tal caso también se dice que a es una pre-imagen de b. Note que pueden existir varias pre-imágenes para un mismo elemento $b \in B$, y también puede que algunos elementos de B no tengan pre-imagen alguna. Pero cada elemento de A tiene exactamente una imagen. Al conjunto A se le llama el dominio de f, y al conjunto B codominio de f. El gráfico G de f satisface

$$G = \{(a, b) \in A \times B : b = f(a)\} = \{(a, f(a)) : a \in A\} \subseteq A \times B.$$

Escribimos $f : A \to B$ para expresar que f es una función de A en B. Es importante insistir en que los conjuntos A y B son parte de la función f, y en ese sentido, si se cambia A o B, obtenemos una función distinta, o incluso podríamos obtener una relación que no es función.

Ejemplo 3.2.1 *Sean* $A = \{1, 2, 3\}$, $B = \{4, 5, 6\}$ *y* $C = \{4, 5\}$, *y sea*

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

Entonces $f = (A, B, G)$ *y* $g = (A, C, G)$ *son funciones distintas, dado que* $B \neq C$. *Note que* $f(a) = g(a)$ *para todo* $a \in A$, *pero esto no implica* $f = g$. *Note que* $6 \in B$ *no tiene pre-imágenes bajo* f. *Por su parte* $4 \in B \cap C$ *tiene dos pre-imágenes bajo* f, *lo mismo que bajo* g.

Ejemplo 3.2.2 *Con* A *y* B *como en el ejemplo anterior, sea* $G = \{(1, 4), (2, 5)\}$. *Entonces* $\mathcal{R} = (A, B, G)$ *no es función, pues* $3 \in A$ *no tiene imagen. Sin embargo, si cambiamos* A *por* $\{1, 2\}$, *obtenemos la función* $f = (\{1, 2\}, B, G)$.

Ejemplo 3.2.3 *Si* $A = B = \mathbb{N}$ *y* $G = \left\{(n, m) \in \mathbb{N} \times \mathbb{N} : n = m^2\right\}$, *entonces* $\mathcal{R} = (\mathbb{N}, \mathbb{N}, G)$ *no es función, pues por ejemplo* $n = 5$ *no tiene imagen. Si en cambio*

$$G = \left\{(n, m) \in \mathbb{N} \times \mathbb{N} : n^2 = m\right\}$$

Entonces $f = (\mathbb{N}, \mathbb{N}, G)$ *sí es función.*

En muchos casos, se puede definir una función dando su dominio, su codominio, y una fórmula para calcular $f(a)$, para cada $a \in A$. En tales casos debe tenerse cuidado de que dicha fórmula genere un elemento de B, para cada $a \in A$. Para aclarar esto veamos:

Ejemplo 3.2.4 *La función* $f : \{1,2,4,7\} \to \{2,4,6,8,14\}$, *definida por* $f(a) = 2a$, *tiene gráfico*

$$G = \{(1,2),(2,4),(4,8),(7,14)\}.$$

Ejemplo 3.2.5 *Por otro lado, es erróneo escribir* $f : \{1,2,4,7\} \to \{2,4,6,8,12\}$, *con* $f(a) = 2a$, *pues la "imagen" de* 7 *no está en el conjunto de llegada* $B = \{2,4,6,8,12\}$. *Es decir,* 7 *no tiene imagen y* f *no es función.*

Ejemplo 3.2.6 *La función* $f : \mathbb{Z} \to \mathbb{Z}$, $f(n) = n^2$, *tiene dominio* $\mathbb{Z}$, *codominio* $\mathbb{Z}$, *y gráfico*

$$G = \left\{(n,m) \in \mathbb{Z} \times \mathbb{Z} : n^2 = m\right\}.$$

3.2.2 Ámbito e imágenes directas e inversas de conjuntos

Como muestran los ejemplos anteriores, dependiendo de la función, los elementos del codominio pueden no tener pre-imágenes, o pueden tener varias. Los elementos que poseen al menos una pre-imagen, forman un subconjunto del codominio, llamado *ámbito* o *rango* de la función dada. Más precisamente, el ámbito de $f : A \to B$ es el conjunto

$$\text{amb}(f) := \{b \in B : \exists\, a \in A \text{ tal que } f(a) = b\} = \{f(a) : a \in A\}.$$

Más generalmente, podemos considerar las imágenes de un subconjunto cualquiera C de A. Estas forman un conjunto llamado el *conjunto imagen de* C, que es denotado por $f(C)$. Esto es

$$f(C) := \{b \in B : \exists\, a \in C \text{ tal que } f(a) = b\} = \{f(a) : a \in C\}.$$

Note que $f(C) \neq \emptyset$ si $C \neq \emptyset$. Note además que en particular se tiene

$$f(A) = \text{amb}(f).$$

Para $D \subseteq B$, el conjunto de pre-imágenes de los elementos de D se llama el *conjunto pre-imagen* de D (o imagen inversa de D), y se denota por $f^{-1}(D)$. Entonces

$$f^{-1}(D) := \{a \in A : f(a) \in D\}.$$

En particular

$$f^{-1}(B) = f^{-1}(\text{amb}(f)) = A.$$

Ejemplo 3.2.7 *La función* $f : \mathbb{N} \to \mathbb{N}$, *definida por* $f(n) = 2n$, *tiene como ámbito al conjunto de números pares. Esto es*

$$\text{amb}(f) = P = \{n \in \mathbb{N} : n \text{ es par}\}.$$

Si $C = \{3,5,7\}$, *entonces* $f(C) = \{6,10,14\}$. *Si* $D = \{4,5,6,7\}$ *entonces* $f^{-1}(D) = \{2,3\}$. *Note que* $f^{-1}(f(C)) = f^{-1}(\{6,10,14\}) = \{3,5,7\} = C$, *mientras que*

$$f\left(f^{-1}(D)\right) = f(\{2,3\}) = \{4,6\} \neq D.$$

Ejemplo 3.2.8 *Sea* $f : \mathbb{N} \to \mathbb{R}$ *definida por*

$$f(n) = \begin{cases} 1 & \text{si } n \text{ es impar} \\ 2 & \text{si } n \text{ es par} \end{cases}$$

Entonces $\text{amb}(f) = \{1, 2\}$. *Sean* $C = \{6\}$, $D = \{2\}$. *Tenemos* $f(C) = D$ *y* $f^{-1}(D) = P$ *(el conjunto de los pares). Note que* $f^{-1}(f(C)) = f^{-1}(D) = P \neq C$, *mientras que* $f\left(f^{-1}(D)\right) = f(P) = D$. *Si* $E = \{2, 3\}$ *se tiene* $f\left(f^{-1}(E)\right) = f(P) = D \neq E$.

Ejemplo 3.2.9 *Sea* $f : P \to \mathbb{N}$ *definida por* $f(n) = \dfrac{n}{2}$. *Note que* $\text{amb}(f) = \mathbb{N}$. *Para el conjunto* $C = \{n \in P : n \text{ es múltiplo de } 4\}$ *tenemos* $f(C) = P \subseteq \mathbb{N}$, *y* $f^{-1}(f(C)) = f^{-1}(P) = C$. *Si* $D = \{n \in \mathbb{N} : n \text{ es múltiplo de } 3\}$ *entonces*

$$f^{-1}(D) = \{p \in P : p \text{ es múltiplo de } 6\},$$

y luego $f\left(f^{-1}(D)\right) = D$.

Los ejemplos de arriba muestran que en general no se tiene $f\left(f^{-1}(D)\right) = D$, ni tampoco $f^{-1}(f(C)) = C$. Vale la pena preguntarse para qué tipo de funciones se cumplen estas igualdades. Esta pregunta se contestará en la siguiente sección. Por ahora notemos que sí podemos decir algo en general:

Lema 3.2.1 *Sea* $f : A \to B$, *y sean* $C \subseteq A$, $D \subseteq B$. *Entonces tenemos*

$$C \subseteq f^{-1}(f(C)), \qquad f\left(f^{-1}(D)\right) \subseteq D.$$

Demostración
En efecto, si $x \in C$ entonces $f(x) \in f(C)$, lo que significa $x \in f^{-1}(f(C))$.
Por otro lado, si $y \in f\left(f^{-1}(D)\right)$, debe existir $x \in f^{-1}(D)$ tal que $f(x) = y$. Pero entonces $f(x) \in D$, o lo que es lo mismo, $y \in D$. □

Cabe preguntarse también qué relación existe por ejemplo entre los conjuntos $f(C \cup D)$y $f(C) \cup f(D)$, para $C, D \subseteq A$, o entre los conjuntos $f^{-1}(G \cap H)$ y $f^{-1}(G) \cap f^{-1}(H)$, con $G, H \subseteq B$. Los siguientes lemas responden estas y otras preguntas en el caso general.

Lema 3.2.2 *Sea* $f : A \to B$ *una función, y sean* C *y* D *subconjuntos de* A. *Tenemos*

$$f(C \cup D) = f(C) \cup f(D), \quad f(C \cap D) \subseteq f(C) \cap f(D).$$

Demostración
Para la identidad note que

$$\begin{aligned} y \in f(C \cup D) &\Leftrightarrow \exists\, x \in C \cup D \text{ tal que } y = f(x) \\ &\Leftrightarrow \exists x\,(x \in C \text{ o } x \in D) \text{ tal que } y = f(x) \\ &\Leftrightarrow y \in f(C) \text{ o } y \in f(D) \\ &\Leftrightarrow y \in f(C) \cup f(D). \end{aligned}$$

Para la inclusión sea $y \in f(C \cap D)$. Entonces existe $x \in C \cap D$ tal que $y = f(x)$. Luego $x \in C$ y $x \in D$, con lo que $y \in f(C)$ y $y \in f(D)$, o sea que $y \in f(C) \cap f(D)$. $\square$

En el ejemplo 3.2.8, con $C = \{2,3\}$ y $D = \{3,4\}$ tenemos $f(C) \cap f(D) = \{1,2\}$, mientras que $f(C \cap D) = f(\{3\}) = \{1\}$. Esto demuestra que en general es falso que $f(C \cap D) = f(C) \cap f(D)$. En la siguiente sección veremos en qué casos hay igualdad. En el caso de conjuntos pre-imagen sí se obtiene igualdad en general, debido a la unicidad de la imagen para $x \in A$.

Lema 3.2.3 *Sea $f : A \to B$ una función, y sean G y H subconjuntos de B. Tenemos*

$$f^{-1}(G \cup H) = f^{-1}(G) \cup f^{-1}(H), \quad f^{-1}(G \cap H) = f^{-1}(G) \cap f^{-1}(H).$$

Demostración
Para la primera identidad, note que

$$\begin{array}{rcl} x \in f^{-1}[G \cup H] & \Leftrightarrow & f(x) \in G \cup H \\ & \Leftrightarrow & f(x) \in G \text{ o } f(x) \in H \\ & \Leftrightarrow & x \in f^{-1}(G) \text{ o } x \in f^{-1}(H) \\ & \Leftrightarrow & x \in f^{-1}(G) \cup f^{-1}(H). \end{array}$$

La segunda identidad se demuestra de manera análoga.$\square$

3.2.3 Tipos de funciones

De acuerdo con la cantidad de pre-imágenes que poseen los elementos del codominio, las funciones se clasifican en:

- Inyectivas: Son aquellas funciones tales que cada elemento del codominio tiene a lo sumo una pre-imagen. En otras palabras, la función $f : A \to B$ es inyectiva si

  $$\forall a, x \in A, \quad f(a) = f(x) \Rightarrow a = x,$$

  o equivalentemente

  $$\forall a, x \in A, \quad a \neq x \Rightarrow f(a) \neq f(x).$$

- Sobreyectivas: Son aquella funciones tales que cada elemento del codominio tiene al menos una pre-imagen. Entonces la función $f : A \to B$ es sobreyectiva si y solo si $\text{amb}(f) = B$. En otras palabras, f es sobreyectiva si

  $$\forall b \in B, \exists\, a \in A \text{ tal que } f(a) = b.$$

- Biyectivas: Son las funciones que son inyectivas y sobreyectivas. Equivalentemente, una función es biyectiva si cada elemento del codominio posee exactamente una pre-imagen:

  $$\forall b \in B, \exists\, a \in A \text{ único, tal que } f(a) = b.$$

  Es evidente que en tal caso podemos definir una función $g : B \to A$ tal que

  $$g(b) = a \Leftrightarrow f(a) = b.$$

  En otras palabras, si $f = (A, B, G)$, entonces $g = (B, A, G')$, donde

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

  Esta función g se llama la inversa de f, y se denota por f^{-1}. Luego se retomará el tema de la función inversa con más detalle.

Ejemplo 3.2.10 *La función $f : \mathbb{N} \to \mathbb{N}$, definida por $f(n) = 2n$, es inyectiva pero no sobreyectiva, lo primero pues $2n = 2m$ implica $n = m$; lo segundo pues* $\text{amb}(f) = P \neq \mathbb{N}$.

Ejemplo 3.2.11 *Sea $f : \mathbb{N} \to \mathbb{N}$ definida por $f(n) = 1$ si n es impar, y $f(n) = 2$ si n es par. Esta función no es inyectiva pues por ejemplo $f(2) = f(4)$. Tampoco es sobreyectiva pues* $\text{amb}(f) = \{1, 2\} \neq \mathbb{N}$.

Ejemplo 3.2.12 *Sea $g : \mathbb{N} \to \{1, 2\}$ definida por $g(n) = 1$ si n es impar, y $g(n) = 2$ si n es par. Esta función no es inyectiva, pero sí es sobreyectiva pues el ámbito coincide con el codominio.*

Ejemplo 3.2.13 *Sea $f : \mathbb{N} \to P$ definida por $f(n) = 2n$. Como* $\text{amb}(f) = P$, *la función es sobreyectiva. Además es inyectiva pues $2n = 2m$ implica $n = m$. Se concluye entonces que f es biyectiva, y su inversa es la función $g : P \to \mathbb{N}$ definida por $g(m) = \frac{m}{2}$*

Ejemplo 3.2.14 *Sea $E = \{1, 2, 3\}$, y considere la relación de equivalencia $\mathcal{R}$ definida por el gráfico $R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3)\}$. Recordemos que*

$$E/\mathcal{R} = \{[1], [3]\} = \{\{1, 2\}, \{3\}\}.$$

Podemos definir una función $f : E \to E/\mathcal{R}$ por $f(x) = [x]$. Entonces $f(1) = f(2) = [1]$, y $f(3) = [3]$. Esta función es sobreyectiva, pero no inyectiva.

Nota: En general, dada una relación de equivalencia sobre un conjunto E cualquiera, la función $\pi : E \to E/\mathcal{R}$ definida por $\pi(x) = [x]$, se llama la *proyección canónica* de E sobre $E/\mathcal{R}$, y es sobreyectiva.

Ejemplo 3.2.15 *En $E = \mathbb{N}$, con la relación*

$$n \sim m \Leftrightarrow n + m \text{ es par,}$$

se tiene $E/\sim = \{[0], [1]\} = \{P, I\}$, donde P es el conjunto de los pares, e I es el conjunto de los impares. El conjunto $E/\sim$ se puede identificar con $\{0, 1\}$ mediante la biyección $f : \{0, 1\} \to E/\sim$, $f(x) = [x]$.

Ejemplo 3.2.16 *Para la relación definida por*

$$(m, n) \sim (p, q) \Leftrightarrow m + q = n + p,$$

en $\mathbb{N} \times \mathbb{N}$. La función $f : \mathbb{Z} \to E/\sim$, definida por $f(n) = [(n, 0)]$ si $n \geq 0$, y $f(n) = [(0, n)]$ si $n < 0$, es biyectiva. Esto es, $E/\sim$ se identifica con $\mathbb{Z}$. Esta es la idea que utilizaremos más adelante para definir $\mathbb{Z}$ a partir de $\mathbb{N}$.

Ejemplo 3.2.17 *Sea A un conjunto no vacío, y sea $f : A \to \mathcal{P}(A)$ definida por $f(x) = \{x\}$. Entonces f es inyectiva pues $\{x\} = \{y\}$ implica $x = y$. Sin embargo f no es sobreyectiva (¿por qué?). Un hecho importante de la teoría de cardinalidades, es que no existe ninguna función sobreyectiva de A en $\mathcal{P}(A)$ (ver los ejercicios).*

Ejemplo 3.2.18 *Sea A un conjunto no vacío, y sea $f : A \times A \to \mathcal{P}(A)$ definida por $f(a, b) = \{a, b\}$. Si A tiene al menos dos elementos, entonces f no es inyectiva, pues en tal caso podemos tomar $a, b \in A$ tales que $a \neq b$, obteniendo $(a, b) \neq (b, a)$ pero $f(a, b) = f(b, a)$. En ningún caso f es sobreyectiva.*

Ahora podemos contestar las preguntas planteadas al inicio de esta sección.

Lema 3.2.4 *Sea $f : A \to B$ una función. Entonces f es sobreyectiva si y solo si $f\left(f^{-1}(D)\right) = D$ para todo $D \subseteq B$. Además f es inyectiva si y solo si $f^{-1}(f(C)) = C$ para todo $C \subseteq A$.*

Demostración
Probamos la primera equivalencia, y dejamos la segunda como ejercicio:
Si f es sobreyectiva, sea $D \subseteq B$. Ya tenemos "$\subseteq$". Para demostrar "$\supseteq$" sea $y \in D$. Como f es sobreyectiva existe $x \in A$ tal que $f(x) = y$. Luego $x \in f^{-1}(D)$, y consecuentemente $y \in f\left(f^{-1}(D)\right)$.
Recíprocamente, suponga ahora que $f\left(f^{-1}(D)\right) = D$ para todo $D \subseteq B$. Dado $y \in B$, considere el conjunto $D = \{y\}$. Entonces $f\left(f^{-1}(\{y\})\right) = \{y\}$, lo que implica $y \in f\left(f^{-1}(\{y\})\right)$, esto es, $y = f(x)$ para algún $x \in f^{-1}(\{y\}) \subseteq A$. Esto demuestra que f es sobreyectiva. □

Lema 3.2.5 *Sea $f : A \to B$ una función. Entonces f es inyectiva si y solo si $f(C \cap D) = f(C) \cap f(D)$, para todo par de conjuntos $C, D \subseteq A$.*

Demostración
En efecto, suponga que f es inyectiva. Como "$\subseteq$" siempre es válido, nos damos $y \in f(C) \cap f(D)$. Entonces $y \in f(C)$ y $y \in f(D)$, lo que significa que existe $x \in C$ tal que $f(x) = y$, y existe $z \in D$ tal que $f(z) = y$. Pero como f es inyectiva, se sigue que $x = z$, de donde $x \in C \cap D$. Esto implica por definición que $y \in f(C \cap D)$.
Recíprocamente, si la igualdad es válida para todo par de subconjuntos de A, mostremos que f es inyectiva: Sean $x, z \in A$ tales $x \neq z$. Tomando $C = \{x\}$ y $D = \{z\}$ tenemos $C \cap D = \emptyset$, de donde $f(C \cap D) = f(\emptyset) = \emptyset$. Por hipótesis se sigue que $f(C) \cap f(D) = \emptyset$, lo que significa $f(x) \neq f(z)$. □

3.2.4 Composición de funciones

Dadas dos funciones $f : A \to B$ y $g : B \to C$, podemos definir la composición $g \circ f : A \to C$ por $(g \circ f)(x) = g(f(x))$, $\forall x \in A$. Esto corresponde con el concepto de composición de relaciones, previamente estudiado.

Ejemplo 3.2.19 *Sea $f : \mathbb{N} \to \mathbb{N}$ tal que $f(n) = 8$ para todo n, y sea $g : \mathbb{N} \to \mathbb{N}$ definida por $g(n) = n^2 + 4n + 4$ para todo $n \in \mathbb{N}$. Podemos definir $g \circ f : \mathbb{N} \to \mathbb{N}$, obteniendo*

$$(g \circ f)(n) = g(8) = 8^2 + 4 \cdot 8 + 4 = 100,$$

para todo $n \in \mathbb{N}$.

Ejemplo 3.2.20 *Sea $f : \{1, 2, 3, 4\} \to \{0, 1, 2, 3\}$ definida por $f(n) = 4 - n$, y sea $g : \{0, 1, 2, 3\} \to \{1, 2, 3, 4\}$ definida por $g(n) = 4 - n$. Entonces*

$$g \circ f : \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$$

es tal que $(g \circ f)(n) = g(4 - n) = 4 - (4 - n) = n$, $\forall n \in \{1, 2, 3, 4\}$.

Definición 3.2.1 *Dado un conjunto $A \neq \emptyset$, la función $f : A \to A$ definida por $f(x) = x$, se llama la función identidad de A, y se denota por id_A. En alguna literatura se acostumbra usar también los símbolos 1_A y I_A.*

Ejemplo 3.2.21 *Sea $f : \mathbb{N} \to P$ definida por $f(n) = 6n$, y sea $g : P \to \mathbb{N}$ definida por $g(p) = \frac{3p}{2}$. Note que g está bien definida pues $\frac{3p}{2} \in \mathbb{N}$ para todo número par p. Podemos componer las funciones obteniendo*

$$g \circ f : \mathbb{N} \to \mathbb{N}, \quad (g \circ f)(n) = g(6n) = \frac{3 \cdot 6n}{2} = 9n, \ \forall n \in \mathbb{N}.$$

3.2.5 Funciones inversas

El concepto de función inversa puede introducirse más fácilmente si se estudia primero el concepto de relación inversa en general. Veamos:

Definición 3.2.2 *Dada una relación* $\mathcal{R} = (A, B, R)$, *definimos la relación inversa* $\mathcal{R}^{-1}$ *por:*

$$\mathcal{R}^{-1} = \left(B, A, R^{-1}\right),$$

donde

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

Ejemplo 3.2.22 *Sean* $A = \{1, 2, 3\}$, $B = \{4, 7, 9\}$ *y* $R = \{(1, 4), (1, 7), (2, 4), (3, 7), (3, 9)\}$. *Entonces la relación* $\mathcal{R} = (A, B, R)$ *tiene por inversa a* $\mathcal{R}^{-1} = \left(B, A, R^{-1}\right)$, *donde*

$$R^{-1} = \{(4, 1), (7, 1), (4, 2), (7, 3), (9, 3)\}.$$

Ejemplo 3.2.23 *La función* $f = \mathbb{R} \to \mathbb{R}$ *definida por* $f(x) = x^2$, *tiene por inversa a la relación* $f^{-1} = (\mathbb{R}, \mathbb{R}, G)$, *donde*

$$G = \left\{(x^2, x) : x \in \mathbb{R}\right\}.$$

Note que f^{-1} *no es una función.*

Definición 3.2.3 *Decimos que una función* f *es invertible si su relación inversa es una función.*

Ejemplo 3.2.24 *El ejemplo anterior muestra que la función* $f : \mathbb{R} \to \mathbb{R}$ *definida por* $f(x) = x^2$, *no es invertible.*

Ejemplo 3.2.25 *Por otro lado, la función* $g : [0, \infty[\to [0, \infty[$, *definida por* $g(x) = x^2$, *sí es invertible, y su inversa es la función* $g^{-1} : [0, \infty[\to [0, \infty[$, *definida por* $g^{-1}(x) = \sqrt{x}$.

Lema 3.2.6 *La función* $f : A \to B$ *es invertible si existe una función* $g : B \to A$ *tal que* $g \circ f = id_A$ *y* $f \circ g = id_B$. *En tal caso* $g = f^{-1}$.

Demostración
Si f es invertible, sabemos que $g = f^{-1}$ es función. Además, si $a \in A$ tenemos $(a, f(a)) \in G$, de donde $(f(a), a) \in G^{-1}$. Esto significa que $f^{-1}(f(a)) = a$. Similarmente se demuestra que $f\left(f^{-1}(b)\right) = b$, para $b \in B$.
Recíprocamente, si tal función g existe, denotemos por G' al gráfico de g. Para $(a, b) \in A \times B$ tenemos

$$(a, b) \in G \Leftrightarrow b = f(a) \Leftrightarrow g(b) = a \Leftrightarrow (b, a) \in G'.$$

Esto demuestra que $G' = G^{-1}$, y por lo tanto $g = f^{-1}$ (recuerde que dos relaciones son iguales cuando tienen mismo dominio, codominio y gráfico). □

Note que en particular

$$\left(f^{-1} \circ f\right)(x) = x,\ \forall x \in A, \quad \left(f \circ f^{-1}\right)(y) = y,\ \forall y \in B.$$

En otras palabras, para $x \in A$ y $y \in B$ se tiene:

$$f(x) = y \Leftrightarrow x = f^{-1}(y).$$

El lema anterior demuestra en particular la unicidad de la inversa, en el sentido que es la única función $g : B \to A$ que satisface $g \circ f = id_A$ y $f \circ g = id_B$.

No es difícil ver que f es biyectiva si y solo si es invertible. En efecto:

$$\begin{aligned} f \text{ es biyectiva} &\Leftrightarrow \forall b \in B, \exists!\, a \in A \text{ tal que } f(a) = b \\ &\Leftrightarrow \forall b \in B, \exists!\, a \in A \text{ tal que } (a, b) \in G \\ &\Leftrightarrow \forall b \in B, \exists!\, a \in A \text{ tal que } (b, a) \in G^{-1} \\ &\Leftrightarrow f^{-1} \text{ es función.} \end{aligned}$$

Escribimos esto como un teorema:

Teorema 3.1 *Sea $f : A \to B$ una función. Entonces f es invertible si y solo si es biyectiva.*

Ejemplo 3.2.26 *Considere la función $f : \mathbb{R} \to \mathbb{R}$ que asocia a cada $x \in \mathbb{R}$ con $2x + 1$. Se tiene $f(x) = 2x + 1$, $\forall x \in \mathbb{R}$. Note que f es inyectiva, pues*

$$f(x) = f(y) \Rightarrow 2x + 1 = 2y + 1 \Rightarrow 2x = 2y \Rightarrow x = y.$$

Para ver si es sobreyectiva tomemos $y \in \mathbb{R}$ y tratemos de encontrar x tal que $f(x) = y$. Debemos entonces resolver $2x + 1 = y$, cuya solución es $x = \frac{1}{2}(y - 1)$. Obtenemos así que f es biyectiva. Además, definiendo $g(y) = \frac{1}{2}(y - 1)$, tenemos que

$$(g \circ f)(x) = g(2x + 1) = \frac{2x + 1 - 1}{2} = x,\ \forall x \in \mathbb{R},$$

y similarmente $(f \circ g)(y) = y$, $\forall y \in \mathbb{R}$. Entonces $g = f^{-1}$.

Ejemplo 3.2.27 *En general, la función definida por $f(x) = mx + b$, donde m y b son números reales fijos, es biyectiva si $m \neq 0$. Resolviendo la ecuación $f(x) = y$, vemos que $f^{-1}(y) = \frac{1}{m}(y - b)$, $\forall y \in \mathbb{R}$.*

Ejemplo 3.2.28 *Consideremos la función $f : \mathbb{Z} \to \mathbb{N}$ definida por*

$$f(z) = \begin{cases} -2z - 1 & si\ z < 0 \\ 2z & si\ z \geq 0. \end{cases}$$

Esta función es biyectiva. En efecto, si $f(x) = f(z) = n$, tenemos dos posibilidades:

Si n es par, entonces x y z deben ser ambos no negativos, y entonces $n = 2x = 2z$, de donde $x = z$. Similarmente, si n es impar, entonces tenemos que x y z son ambos negativos, y $-2x - 1 = -2z - 1$, lo que implica $x = z$. Esto demuestra que f es inyectiva. Para ver que es también sobreyectiva, tomemos $n \in \mathbb{N}$. Si n es par, entonces $n = 2k = f(k)$, para algún $k \in \mathbb{N}$. Si n es impar, entonces $n = 2k-1 = f(-k)$, con $k = \dfrac{n+1}{2}$. En particular, la función inversa está dada por

$$f^{-1}(n) = \begin{cases} \frac{n}{2} & \text{si } n \text{ es par} \\ -\frac{n+1}{2} & \text{si } n \text{ es impar.} \end{cases}$$

Ejemplo 3.2.29 *Considere la función $f : \mathbb{R} - \{-1\} \to \mathbb{R}$, definida por $f(x) = \frac{1}{x+1}$. Esta función es inyectiva, pues*

$$f(x) = f(y) \Rightarrow \frac{1}{x+1} = \frac{1}{y+1} \Rightarrow y + 1 = x + 1 \Rightarrow y = x.$$

Para ver si es sobreyectiva, tomemos $y \in \mathbb{R}$ y tratemos de hallar x tal que $f(x) = y$. Tenemos

$$\frac{1}{x+1} = y \Rightarrow \frac{1}{y} = x + 1 \Rightarrow x = \frac{1}{y} - 1,$$

siempre que $y \neq 0$. Note que $y = 0$ no tiene preimagen, así que f no es sobreyectiva.

Ejemplo 3.2.30 *La función $f : \mathbb{R}-\{-1\} \to \mathbb{R}-\{0\}$, definida por $f(x) = \dfrac{1}{x+1}$, es biyectiva. Su inversa está dada por $f^{-1}(y) = \dfrac{1}{y} - 1$, $\forall y \in \mathbb{R} - \{0\}$.*

3.2.6 Gráficas de funciones reales

En esta sección estudiaremos los gráficos de algunas funciones elementales, y trazaremos algunas representaciones geométricas (gráficas) de ellos. Para esto es útil conocer el concepto de función monótona que veremos a continuación.

Definición 3.2.4 *Sean A y B dos subconjuntos de $\mathbb{R}$. Decimos que la función $f : A \to B$ es creciente si, al aplicarla a los elementos de A, preserva el orden. Más precisamente, si $x, y \in A$ son tales que $x < y$, entonces $f(x)$ y $f(y) \in B$ son tales que $f(x) \leq f(y)$. Simbólicamente esto se escribe:*

$$\forall x, y \in A,\ x < y \Rightarrow f(x) \leq f(y),$$

Si lo anterior se cumple con desigualdad estricta, se dice que la función f es estrictamente creciente. Es decir, f se llama estrictamente creciente si cumple:

$$\forall x, y \in A,\ x < y \Rightarrow f(x) < f(y).$$

Similarmente, decimos que $f : A \to B$ *es decreciente si*

$$x, y \in A,\ x < y \Rightarrow f(x) \geq f(y),$$

y estrictamente decreciente si

$$x, y \in A,\ x < y \Rightarrow f(x) > f(y).$$

Gráficamente, una función es creciente si cuando x se mueve hacia la derecha en el eje de las abscisas, su imagen se mueve hacia arriba en el eje de la ordenadas.

Ejemplo 3.2.31 *Considere la función* $f : \mathbb{R} \to \mathbb{R}$ *que asocia a cada* $x \in \mathbb{R}$ *con* $2x$. *Se tiene entonces* $f(x) = 2x$, *para cada* $x \in \mathbb{R}$. *Es claro que esta función es estrictamente creciente. En efecto, para* $x, y \in \mathbb{R}$ *se tiene*

$$x < y \Rightarrow 2x < 2y \Rightarrow f(x) < f(y).$$

El gráfico de f *es el conjunto* $G = \{(x, 2x) : x \in \mathbb{R}\}$. *La gráfica de* f *contiene al origen, y al punto de coordenadas* $(1, 2)$. *Por el teorema de Tales, la recta que pasa por dichos puntos, pasa también por el punto de coordenadas* $(x, 2x) \in G$. *Consecuentemente, la gráfica de* f *es precisamente dicha recta.*

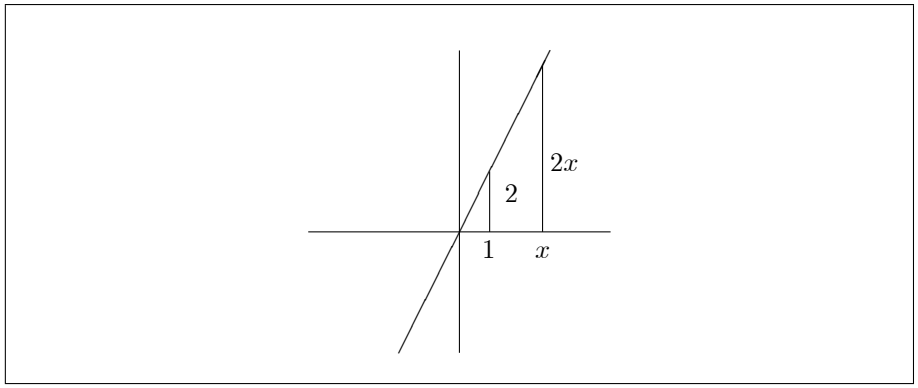


Figura 3.2: Gráfica de la función dada por $f(x) = 2x$.

Ejemplo 3.2.32 *Considere la función* $f : \mathbb{R} \to \mathbb{R}$ *que asocia a cada* $x \in \mathbb{R}$ *con* $2x + 1$. *Se tiene entonces* $f(x) = 2x + 1$, *para cada* $x \in \mathbb{R}$. *Veamos que esta función es estrictamente creciente:*

$$x < y \Rightarrow 2x < 2y \Rightarrow 2x + 1 < 2y + 1 \Rightarrow f(x) < f(y).$$

El gráfico de f *es el conjunto* $\{(x, 2x + 1) : x \in \mathbb{R}\}$. *Su gráfica se obtiene trasladando la gráfica del ejemplo anterior, una unidad hacia arriba en el plano cartesiano (ver figura 3.3).*

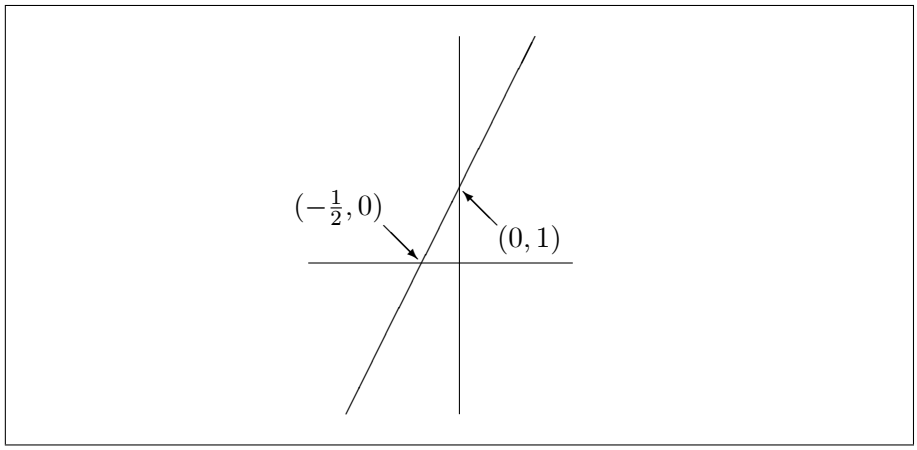


Figura 3.3: Gráfica de la función dada por $f(x) = 2x + 1$.

Gráficas de funciones afines

La función definida por $f(x) = mx$, donde m es un número real fijo, es estrictamente creciente si $m > 0$, y estrictamente decreciente si $m < 0$. Su gráfica es una recta en el plano que pasa por el origen y el punto $(1, m)$. Para justificar esto, considere un punto (x, y) sobre dicha recta. Por semejanza de triángulos (ver figura 3.4) se tiene

$$\frac{y}{x} = \frac{m}{1} = m,$$

de donde se sigue que $y = mx = f(x)$. Esto demuestra que efectivamente, la gráfica de f es la recta en cuestión. El número m se llama la pendiente de esta recta.

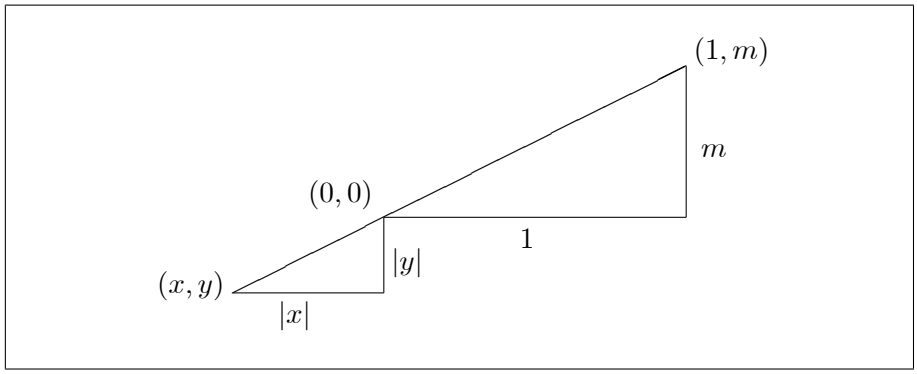


Figura 3.4: Recta de ecuación $y = mx$.

Ejemplo 3.2.33 *Para $m = -3$ se obtiene la recta que pasa por el origen y el punto $(1, -3)$. Se invita al lector a trazar dicha recta.*

En general, la gráfica de la función definida por $g(x) = mx + b$, se obtiene trasladando la recta anterior, una distancia $|b|$ hacia arriba o hacia abajo, dependiendo del signo de b. Es decir, la gráfica de g será una recta de pendiente m que pasa por el punto $(0, b)$.

Uso del valor absoluto

La función $f : \mathbb{R} \to \mathbb{R}$, definida por $f(x) = |x|$, no es inyectiva (pues $f(-1) = f(1)$) ni sobreyectiva (pues ningún número negativo tiene preimagen). Su gráfica coincide con la recta de ecuación $y = x$ para $x \geq 0$, y con la recta de ecuación $y = -x$ para $x < 0$. Note que en particular f es estrictamente decreciente en el intervalo $]-\infty, 0]$, y estrictamente creciente en $[0, \infty[$.

Para trazar la gráfica podemos entonces dibujar las dos rectas en cuestión, y luego borrar las partes de estas que quedan por debajo del eje x.

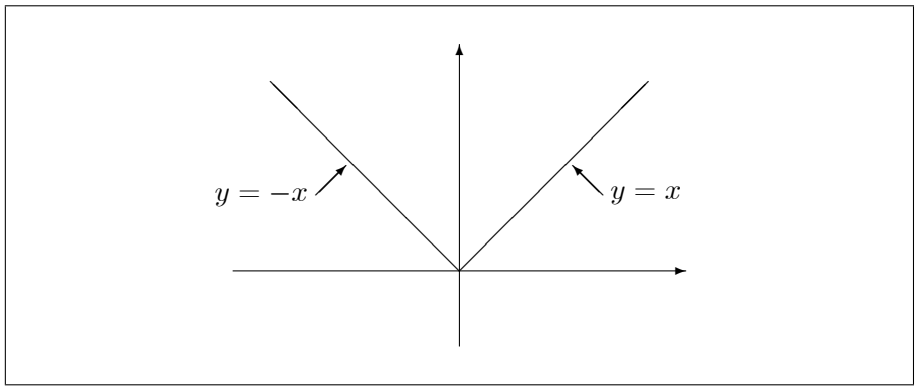


Figura 3.5: Gráfica de la función $f(x) = |x|$.

Ejemplo 3.2.34 *Para graficar la función $g : \mathbb{R} \to \mathbb{R}$ definida por $g(x) = |x - 1|$, podemos proceder como en el ejemplo anterior, considerando los casos $x \geq 1$ y $x < 1$. Otra forma de hacerlo es observando que la gráfica de g se obtiene de la gráfica de $f(x) = |x|$, trasladándola una unidad a la derecha. En efecto, dado que $g(x + 1) = f(x)$, la imagen de x bajo f es la imagen de $x + 1$ bajo g.*

Nota: En general, si la función g se define por $g(x) = f(x-c)$, con $c > 0$, entonces su gráfica se obtiene trasladando c unidades a la derecha la gráfica de f. Si la función h se define por $h(x) = f(x)+c$, con $c > 0$, entonces su gráfica se obtiene trasladando c unidades hacia arriba la gráfica de f.

Ejemplo 3.2.35 *Para trazar la gráfica de la función $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = |x| + |x - 1|$, consideramos los siguientes casos:*

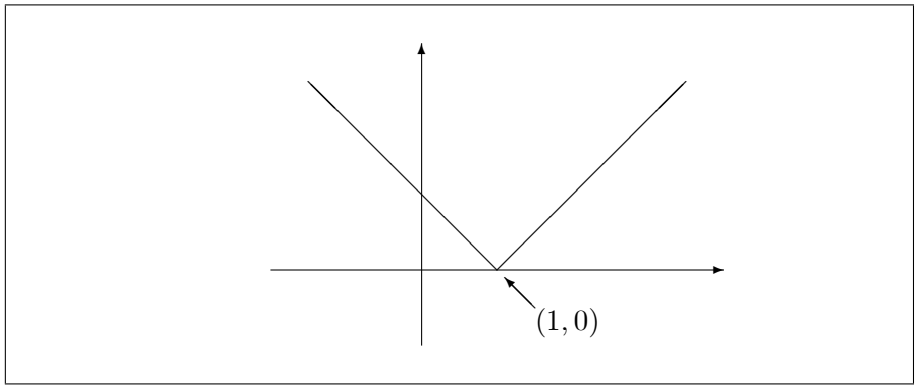


Figura 3.6: Gráfica de la función $f(x) = |x - 1|$.

- *Si* $x < 0$ *entonces* $|x| = -x$ *y* $|x - 1| = 1 - x$*, así que* $f(x) = -2x + 1$.
- *Si* $0 \leq x < 1$ *se tiene* $f(x) = x + 1 - x = 1$.
- *Si* $x \geq 1$ *se tiene* $f(x) = x + x - 1 = 2x - 1$.

En resumen, podemos expresar la función f *así:*

$$f(x) = \begin{cases} 2x - 1 & si\ x \geq 1 \\ 1 & si\ 0 \leq x < 1 \\ -2x + 1 & si\ x < 0. \end{cases}$$

De lo anterior se sigue que la función no es sobreyectiva ni inyectiva. Su ámbito es el intervalo $[1, \infty[$. *Se invita al lector a demostrar estos hechos con detalle. La gráfica de* f *coincide con la recta de ecuación* $y = -2x + 1$ *en el intervalo* $]-\infty, 0]$*, con la recta de ecuación* $y = 1$ *en* $[0, 1]$*, y con la recta de ecuación* $y = 2x - 1$ *en* $[1, \infty[$.

Parábolas

La función $f : \mathbb{R} \to \mathbb{R}$, definida por $f(x) = x^2$, no es inyectiva ni sobreyectiva. En efecto, no es inyectiva pues $f(-1) = f(1)$, y no es sobreyectiva pues el ámbito es $[0, \infty[\neq \mathbb{R}$. Esta función es estrictamente decreciente en el intervalo $]-\infty, 0]$ y estrictamente creciente en $[0, \infty[$. Para ver que es estrictamente creciente en $[0, \infty[$, tomemos a, b tales que $0 \leq a < b$. Entonces $b + a$ y $b - a$ son positivos, con lo que $(b + a)(b - a) > 0$. Esto es, $b^2 - a^2 > 0$, o sea $a^2 < b^2$. Similarmente se demuestra que f es decreciente en $]-\infty, 0]$.
Su gráfica tiene la forma de la figura 3.8.
Nota: La forma de la gráfica no es evidente del hecho que f sea decreciente antes del origen y creciente después, pues ese hecho deja aún la posibilidad de que dicha gráfica tenga formas como las dadas en la figura **??**.
En el ejercicio 21 invitamos al lector a descartar estas posibilidades.

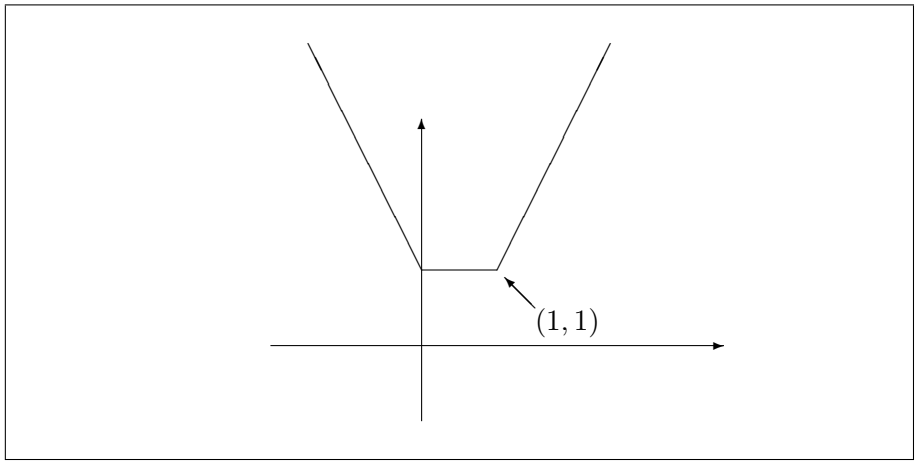


Figura 3.7: Gráfica de la función $f(x) = |x| + |x - 1|$.

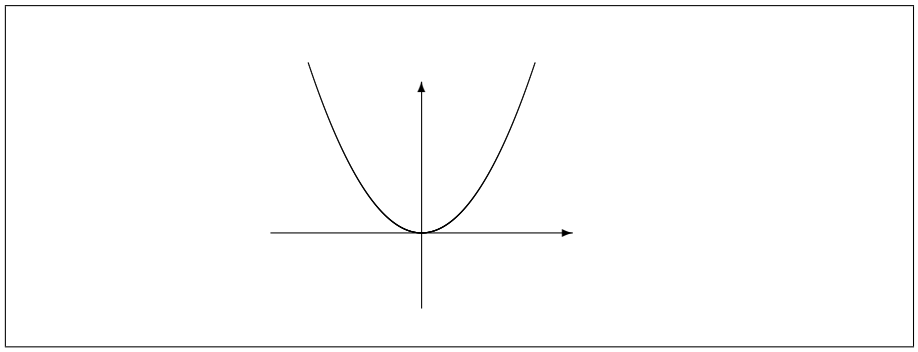


Figura 3.8: Gráfica de la función $f(x) = x^2$.

Ejemplo 3.2.36 *Para graficar la función cuadrática definida por* $g(x) = x^2 + 3x + 2$, *completamos el cuadrado, obteniendo* $f(x) = (x + \frac{3}{2})^2 - \frac{1}{4}$. *Entonces la gráfica de* g *se obtiene trasladando la del ejemplo anterior* $\frac{3}{2}$ *hacia la izquierda y* $\frac{1}{4}$ *hacia abajo. El punto* $\left(-\frac{3}{2}, -\frac{1}{4}\right)$ *se llama el vértice de la parábola, y la función es estrictamente decreciente en* $]-\infty, -\frac{3}{2}]$, *y estrictamente creciente en* $[-\frac{3}{2}, \infty[$. *En la figura 3.10 se describe la gráfica de* f.

Ejemplo 3.2.37 *Para analizar la gráfica de la función* $g(x) = 4x^2$, *observemos que* $4x^2 = (2x)^2$. *Entonces la gráfica se obtiene dibujando la función* $f(x) = x^2$ *en el plano cartesiano que resulta de reducir la escala en el eje* x *a la mitad.*

En general, $g(x) = ax^2$ (con $a > 0$) es una parábola que se obtiene de $y = x^2$ mediante un cambio de escala. Cuando $a < 0$, se debe realizar también una reflexión con respecto al eje x.

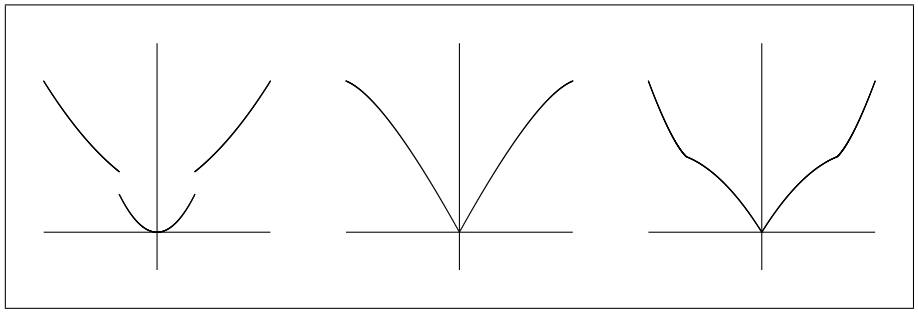


Figura 3.9: Gráficas no convexas.

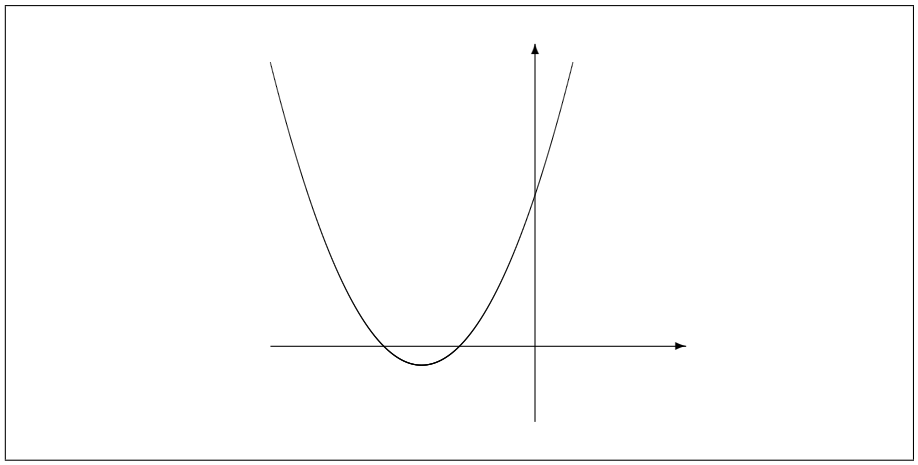


Figura 3.10: Gráfica de $f(x) = x^2 + 3x + 2$

La forma general de la ecuación cuadrática

La función definida por $f(x) = ax^2 + bx + c$, donde $a \neq 0$, b y c son constantes, puede escribirse en la forma

$$f(x) = a\left(x + \frac{b}{2a}\right)^2 - \frac{\Delta}{4a},$$

donde $\Delta = b^2 - 4ac$ es el discriminante. Su gráfica es entonces una parábola con vértice en el punto $\left(-\frac{b}{2a}, -\frac{\Delta}{4a}\right)$. Si $\Delta > 0$, la parábola corta al eje x en los puntos

$$\left(\frac{-b - \sqrt{\Delta}}{2a}, 0\right), \left(\frac{-b + \sqrt{\Delta}}{2a}, 0\right).$$

Si $\Delta = 0$, el vértice está sobre el eje x. Si $\Delta < 0$, la parábola no corta al eje x.

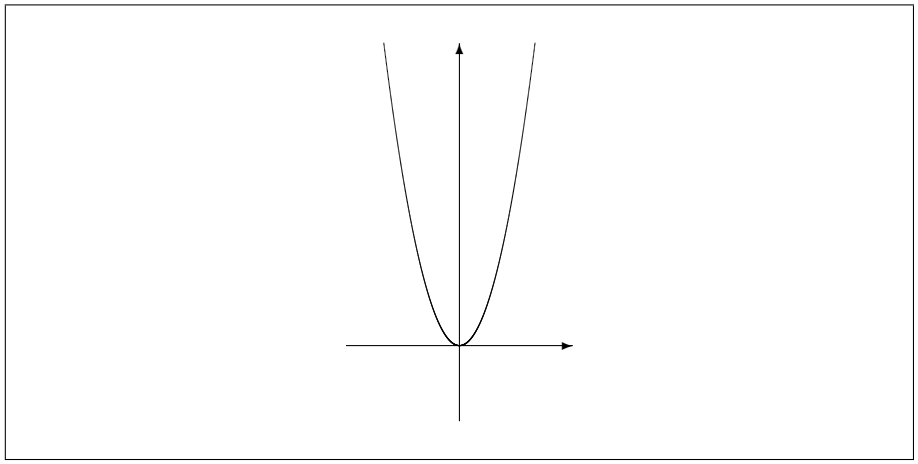


Figura 3.11: Gráfica de $f(x) = 4x^2$

La parábola abre hacia arriba si $a > 0$, y hacia abajo si $a < 0$.

Ejemplo 3.2.38 *Para graficar la función dada por* $f(x) = \left|x^2 + x\right| - x^2$, *observemos que* $x^2 + x = x(x+1)$, *así que*

$$f(x) = \begin{cases} x, & \text{si } x \notin [-1, 0] \\ -2x^2 - x & \text{si } x \in [-1, 0]. \end{cases}$$

En la figura 3.12 se grafican la recta $y = x$ *y la parábola* $y = -2x^2 - x$.

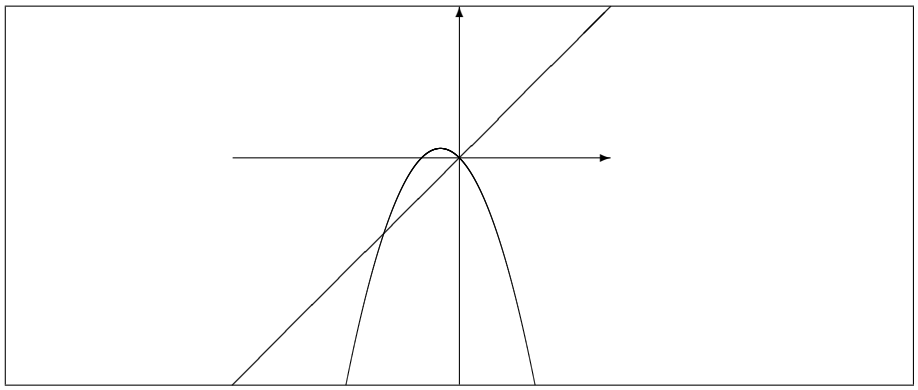


Figura 3.12: Gráficas de $y = x - 2$ y $y = -2x^2 - x$

Luego debemos borrar la parte de la recta que corresponde al intervalo $[-2, 1]$, *y la parte de la parábola que corresponde al complemento de dicho intervalo. La gráfica de* f *se presenta en la figura 3.13.*

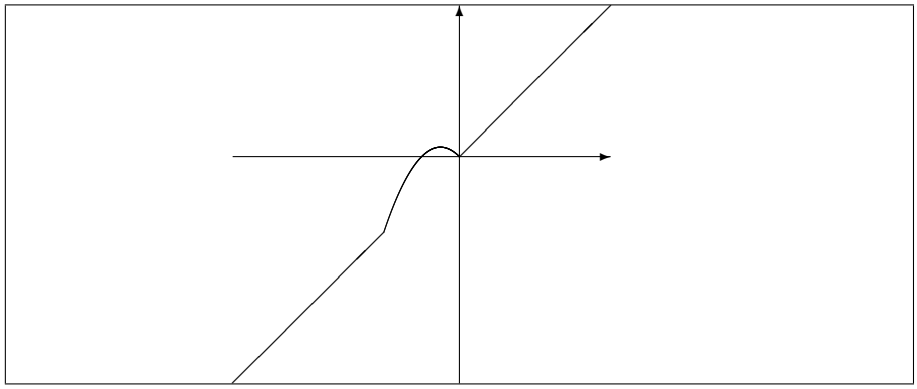


Figura 3.13: Gráfica de la función dada por $f(x) = \left|x^2 + x\right| - x^2$

3.2.7 Búsqueda de dominios

En diversas situaciones, uno se puede encontrar con una fórmula que puede ser utilizada para definir una función. En tales casos, se plantea el problema de hallar el conjunto más grande, sobre el cual se puede definir una función mediante la fórmula dada. Tal conjunto se denomina "Dominio máximo".

Es común abusar un poco del lenguaje en este contexto, escribiendo frases como: "Hallar el dominio máximo de la función $f(x)$", cuando en realidad se quiere decir: "Hallar el dominio máximo sobre el cual se puede definir una función mediante la fórmula $f(x)$". Debe recordarse que cuando se habla de una función, en sentido estricto se trata de una tripleta (A, B, G). Nosotros trataremos de evitar este tipo de abusos, y los usaremos solo cuando esto ayude a no hacer la lectura muy tediosa.

Ejemplo 3.2.39 *Considere la fórmula* $f(x) = \sqrt{x+2}$. *Para que la raíz tenga sentido, se necesita* $x + 2 \geq 0$, *así que el dominio máximo es* $[-2, \infty[$.

Ejemplo 3.2.40 *Para* $f(x) = \sqrt{x} - \sqrt{4-x}$ *necesitamos que* $x \geq 0$ *y* $4 - x \geq 0$, *de donde* $0 \leq x \leq 4$. *El dominio máximo en que puede definirse una función mediante esta fórmula es entonces* $[0, 4]$. *Note que aquí se tiene una suma de dos expresiones. La primera está definida en* $[0, \infty[$, *mientras que la segunda está definida en* $]-\infty, 4]$. *Para la suma requerimos que ambas estén definidas, y esto ocurre en la intersección*

$$[0, \infty[\cap]-\infty, 4] = [0, 4].$$

Ejemplo 3.2.41 *Hallar el dominio máximo sobre el cual se puede definir una función mediante la fórmula*

$$f(x) = \frac{x - \sqrt{x+4}}{x + \sqrt{2-x}}.$$

Primero necesitamos $x+4 \geq 0$ *y* $2-x \geq 0$, *de donde* $-4 \leq x \leq 2$. *Luego necesitamos que el denominador no se anule, y entonces debemos excluir los* x *tales que* $x+\sqrt{2-x}=0$. *Resolvamos:*

$$\begin{aligned} x+\sqrt{2-x}=0 &\Leftrightarrow -x=\sqrt{2-x}\geq 0 \\ &\Leftrightarrow x^2=2-x, \quad x\leq 0 \\ &\Leftrightarrow x^2+x-2=0, \quad x\leq 0 \\ &\Leftrightarrow (x+2)(x-1)=0, \quad x\leq 0. \end{aligned}$$

Como $x \leq 0$, *obtenemos* $x=-2$, *así que el dominio máximo en este caso es*

$$[-4,2]-\{-2\}=[-4,-2[\cup]-2,2].$$

Note que en este caso $f(x)$ *es el cociente de dos expresiones* $g(x)$ *y* $h(x)$, *definidas por* $g(x)=x+\sqrt{x+4}$ *y* $h(x)=x-\sqrt{2-x}$. *El dominio de* f *es entonces la intersección de los dominios de* g *y* h, *excluyendo los puntos donde* $h(x)=0$.

Ejemplo 3.2.42 *Hallar el dominio máximo sobre el cual se puede definir una función mediante la fórmula*

$$f(x)=\frac{1}{[\![x]\!]-x}.$$

Aquí, $[\![x]\!]$ *denota la parte entera de* x. *Así que* $x=[\![x]\!]$ *cuando, y únicamente cuando* $x \in \mathbb{Z}$. *Luego, el dominio máximo es* $\mathbb{R}-\mathbb{Z}$.

Nota: Cabe recalcar que en este tipo de ejercicios se busca hallar el dominio *máximo*, aunque nada impide que definamos una función en un conjunto más pequeño. Por ejemplo, podemos definir una función mediante la fórmula $f(x)=\sqrt{x-1}$ en el conjunto $[2,3]$. El dominio de esta función es entonces $[2,3]$, aunque el dominio máximo en que podría definirse una función con esa misma fórmula es $[1,\infty[$.

3.2.8 Diferentes operaciones con funciones

Se dice que una función $f: A \to B$ es una función real si

$$\operatorname{amb}(f)=\{f(x): x \in A\} \subseteq \mathbb{R}.$$

Seguidamente, vamos a definir algunas operaciones sobre las funciones reales.

Suma de funciones

Sean $f: A \to \mathbb{R}$ y $g: B \to \mathbb{R}$ dos funciones reales de dominios A y B respectivamente (en la mayoría de las funciones que estudiaremos A y B son subconjuntos de $\mathbb{R}$). Definimos la función $f+g$, a la cual llamamos función suma de f y g, de la siguiente manera:

$$f+g: A \cap B \to \mathbb{R}, \quad (f+g)(x)=f(x)+g(x).$$

Observe que por la manera como se define la suma de funciones, para poder evaluarla en un punto es necesario evaluar f y g en ese punto, lo que obliga a que el punto x pertenezca a ambos dominios. Por tal razón, el dominio de $f+g$ es $A \cap B$.

Ejemplo 3.2.43 *Sean* $f(x) = \sqrt{x+5}$ *y* $g(x) = \sqrt{8-x}$, *donde* $A = dom(f) = [-5, +\infty[$ *y* $B = dom(g) =]-\infty, 8]$.
Para poder definir $f + g$ *debemos encontrar* $A \cap B$. *Es decir:*

$$[-5, +\infty[\cap]-\infty, 8] = [-5, 8]$$

Tenemos entonces

$$f + g : [-5, 8] \to \mathbb{R}, \quad (f+g)(x) = \sqrt{x+5} + \sqrt{8-x}.$$

Ejemplo 3.2.44 *Considere* f *y* g *definidas con las mismas fórmulas del ejemplo anterior, pero ahora en los dominios* $A = dom(f) = [0, 4]$ *y* $B = dom(g) =]1, 7]$.
El dominio de $f + g$ *será, en este caso,* $A \cap B =]1, 4]$.

Producto de funciones

Sean $f : A \to \mathbb{R}$ y $g : B \to \mathbb{R}$ dos funciones definidas como en el caso de la suma, definimos la función:

$$f \cdot g : A \cap B \to \mathbb{R}, \quad (f \cdot g)(x) = f(x) \cdot g(x).$$

y la llamamos el producto de f y g.

La razón por la cual el dominio del producto se debe tomar como la intersección de los dominios de f y g, es totalmente análoga al caso de la suma. Es decir, la necesidad de poder evaluar $f(x)$ y $g(x)$ simultáneamente.

Ejemplo 3.2.45 *Considere* $f : [-3, +\infty[\to \mathbb{R}$ *definida por* $f(x) = \sqrt{x+3}$, *y sea* $g :]-\infty, 6[\to \mathbb{R}$, *definida por* $g(x) = \frac{1}{\sqrt{6-x}} - 1$.

En este caso se tiene $A \cap B = [-3, 6[$, *así que:*

$$f \cdot g : [-3, 6[\to \mathbb{R}, \quad (fg)(x) = \frac{\sqrt{x+3}}{\sqrt{6-x}} - \sqrt{x+3}.$$

Cociente de funciones

Sean $f : A \to \mathbb{R}$ y $g : B \to \mathbb{R}$ definidas como en la suma y el producto. Se define el cociente de f entre g como la función:

$$\frac{f}{g} : D \to \mathbb{R}, \quad \left(\frac{f}{g}\right)(x) = \frac{f(x)}{g(x)},$$

donde $D = A \cap B - \{x \in B : g(x) = 0\}$. Note que para obtener el dominio de $\frac{f}{g}$, se deben eliminar de $A \cap B$, aquellos puntos donde g se anula.

Ejemplo 3.2.46 *Considere las funciones definidas por* $f(x) = \sqrt{x+7}$, $g(x) = x^4 - 1$, *donde el dominio de* f *está dado por*

$$A = \{x \in \mathbb{R} : x + 7 \geq 0\} = [-7, +\infty[\,,$$

mientras el de g *es* $B = \mathbb{R}$. *El dominio de* $\frac{f}{g}$ *es*

$$\begin{aligned} D &= A \cap B - \{x \in B : g(x) = 0\} \\ &= [-7, +\infty[- \{-1, 1\}\,, \end{aligned}$$

y se tiene

$$\frac{f}{g} : D \to \mathbb{R}, \quad \left(\frac{f}{g}\right)(x) = \frac{\sqrt{x+7}}{x^4 - 1}.$$

3.3 Ejercicios

1. Sea E un conjunto y sea $f : E \to \mathcal{P}(E)$ una función cualquiera. Se define

   $$A = \{a \in E : a \notin f(a)\}\,.$$

   Demuestre que A no tiene pre-imagen bajo f, y que por lo tanto f no puede ser sobreyectiva.

2. Demuestre que la función identidad en A es la única relación binaria de A en A que es reflexiva, simétrica y antisimétrica.

3. Sea $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ definida por $f(n) = (n, n+1)$. Es f sobreyectiva? inyectiva?

4. Sea $f : E \to B$ una función. En E se define la relación $\mathcal{R}$ por: $a\mathcal{R}b \Leftrightarrow f(a) = f(b)$. Muestre que $\mathcal{R}$ es de equivalencia. Describa las clases de equivalencia en los siguientes casos:

   (a) $E = B = \mathbb{Z}$, $f(x) = |x|\,.$
   (b) $E = B = \mathbb{R}$, $f(x) = [\![x]\!]$ (parte entera de x).
   (c) $E = B = \mathbb{R}$, $f(x) = x - [\![x]\!]$ (parte fraccionaria de x).
   (d) $E = B = \mathcal{P}(\mathbb{N})$, $f(A) = A \cap \{1, 2, 3\}\,.$

5. Sea $f : \mathbb{N} \to \mathbb{N}$ definida por $f(n) = 2n$, y sea $g : \mathbb{N} \to \mathbb{N}$ definida por:

   $$g(n) = \text{ el menor primo que divide a } n.$$

   Halle $(g \circ f)(n)$ para todo $n \in \mathbb{N}$.

6. Resuelva el ejercicio anterior cambiando $2n$ por $3n$, en la definición de f.

7. Si $f : A \to B$ y $g : B \to C$ son inyectivas, muestre que $g \circ f$ es inyectiva. Haga lo mismo con sobreyectivas.

8. Si $f : A \to B$ y $g : B \to C$ son invertibles, muestre que $g \circ f$ lo es, y que

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

9. De las siguientes funciones de $\mathbb{N}$ en $\mathbb{N}$, diga cuáles son inyectivas, halle el ámbito y diga cuáles son sobreyectivas.

   (a) $f(n) = n + 5, amb\,(f) = N \setminus \{0, 1, 2, 3, 4\} \neq N$
   (b) $g(n) = n$ para $n \leq 5$, y $g(n) = n - 5$ para $n > 5$.
   (c) $h(n) = \frac{n}{2}$ si n es par, y $h(n) = \frac{n+1}{2}$ si n es impar.
   (d) $f(n) = 7n$.
   (e) $f(n) = n^2 + n + 1$.

10. Sea $f : \mathbb{N} \to \mathbb{N}$ definida por $f(n) = n^3 + 3n^2 + 40$. Muestre que f es inyectiva.

11. Sea $f : \mathbb{N} \to \mathbb{N}$ definida por $f(n) = n^3 - 3n^2 + 40$. Muestre que f no es inyectiva, pero si se restringe el dominio a $\mathbb{N}^*$, la función resultante sí es inyectiva.

12. Sea $E \neq \emptyset$ y sea $f : \mathcal{P}(E) \times \mathcal{P}(E) \to \mathcal{P}(E)$ definida por $f(A, B) = A \cup B$. ¿Es f inyectiva? ¿sobreyectiva?

13. Sea $f : \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{N})$ definida por $f(A) = A \cup \{0\}$. ¿Es f inyectiva? ¿sobreyectiva?

14. Sea $f : \mathcal{P}(A) \times \mathcal{P}(B) \to \mathcal{P}(A \times B)$ definida por $f(X, Y) = X \times Y$. ¿Es f inyectiva? ¿sobreyectiva?

15. En cada caso, halle el "dominio máximo" sobre el cual se puede definir una función usando la fórmula proporcionada:

   (a) $f(x) = \sqrt{x} + \sqrt{3 - x}$,
   (b) $f(x) = \sqrt{-x} + \dfrac{1}{\sqrt{x + 2}}$,
   (c) $f(x) = \left((|x| - 5)^2 - 4 \right)^{-1/2}$,
   (d) $f(x) = \sqrt{[\![x]\!] - x}$,
   (e) $f(x) = \sqrt{(-1)^{[\![x]\!]}} + \sqrt{x\,(5 - x)}$,
   (f) $f(x) = (-1)^{1/[\![x]\!]} + \sqrt{2x + |x|}$.

16. Sea $f : D \to \mathbb{R}$ definida por

$$f(x) = \frac{\sqrt{(x+1)(x+2)}}{\sqrt{|x| - x}},$$

donde D es el dominio máximo. Determine el mayor intervalo $J \subseteq D$ tal que $-5 \in J$.

17. Repita el ejercicio anterior, ahora con $f(x) = \frac{\sqrt{4-x}}{|x-1|-1}$, si se sabe que $3 \in J$.

18. Para las siguientes funciones, determine inyectividad, sobreyectividad, crecimiento, existencia de la inversa. Justifique su respuesta, y halle la inversa cuando exista.

    (a) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2 + 1$,
    (b) $f : \mathbb{R} \to [2, \infty[$, $f(x) = x^2 + 2$,
    (c) $f : [0, \infty[\to]-\infty, 1]$, $f(x) = 1 - x^2$,
    (d) $f :]0, \infty[\to]0, \infty[$, $f(x) = \dfrac{1}{x}$,
    (e) $f :]2, \infty[\to]1, \infty[$, $f(x) = \dfrac{x+1}{x-2}$,
    (f) $f : \mathbb{R} - \{0\} \to \mathbb{R}$, $f(x) = \dfrac{x}{|x|}$,
    (g) $f : \mathbb{R} \to [0, \infty[$, $f(x) = x + |x|$.
    (h) $f : \mathbb{R}^* \to \mathbb{R}^*$ $f(x) = x + \frac{1}{x}$.

19. Una función $f : \mathbb{R} \to \mathbb{R}$ se llama par si satisface: $f(-x) = f(x)$, y se llama impar si $f(-x) = -f(x)$, para todo $x \in \mathbb{R}$. Diga cuáles de las siguientes funciones son pares o impares:

    (a) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2 + 1$
    (b) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = \dfrac{1}{x}$
    (c) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2 + 2x$
    (d) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = |x|$
    (e) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^3 + 2x$
    (f) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = \dfrac{x^4}{x^2 + 2}$

20. Sean f g funciones de $\mathbb{R}$ en $\mathbb{R}$. Demuestre que

    (a) Si f y g son pares entonces $f + g$, fg y $f \circ g$ son pares.
    (b) Si f y g son impares, entonces $f + g$ y $f \circ g$ son impares, mientras que fg es par.

(c) Si f es par y g es impar, entonces $f-g$ es par.

21. En este ejercicio usted se va a convencer de que la gráfica de función $f(x)=x^2$, tiene la forma descrita en el ejemplo 3.2.6.

    (a) Demuestre que para $a<b$ se tiene

    $$\left(\frac{a+b}{2}\right)^2 < (a+b)\left(\frac{a+b}{2}-a\right)+a^2.$$

    Note que el lado izquierdo es $f\left(\frac{a+b}{2}\right)$, mientras que el lado derecho es $g\left(\frac{a+b}{2}\right)$, donde $g(x)=(a+b)(x-a)+a^2$. ¿Cuál es la gráfica de g?

    (b) Más generalmente, demuestre que $f(x)<g(x)$, para $a<x<b$. Sug. $g(x)-f(x)=(b-x)(x-a)$.

    (c) Concluya que el segmento de recta que une los puntos $\left(a,a^2\right)$ y $\left(b,b^2\right)$ está por encima de la gráfica de f.

22. Grafique la función $f:[0,\infty[\to[0,\infty[$, definida por $f(x)=\sqrt{x}$. Sug. Esta es la inversa de $g(x)=x^2$. Use esto para graficar las funciones dadas a continuación, en sus respectivos dominios:

    (a) $f:[-2,\infty[\to\mathbb{R}$, $f(x)=\sqrt{x+2}$.
    (b) $f:[3,\infty[\to\mathbb{R}$, $f(x)=\sqrt{x-3}$.
    (c) $f:[-\infty,1[\to\mathbb{R}$, $f(x)=\sqrt{1-x}$.
    (d) $f:[0,\infty[\to\mathbb{R}$, $f(x)=4+\sqrt{x}$.
    (e) $f:[-\infty,2[\to\mathbb{R}$, $f(x)=3\left(1-\sqrt{2-x}\right)$.

23. En cada caso, grafique la función definida en $\mathbb{R}$ mediante la fórmula dada.

    (a) $f(x)=|2x+1|-3$,
    (b) $f(x)=5-(x-3)^2$,
    (c) $f(x)=\left|5-4x-x^2\right|$,
    (d) $f(x)=\left|x^2-3x+2\right|-3x$.
    (e) $f(x)=\left|x^2-3x+2\right|-x^2$.
    (f) $f(x)=\left|x^2-3x+2\right|+x^2$.

24. Halle $f\circ g$ y $g\circ f$, en sus respectivos dominios:

    (a) $f(x)=\sqrt{x}$, $g(x)=x^2-1$,

(b) $f(x) = -\dfrac{1}{x}$, $g(x) = \dfrac{1}{x}$,

(c) $f(x) = -2$, $g(x) = x^5 + 3x^2 + 1$,

(d) $f(x) = |x|$, $g(x) = \begin{cases} 1 & \text{si } x \in \mathbb{Q} \\ -1 & \text{si } x \in \mathbb{I}. \end{cases}$

25. Sea $f : \mathbb{R} \to]-1, 1[$ definida por $f(x) = \dfrac{x}{\sqrt{x^2+1}}$. Demuestre que f está bien definida; es decir, que efectivamente $f(x) \in]-1, 1[$ para cada $x \in \mathbb{R}$. Demuestre que f es una biyección.

26. Repita el ejercicio anterior con $f(x) = \dfrac{x}{1+|x|}$.

27. Sean $f : A \to B$ y $g : B \to A$ tales que $(g \circ f)(x) = x$, $\forall x \in A$. Demuestre que f es inyectiva y g es sobreyectiva.

28. Si f está definida por
$$f(x) = \begin{cases} 2x^3 + 1 & \text{si } x < 1 \\ x + 2 & \text{si } x \geq 1 \end{cases}$$
calcule $f(0) + f(1) + f(2)$. Calcule además $f(1 - f(2 + f(0)))$.

29. Sea $f : \mathbb{R} - \{-b, b\} \to \mathbb{R}$, definida por
$$f(x) = \frac{3x^2 - a}{x^2 - b^2}$$
¿Qué condiciones deben satisfacer a y b para que $y_0 = 2$ pertenezca al rango de f?

30. Sea f una función de A en $\mathbb{R}$, y sea c es una constante. Se define $cf : A \to \mathbb{R}$ por $(cf)(x) = cf(x)$. Note que $f - g = f + (-1)g$. Calcule $f + g$, $2f + 3g$, $f - g$, fg, $\frac{f}{g}$, en sus respectivos dominios, para:

(a) $f(x) = \dfrac{1}{x}, g(x) = 1 - \dfrac{1}{x}$.

(b) $f(x) = \dfrac{2x-3}{4x-1}, g(x) = \dfrac{x+1}{4x-1}$

31. Sea $F(x) = 2 + 3\,\mathrm{sen}^2\left(1 + 3\sqrt{4 + 7x^3}\right)$. Determine las funciones: $f_1, f_2, ..., f_{10}$ tal que $F = f_1 \circ f_2 \circ ... \circ f_{10}$.

32. Sea $f : \mathbb{R} \to \mathbb{R}$ y $g : \mathbb{R} \to \mathbb{R}$. Determinar $f + g$, $f \cdot g$ y $f \circ g$ en los siguientes casos:

(a) $f(x) = \begin{cases} 4x + 3 & \text{si } x < 1 \\ x^3 & \text{si } x \geq 1 \end{cases}$, $g(x) = x + 2$

(b) $f(x) = \begin{cases} 3x+2 & \text{si } x \leq 0 \\ 5x+4 & \text{si } x > 0 \end{cases}$, $g(x) = \begin{cases} 2x+1 & \text{si } x \leq 0 \\ -x+2 & \text{si } x > 0 \end{cases}$

(c) $f(x) = \begin{cases} x & \text{si } x < 0 \\ 2x & \text{si } x \geq 0 \end{cases}$, $g(x) = \begin{cases} x+1 & \text{si } x < -1 \\ 4x+4 & \text{si } x \geq -1 \end{cases}$

(d) $f(x) = \begin{cases} x^2 & \text{si } x < 0 \\ -x^2 & \text{si } x \geq 0 \end{cases}$, $g(x) = \begin{cases} -x^2+1 & \text{si } x < 0 \\ x^2-1 & \text{si } x \geq 0 \end{cases}$

(e) $f(x) = \begin{cases} x & \text{si } x < -1 \\ x^3 & \text{si } -1 \leq x \leq 1 \\ 2x-1 & \text{si } x > 1 \end{cases}$, $g(x) = \begin{cases} -x^2+1 & \text{si } x < 0 \\ x^2-1 & \text{si } x \geq 0 \end{cases}$

(f) $f(x) = \begin{cases} -x & \text{si } x < -1 \\ x^4 & \text{si } -1 \leq x \leq 1 \\ x & \text{si } x > 1 \end{cases}$, $g(x) = \begin{cases} x & \text{si } x < -1 \\ x^5 & \text{si } -1 \leq x \leq 1 \\ 2x-1 & \text{si } x > 1 \end{cases}$

Parte II

Construcción de conjuntos numéricos

Capítulo 4

Los números naturales

4.1 Introducción

El estudio sistemático de los números naturales puede hacerse por diferentes vías. Por ejemplo, haciendo la construcción mediante la teoría de conjuntos, o a través de una presentación axiomática, sustentada en los axiomas de Peano. Aquí se hará una presentación más informal, buscando sobre todo aprovechar el conocimiento que el estudiante tiene, de las propiedades básicas de los números naturales. La presentación comienza enunciando el principio de inducción, y tratando de familiarizar al lector con este principio, por medio de ejemplos y la deducción de otros resultados como consecuencia del mismo. El lector interesado en la presentación axiomática, puede consultar el apéndice.

4.2 El principio de inducción

4.2.1 Enunciado y ejemplos

La idea intuitiva del principio de inducción es que $\mathbb{N}$ es el menor conjunto que satisface:

(a) $0 \in A$.

(b) Para todo $n \in A$ se tiene $n + 1 \in A$.

Un conjunto A se llama *inductivo* si satisface estas dos propiedades.

Principio de inducción
Si A es un subconjunto inductivo de $\mathbb{N}$, entonces $A = \mathbb{N}$.

En otras palabras, ningún subconjunto propio de $\mathbb{N}$ es inductivo. Como ya lo mencionamos, nuestro primer objetivo es familiarizarnos con este principio. Los ejemplos que siguen persiguen ese objetivo.

Ejemplo 4.2.1 *Demostrar que* $2^n \geq n+1$, *para todo* $n \in \mathbb{N}$.
La afirmación quedará demostrada si comprobamos que el conjunto

$$A = \{n \in \mathbb{N} : 2^n \geq n+1\}$$

es igual a $\mathbb{N}$. *De acuerdo con el principio de inducción, bastará con demostrar que dicho conjunto es inductivo.*
(a) *En primer lugar,* $0 \in A$ *puesto que* $2^0 = 1 \geq 0+1$.
(b) *Ahora supongamos que* $n \in A$, *esto es* $2^n \geq n+1$. *Entonces*

$$2^{n+1} = 2 \cdot 2^n \geq 2\,(n+1) = 2n+2 \geq n+2 = (n+1)+1,$$

lo que demuestra que $n+1 \in A$.
Por el principio de inducción se concluye entonces que $A = \mathbb{N}$. *Consecuentemente, la desigualdad es válida para todo* $n \in \mathbb{N}$.

Ejemplo 4.2.2 *Demostrar que para todo* $n \in \mathbb{N}$ *se tiene*

$$0 + 1 + \cdots + n = \frac{n(n+1)}{2}.$$

Se trata de demostrar que el conjunto

$$A = \left\{n \in \mathbb{N} : 0 + \cdots + n = \tfrac{n(n+1)}{2}\right\}$$

es igual a $\mathbb{N}$. *Usando el principio de inducción, es suficiente demostrar que el conjunto* A *es inductivo.*
(a) *Para* $n = 0$, *la suma del lado izquierdo solo tiene un término, y es igual a* 0, *mientras que el lado derecho es* $\frac{0(0+1)}{2} = 0$. *Entonces* $0 \in A$.
(b) *Si* $n \in A$, *se tiene*

$$0 + \cdots + n = \frac{n(n+1)}{2},$$

y debemos demostrar que $n+1 \in A$. *Veamos:*

$$\begin{aligned} 0 + \cdots + (n+1) &= (0 + \cdots + n) + (n+1) \\ &= \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1) + 2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2}. \end{aligned}$$

Esto demuestra que efectivamente $n+1 \in A$. *Por el principio de inducción se concluye que* $A = \mathbb{N}$, *como se deseaba.*

Ejemplo 4.2.3 *Demostrar que todo $n \in \mathbb{N}$ tiene la forma $2k$ ó $2k+1$, para algún $k \in \mathbb{N}$. Definimos el conjunto*

$$A = \{n \in N : n \text{ tiene la forma } 2k \text{ ó } 2k+1\}.$$

*Note que $0 \in A$, pues $0 = 2k$, con $k = 0$. Entonces A satisface la propiedad **(a)**. Por otro lado, si $n \in A$, entonces n tiene una de las dos formas $2k$ ó $2k+1$. Si $n = 2k$ se sigue que $n+1 = 2k+1$. Si por el contrario n tiene la forma $2k+1$, entonces $n+1 = 2(k+1)$, donde $k+1 \in \mathbb{N}$. En ambos casos concluimos que $n+1 \in A$, así que A satisface también la propiedad **(b)**. Luego $A = \mathbb{N}$ por el principio de inducción.*

Nota: En la práctica, no se acostumbra definir el conjunto A explícitamente, sino que se demuestra la propiedad planteada para $n = 0$, y luego se demuestra que si se cumple para n, debe cumplirse para $n+1$. Esta última parte se conoce como el paso inductivo.

Ejemplo 4.2.4 *Demostrar que $n^3 + 5n$ es divisible por 6, para todo $n \in \mathbb{N}$.*
En efecto, para $n = 0$ se tiene $n^3 + 5n = 0$, el cual es divisible por 6. Para el paso inductivo, se supone que n satisface la rpopiedad, lo cual quiere decir que $n^3 + 5n = 6k$, para algún $k \in \mathbb{N}$. Luego

$$\begin{aligned} (n+1)^3 + 5(n+1) &= \left(n^3 + 5n\right) + 3n^2 + 3n + 6 \\ &= 6k + 3n(n+1) + 6 \\ &= 6(k+1) + 3n(n+1). \end{aligned}$$

Como $n(n+1)$ es siempre par (¿por qué?), se tiene que $3n(n+1)$ es múltiplo de 6, y consecuentemente $(n+1)^3 + 5(n+1)$ es también múltiplo de 6.

4.2.2 Extensiones y consecuencias

El principio de inducción es también aplicable a propiedades que son válidas a partir de cierto valor de n. Veamos el siguiente resultado, que llamaremos *inducción truncada*.

Lema 4.2.1 ***(Inducción truncada)*** *Sea $A \subseteq \mathbb{N}$, y sea $N \in \mathbb{N}$ tales que*
(a) *$N \in A$.*
(b) *Para todo $n \in A$ tal que $n \geq N$, se tiene $n+1 \in A$.*
Entonces A contiene todos los naturales a partir de N. Esto es:

$$\{n \in \mathbb{N} : n \geq N\} \subseteq A.$$

Demostración
Si $N = 0$, el resultado es precisamente el principio de inducción.
Si $N > 0$ considere el conjunto

$$B = A \cup \{0, 1, \ldots, N-1\}.$$

Entonces claramente B es inductivo, y por el principio de inducción se sigue que $B = \mathbb{N}$. Ahora, dado $n \in \mathbb{N}$ tal que $n \geq N$, se tiene $n \in B - \{0, 1, \ldots, N-1\}$, lo que demuestra que $n \in A$. $\square$

Los siguientes ejemplos hacen uso de este resultado.

Ejemplo 4.2.5 *Demostrar que $n + 3 < 2^n$, para todo $n \geq 3$.*
Nótese que la desigualdad es falsa para $n < 3$. Para $n = 3$ sí es válida, pues tenemos $3+3 = 6 < 2^3 = 8$. Ahora, si la desigualdad se cumple para cierto $n \geq 3$, tenemos $n+3 < 2^n$, y luego

$$(n+1) + 3 = (n+3) + 1 < 2^n + 1 < 2^n + 2^n = 2^{n+1}.$$

Esto demuestra que la desigualdad también se cumple para $n + 1$. Por el lema anterior, la desigualdad es válida para todo $n \geq 3$.

Ejemplo 4.2.6 *Demostrar que $n^2 \leq 2^n$, para todo $n \geq 4$.*
Note que aunque la desigualdad es válida para $n = 1$ y $n = 2$, no lo es para $n = 3$. Es de esperarse entonces que para el paso inductivo se requiera usar el hecho que $n \geq 4$. Para $n = 4$ se tiene $4^2 = 16 = 2^4$, así que se cumple $4^2 \leq 2^4$.
Ahora supongamos que $n^2 \leq 2^n$ para algún $n \geq 4$. Entonces

$$2^{n+1} = 2 \cdot 2^n \geq 2n^2.$$

La desigualdad para $n+1$ quedará demostrada si demostramos que $2n^2 \geq (n+1)^2$, lo cual es equivalente a $n^2 - 2n - 1 \geq 0$. Esto es cierto para $n \geq 4$, puesto que

$$n^2 - 2n - 1 = n(n-2) - 1 \geq 4 \cdot 2 - 1 = 7 > 0.$$

Esto demuestra entonces que $2n^2 \geq (n+1)^2$, y luego

$$2^{n+1} \geq 2n^2 \geq (n+1)^2.$$

En algunos ejemplos, al demostrar que $n + 1 \in A$, se debe hacer uso no sólo del hecho que $n \in A$, sino también de que $n - 1 \in A$, o en general de que $k \in A$ para $k \leq n$. El siguiente resultado permite hacer este tipo de razonamientos.

Lema 4.2.2 ***(Principio de inducción completa)*** *Sea $A \subseteq \mathbb{N}$ que satisface las siguientes propiedades:*

1. *$0 \in A$.*
2. *Si $k \in A$ para todo $k \leq n$, se sigue que $n + 1 \in A$.*

Entonces $A = \mathbb{N}$.

Demostración
Se define el conjunto

$$B = \{n \in \mathbb{N} : k \in A \text{ para todo } k \leq n\}.$$

Nótese que $B \subseteq A$, y por la propiedad **1** se tiene $0 \in B$. Por otro lado, supongamos que $n \in B$. Entonces por definición tenemos que $k \in A$ para todo $k \leq n$, y por la propiedad **2** se concluye que $n + 1 \in A$. Consecuentemente

$$k \in A \text{ para todo } k \leq n + 1,$$

lo que significa $n + 1 \in B$. Se ha demostrado entonces que B es inductivo, y por el principio de inducción se sigue que $B = \mathbb{N}$. Finalmente, dado que $\mathbb{N} = B \subseteq A \subseteq \mathbb{N}$, se concluye que $A = \mathbb{N}$. □

Ejemplo 4.2.7 *Todo natural $n \geq 2$ tiene al menos un divisor primo.*
Recordemos que los primos son los naturales que poseen exactamente dos divisores en $\mathbb{N}$ (el 1 y el número mismo), y en particular 1 no es primo. Procedamos usando inducción completa.

- *Si $n = 2$, entonces $p = 2$ es divisor primo de n.*
- *Asumiendo que todo $k \in \{2, \ldots, n\}$ tiene al menos un divisor primo, demostremos que $n + 1$ también tiene al menos un divisor primo. Hay dos posibilidades:*

  Si $n + 1$ es primo, entonces $p = n + 1$ es un divisor primo de $n + 1$.

  Si $n + 1$ no es primo, entonces se puede escribir como

  $$n + 1 = k \cdot l,$$

  donde k es tal que $1 < k < n + 1$. Como esto implica $2 \leq k \leq n$, por la hipótesis de inducción completa se sigue que k tiene al menos un divisor primo p. Digamos $k = p \cdot m$, donde p es primo. Luego

  $$n + 1 = k \cdot l = p \cdot (ml),$$

  así que p es un divisor primo de $n + 1$.

Por el principio de inducción completa obtenemos el resultado.

Otra propiedad importante de los números naturales es el principio del buen orden. Para establecerlo necesitamos primero la siguiente definición.

Definición 4.2.1 *Dado $A \subseteq \mathbb{N}$, decimos que n_0 es el primer elemento de A si satisface:*

1. $n_0 \in A$.
2. $n_0 \leq n$, $\forall n \in A$.

Nótese que de existir el primer elemento, este debe ser único. Note además que si $0 \in A$, entonces 0 es el primer elemento de A.

Lema 4.2.3 ***(Principio del buen orden)*** *Si A es un subconjunto no vacío de $\mathbb{N}$, entonces A tiene primer elemento.*

Demostración
Supongamos que A no tiene primer elemento, y definamos

$$B = \mathbb{N} - A = \{n \in \mathbb{N} : n \notin A\}.$$

Tenemos que $0 \in B$, pues de lo contrario 0 sería el primer elemento de A. Ahora, si $k \in B$ para todo $k \leq n$, entonces $n+1 \in B$, pues de lo contrario $n+1$ sería el primer elemento de A. Por el principio de inducción completa se sigue que $B = \mathbb{N}$, y consecuentemente $A = \emptyset$. Como esto contradice la hipótesis, A debe tener primer elemento. □

Como una aplicación de este hecho, demostremos el algoritmo de la división.

Lema 4.2.4 ***(Algoritmo de la división)*** *Para a y b naturales, con $b > 0$, existen naturales q y r tales que*

$$a = bq + r, \quad 0 \leq r < b.$$

Demostración
En efecto, considere el conjunto

$$A = \{n \in \mathbb{N} : n = a - bq, \text{ para algún } q \in \mathbb{N}\}.$$

Note que $A \neq \emptyset$, pues $a \in A$ (tomando $q = 0$). Por el principio del buen orden, existe el primer elemento de A, que denotaremos por r. Como $r \in A$, existe $q \in \mathbb{N}$ tal que $r = a - bq$. Ahora, si r no fuera menor que b, tendríamos $r - b \in \mathbb{N}$, pero $r - b = a - b(q+1)$, así que $r - b$ sería elemento de A, contradiciendo el hecho que r es el primer elemento de A. Debe tenerse entonces $r < b$. □

Es un buen ejercicio para el lector, demostrar que q y r son únicos. El número q es el cociente que se obtiene mediante la división euclideana de a por b, y r es el residuo respectivo.

Ejemplo 4.2.8 *Si $a = 145$ y $b = 15$, tenemos $a = b \cdot 9 + 10$, así que $q = 9$ y $r = 10$.*

4.2.3 Definiciones por recurrencia

Muchas veces, para definir una función $f : \mathbb{N} \to A$, se hace uso implícito del principio de inducción. Por ejemplo, cuando se define

$$a^n = a \cdot a \cdot \cdots \cdot a \quad (n \text{ veces}),$$

realmente se está pensando en la definición: $a^0 = 1$, $a^{n+1} = a^n \cdot a$. Esto define a^0, y asumiendo que a^n está definido, permite definir a^{n+1}. El principio de inducción garantiza que esta es una buena definición de la función

$$f : \mathbb{N} \to \mathbb{R},\ f(n) = a^n.$$

En general, dado un conjunto A, un elemento $a \in A$, y una función $g : \mathbb{N} \times A \to A$, podemos definir una función $f : \mathbb{N} \to A$ mediante la fórmula recurrente:

$$f(0) = a, \qquad f(n+1) = g(n, f(n)). \tag{4.1}$$

Usando el principio de inducción se puede demostrar el siguiente principio.

Principio de recurrencia
Con estas hipótesis, existe una única función $f : \mathbb{N} \to A$ que satisface la fórmula recurrente (4.1).

En lo que sigue hacemos uso de este principio. Para una demostración de este principio, se puede consultar el apéndice.

Ejemplo 4.2.9 *(El factorial) Se define $0! = 1$, y para $n \in \mathbb{N}$ se define*

$$(n+1)! = (n+1) \cdot n!.$$

Tenemos entonces $1! = 1 \cdot 0! = 1$, $2! = 2 \cdot 1! = 2 \cdot 1$, $3! = 3 \cdot 2 \cdot 1$, y en general $n! = n \cdot (n-1) \cdots 3 \cdot 2 \cdot 1$. Aquí se tiene $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ definida por $g(n, x) = (n+1)\, x$, $a = 1$.

Para familiarizarnos con esta definición, veamos algunos ejemplos.

Ejemplo 4.2.10 *Demostrar que $2^n < n!$, para todo $n \geq 4$.*
Para $n = 4$ tenemos $2^4 = 16 < 24 = 4!$. Ahora supongamos que $2^n < n!$ para algún $n \geq 4$. Entonces

$$2^{n+1} = 2 \cdot 2^n < 2 \cdot n! < 4 \cdot n! < (n+1) \cdot n! = (n+1)!,$$

con lo que $n+1$ también satisface la desigualdad. El principio de inducción truncada se encarga del resto.

Ejemplo 4.2.11 *Dada una función $f : \mathbb{N} \to \mathbb{R}$, podemos definir la suma*

$$S_n = f(0) + \ldots + f(n)$$

en forma recursiva:

$$S_0 = f(0), \quad S_{n+1} = S_n + f(n+1).$$

Las funciones de dominio $\mathbb{N}$ se llaman sucesiones, y se acostumbra usar la notación $a_k = f(k)$. La suma anterior se denota entonces

$$S_n = a_0 + \ldots + a_n,$$

y en forma más resuminda

$$S_n = \sum_{k=0}^{n} a_k$$

(se lee: "suma desde k igual 0 hasta n de los a_k"). Note que por definición se tiene

$$\sum_{k=0}^{n+1} a_k = \sum_{k=0}^{n} a_k + a_{n+1}.$$

Si se comienza en 1 en vez de 0, se denota

$$\sum_{k=1}^{n} a_k = a_1 + \ldots + a_n.$$

Ejemplo 4.2.12 *Un caso particular del ejemplo anterior es la suma del ejemplo 4.2.2:*

$$\sum_{k=0}^{n} k = \frac{n(n+1)}{2}.$$

Ejemplo 4.2.13 *Demostrar que para todo $n \in \mathbb{N}$ se tiene*

$$\sum_{k=0}^{n} k \cdot k! = (n+1)! - 1.$$

Para $n = 0$ la suma del lado izquierdo es $0 \cdot 0! = 0$, mientras que al lado derecho tenemos $(0+1)! - 1 = 0$. Entonces la igualdad es válida para $n = 0$.
Supongamos que la igualdad es válida para n, y probémosla para $n+1$. Por definición se tiene

$$\sum_{k=0}^{n+1} k \cdot k! = \sum_{k=0}^{n} k \cdot k! + (n+1) \cdot (n+1)!,$$

y por hipótesis de inducción se sigue que

$$\begin{aligned} \sum_{k=0}^{n+1} k \cdot k! &= (n+1)! - 1 + (n+1) \cdot (n+1)! \\ &= (1+n+1)(n+1)! - 1 \\ &= (n+2)(n+1)! - 1 \\ &= (n+2)! - 1. \end{aligned}$$

Esto demuestra la igualdad para $n+1$, y por el principio de inducción se sigue que es válida para todo $n \in \mathbb{N}$.

4.2.4 Sobre los conjuntos finitos

A menudo se usa la notación

$$A = \{a_1, \ldots, a_n\} \tag{4.2}$$

para expresar que el conjunto A es finito y tiene exactamente n elementos. En este caso diremos que la cardinalidad de A es n, y denotaremos $|A| = n$. Para precisar esto mejor, definimos $S_0 = \emptyset$ y

$$S_n = \{k \in \mathbb{N} : 1 \leq k \leq n\}, \text{ para } n \geq 1.$$

Intuitivamente, A tiene n elementos si al contar sus elementos nos da n. Pero qué significa contar en matemática? Cuando contamos, en realidad lo que hacemos es asociar los elementos contados con los números naturales, comenzando en orden desde $n = 1$. Diremos entonces que A tiene n elementos si existe una función biyectiva $f : S_n \to A$, para algún $n \in A$.Para darle rigor a la definición anterior, debemos sin embargo tomar ciertos cuidados. En particular, la definición no debe ser ambigua, esto es, debemos demostrar que no hay dos valores distintos de n que satisfagan la definición para el mismo conjunto. Para hacer eso, el concepto de equipotencia es de gran ayuda.

Definición 4.2.2 *Decimos que el conjunto A es equipotente al conjunto B, si existe una biyección $f : A \to B$. En tal caso se escribe $A \sim B$.*

Es un buen ejercicio demostrar que la relación "$\sim$" es de equivalencia. En particular es simétrica, y entonces cuando $A \sim B$, podemos decir en forma simétrica que A y B son equipotentes.

Ejemplo 4.2.14 *El conjunto $\mathbb{P}$ de los naturales pares es equipotente a $\mathbb{N}$. En efecto, considere la función*

$$\varphi : \mathbb{N} \to \mathbb{P}, \quad \varphi(n) = 2n$$

Le dejamos al lector la tarea de comprobar que φ es una biyección.

Ejemplo 4.2.15 *El conjunto $A = \{2, 4, 6, \ldots, 40\}$ es equipotente a S_{20}. Basta con ver que la función $f = S_{20} \to A$ definida por $f(n) = 2n$, es biyectiva.*

Los siguientes lemas nos permitirán darle rigor a la definición de conjunto finito.

Lema 4.2.5 *Si $a, b \in A$, entonces $A - \{a\} \sim A - \{b\}$.*

Demostración
Considere la función $\varphi : A - \{a\} \to A - \{b\}$ definida por

$$\varphi(x) = \begin{cases} a & \text{si } x = b \\ x & \text{si } x \neq b \end{cases}$$

Esta función es claramente biyectiva. □

Lema 4.2.6 *Si $A \sim B$, $a \in A$, $b \in B$, entonces $A - \{a\} \sim B - \{b\}$.*

Demostración
Sea $f : A \to B$ una biyección. La función $g : A - \{a\} \to B - \{f(a)\}$ definida por $g(x) = f(x)$ es biyectiva (g es la restricción de f). Entonces $A - \{a\} \sim B - \{f(a)\}$, y sabemos por el lema anterior que $B - \{f(a)\} \sim B - \{b\}$. La transitividad de la relación de equipotencia se encarga del resto. □

Note que el único conjunto equipotente a $\emptyset$, es él mismo. Tomando $B = S_n$ y $b = n$ en el lema anterior, se obtiene el siguiente resultado.

Lema 4.2.7 *Si $A \sim S_n$ y $a \in A$, entonces $A - \{a\} \sim S_{n-1}$.*

Usando este resultado, no es difícil demostrar la unicidad de n en la siguiente definición (ver ejercicio 23).

Definición 4.2.3 *Un conjunto A se llama finito si es equipotente a algún S_n, con $n \in \mathbb{N}$. En tal caso decimos además que A tiene n elementos, y escribimos $|A| = n$.*

Teorema 4.1 *Dado $A \subseteq \mathbb{R}$ finito y no vacío, existe un elemento en A que es mayor que todos los demás. A tal elemento lo llamaremos el máximo de A, y lo denotaremos por* $\max A$.

Demostración
Procederemos usando inducción sobre $n = |A|$, veamos:
Si $n = 1$, tenemos $A = \{a\}$, así que $\max A = a$.
Si el resultado es válido para n, consideremos un conjunto A con $n + 1$ elementos. Tomemos $a \in A$ y definamos $B = A - \{a\}$. Como $|B| = n$, la hipótesis de inducción dice que existe $b = \max B$. Ahora hay dos posibilidades:
Si $a > b$, entonces $a = \max A$. En caso contrario tenemos $b = \max A$. □

Un argumento similar demuestra que todo conjunto finito no vacío A, posee un mínimo, denotado por $\min A$.

Ejemplo 4.2.16 *Si $A = \{n^2 : n \in \mathbb{N},\ n < 7\}$, entonces* $\min A = 0$, $\max A = 36$.

Definición 4.2.4 *Decimos que un conjunto A es infinito si no es finito. Es decir, si no existe $n \in \mathbb{N}$ tal que $A \sim S_n$.*

Teorema 4.2 *$\mathbb{N}$ es infinito.*

Demostración
Por el teorema anterior, si $\mathbb{N}$ fuera finito existiría $n = \max \mathbb{N}$. Pero como $n+1 \in \mathbb{N}$, se tendría $n + 1 \leq n$, lo cual es contradictorio. Esto demuestra el resultado. □

4.2.5 Ejercicios

1. Demuestre, usando el principio de inducción, que para cada $n \in \mathbb{N}$ se tiene

$$1 + \frac{1}{2} + \cdots + \frac{1}{2^n} = 2 - \frac{1}{2^n}.$$

2. Más generalmente, si $r \neq 1$, demuestre que para todo $n \in \mathbb{N}$ se riene

$$1 + r + \cdots + r^n = \frac{1 - r^{n+1}}{1 - r}.$$

3. Use el ejercicio anterior para demostrar la identidad

$$a^n - b^n = (a - b)\left(a^{n-1} + a^{n-2}b + \ldots + b^{n-1}\right), \tag{4.3}$$

   para $a, b \in \mathbb{R}$, $n \in \mathbb{N}$. Concluya que si $a, b \in \mathbb{N}$ y $a > b$, entonces $a^n - b^n$ es múltiplo de $a - b$.

4. Dmuestre las siguientes desigualdades usando inducción:

   (a) $1 + 2^n \leq 3^n$ para $n \geq 1$
   (b) $1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{2^n} \geq \frac{n+2}{2}$, para todo $n \in \mathbb{N}$
   (c) $2^n \geq n^2 + 3n + 7$, para $n \geq 6$
   (d) $2n - 3 \leq 2^{n-2}$ para todo $n \geq 5$.

5. ¿Para cuáles n es válida la desigualdad $n^2 + 3 < 2^n$? Demuestre su afirmación.

6. Demuestre que para $n \in \mathbb{N}^*$ se tiene $1 + 3 + 5 + \ldots + (2n - 1) = n^2$. Use esto para calcular $1 + 3 + 5 + \ldots + 99$.

7. Demuestre por inducción que $f(x) = x^n$ es estrictamente creciente en $[0, \infty[$, para todo $n \in \mathbb{N}$.

8. Resuelva el ejercicio anterior usando la identidad (4.3).

9. Demuestre usando inducción, que si A tiene n elementos entonces $\mathcal{P}(A)$ tiene 2^n elementos.

10. Demuestre cada una de las siguientes propiedades de dos formas: usando inducción, y usando la identidad (4.3).

    (a) Para cada $n \in \mathbb{N}$, $11^n - 4^n$ es múltiplo de 7
    (b) Para cada $n \in \mathbb{N}$, $2^{6n} - 1$ es múltiplo de 9
    (c) Para cada $n \in \mathbb{N}$, $5^{2n} - 1$ es divisible por 8.

(d) Para cada $n \in \mathbb{N}$, el polinomio $x^{2n} - a^{2n}$ es divisible por $x + a$.

11. Utilice la identidad (4.3) para demostrar el teorema del factor: Si $p(x)$ es un polinomio, y $p(a) = 0$, entonces $p(x)$ es divisible por $x - a$.

12. Demuestre que un número natural es divisible por 9 si, y solo si, la suma de sus dígitos lo es.

13. Demuestre que para cada $n \in \mathbb{N}$ se tiene que

    (a) $3^{2n} + 7$ es divisible por 8
    (b) $n^5 - n$ es divisible por 30
    (c) $n^3 - n$ es múltiplo de 3
    (d) $7^n + 4 \cdot 7^{n-1} + 1$ es divisible por 3
    (e) $4 \cdot 10^{n+1} + 7 \cdot 10^n - 2$ es divisible por 9
    (f) $5^n - 4n - 1$ es divisible por 16 $(n \geq 1)$.
    (g) $n^3 + (n+1)^3 + (n+2)^3$ es divisible por 9.
    (h) $4^n + 15n - 1$ es divisible por 9 $(n \geq 1)$.

14. Demuestre que $n^2 + 3n + 1$ es impar para todo $n \in \mathbb{N}$.

15. Para $x > 0$, use el principio del buen orden para demostrar que existe $n \in \mathbb{N}$ tal que $n \leq x < n + 1$ (tal n se llama la parte entera de x).

16. Demuestre el principio de inducción, usando el principio del buen orden.

17. Un conjunto $A \subseteq \mathbb{Z}$ se llama acotado superiormente si existe $m \in \mathbb{Z}$ tal que $n \leq m$ para todo $n \in A$. Demuestre que todo subconjunto de $\mathbb{Z}$, acotado superiormente, tiene máximo.

18. Usando la definición, y el principio de inducción, demuestre que para $m, n \in \mathbb{N}$ y $a, b \in \mathbb{R}^*$ se tiene

$$a^m a^n = a^{m+n}, \quad (ab)^n = a^n b^n, \quad (a^n)^m = a^{mn}.$$

19. Demuestre usando el principio de inducción que para todo $n \in \mathbb{N}$ se tiene:

$$\sum_{k=0}^{n} k^2 = \frac{n}{6}(n+1)(2n+1), \qquad \sum_{k=0}^{n} k^3 = \frac{n^2}{4}(n+1)^2.$$

20. Use inducción para demostrar que todo $n \in \mathbb{N}$ tiene una de las tres formas $3k$, $3k + 1$, o $3k + 2$, con $k \in \mathbb{N}$.

21. Use inducción completa para demostrar que todo $n \in \mathbb{N}$ tiene la forma $2^p l$, donde $p \in \mathbb{N}$ y l es impar.

22. Sea E un conjunto. En $\mathcal{P}(E)$ definimos la relación: $A \sim B$ sii A y B son equipotentes. Demuestre que esta relación es de equivalencia.

23. Demuestre que si $S_n \sim S_m$, entonces $n = m$.

24. Si A y B son finitos y equipotentes, demuestre que A y B tienen la misma cantidad de elementos. Se escribe $|A| = |B|$.

25. Si A es tal que existe una función inyectiva $f : A \to S_n$ (algún $n \in \mathbb{N}$), demuestre que A es finito, y que $|A| \leq n$. Sug. Considere el primer elemento del conjunto $\{k \in \mathbb{N} : \text{existe } f : A \to S_k \text{ inyectiva}\}$.

26. Use el ejercicio anterior para demostrar que si A es finito y existe $f : B \to A$ inyectiva, entonces B es finito y $|B| \leq |A|$.

27. Si A es finito y $B \subseteq A$, entonces B es finito y $|B| \leq |A|$.

28. Si A es infinito y $n \in \mathbb{N}$, muestre que no existe una función inyectiva $f : A \to S_n$.

29. Demuestre que si existe una inyección $f : \mathbb{N} \to A$, entonces A es infinito.

30. Considere la suma $S_n = 2 + 4 + \ldots + 2n$. Encuentre una fórmula para esta suma, y demuestre su validez.

31. Demuestre que para cualquier $x > -1$, y cualquier natural $n \geq 1$, se cumple $(1 + x)^n \geq 1 + nx$. Esta desigualdad se conoce como *Desigualdad de Bernoulli.*

32. Demuestre que $n! > \sqrt{n \cdot 2^n}$ para todo natural $n \geq 3$.

33. Sean a, b dos números reales positivos, y sea n un natural. Demuestre que

$$(a + b)^n < 2^n \left(a^n + b^n\right).$$

Recuerde que $\left(a^n - b^n\right)(a - b) \geq 0$.

34. Demuestre que para todo natural positivo, se cumple

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \ldots + \frac{1}{n\,(n+1)} = 1 - \frac{1}{n+1}.$$

Concluya que

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \ldots + \frac{1}{n\,(n+1)} < 1.$$

35. Demuestre que para todo natural positivo, se cumple
$$\frac{1}{1\cdot 3}+\frac{1}{3\cdot 5}+\ldots+\frac{1}{(2n-1)(2n+1)}=\frac{n}{2n+1}.$$

36. Demuestre que para todo natural positivo, se cumple
$$1\cdot 2+2\cdot 3+\ldots+(n-1)n=\frac{n\left(n^2-1\right)}{3}.$$

37. Demuestre que para $x\neq 1$ y $n\geq 1$ se tiene
$$\prod_{i=0}^{n}\left(1+x^{2^i}\right)=\frac{x^{2^{n+1}}-1}{x-1}.$$

38. Demuestre que para $n\geq 2$, la media geométrica de n números reales positivos, es menor que la media aritmética. Es decir, si $x_1,\ldots,x_n$ son números reales positivos, entonces
$$\sqrt[n]{x_1x_2\ldots x_n}\leq\frac{x_1+\ldots+x_n}{n}.$$

39. Si $r\neq 1$, demuestre que para todo $n\in\mathbb{N}^*$ se tiene
$$\sum_{k=1}^{n}kr^{k-1}=\frac{1-(n+1)r^n+nr^{n+1}}{(1-r)^2}.$$

40. Demuestre que para $n\in\mathbb{N}^*$ se tiene
$$\sum_{k=1}^{n}k\cdot 3^k=\frac{3}{4}\left[3^n(2n-1)+1\right].$$

41. Demuestre que para $n\in\mathbb{N}$, $n>1$ se tiene
$$\sum_{k=1}^{n}\frac{1}{\sqrt{k}}>\sqrt{n}.$$

42. Para $n\in\mathbb{N}$ positivo demuestre que
$$\sum_{k=1}^{n}\frac{k+2}{k(k+1)2^k}=1-\frac{1}{2^n(n+1)}.$$

43. Sea $a_n=f(n)$, donde f es una sucesión. Demuestre usando inducción que para cada $n\in\mathbb{N}$ se tiene
$$\sum_{k=0}^{n}(a_k-a_{k+1})=a_0-a_{n+1}.$$
A las sumas de este tipo se les llama *sumas telescópicas*. Use lo anterior para calcular
$$\sum_{k=0}^{n}\left(\sqrt{k}-\sqrt{k+1}\right),\quad\sum_{k=1}^{n}\frac{1}{k(k+1)}.$$

4.3 Sistemas de numeración

De idéntica manera al español, en donde todas las palabras se escriben con un número finito de símbolos (las veinte y tantas letras del alfabeto), en matemática es posible escribir todos los números con un número finito de símbolos.

El rápido progreso experimentado en los últimos años en el uso de las computadoras y máquinas similares, ha hecho que las bien conocidas reglas de la aritmética del sistema decimal devengan insuficientes. Particularmente, este auge ha llevado inevitablemente a la adopción, entre otros, del sistema binario de numeración.

Históricamente, el hombre siempre tuvo la necesidad de buscar símbolos que le sirvieran para representar números. Desde luego que en un principio se utilizaron símbolos muy sencillos: dibujos, marcas u otros. Es justo decir, que inclusive algunos de estos métodos de representación se han conservado hasta hace relativamente poco tiempo.

Diferentes culturas han utilizado diversos conjuntos de símbolos para representar los números. Por ejemplo, los babilonios utilizaron el sistema cuneiforme, los egipcios recurrieron a los jeroglíficos, los griegos hicieron uso del alfabeto y por último el muy conocido sistema romano de numeración. Un estudio detallado de estos sistemas, revela que los aspectos más importantes a señalar son: la base utilizada, la falta de un símbolo para denotar el cero y la falta total o uso muy limitado de la idea de valor de posición.

Por ejemplo, el sistema romano de numeración usaba símbolos como: I, V, X, L, C, D, M, mientras que en el sistema hindu-arábico, que es el utilizado actualmente, los símbolos anteriores correponden a: 1, 5, 10, 50, 100, 500, 1000.

El sistema utilizado por nosotros, conocido como hindú-arábico debido a su origen, utiliza diez símbolos para representar los números: $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$. La utilización de diez símbolos, le ha ganado el nombre de sistema decimal. En este sistema, cuando escribimos un número, los símbolos o dígitos se colocan en diferentes posiciones y se le asigna un valor a cada posición: la de la extrema derecha, representa las unidades; la segunda representa las decenas; la tercera representa los centenas; la cuarta las unidades de millar; la quinta las decenas de millar; y así sucesivamente.

Antes de entrar propiamente en el problema de la representación de los números en una base cualquiera, y efectuar operaciones aritméticas con dichas representaciones, vamos a presentar algunos resultados preliminares sobre el algoritmo de la división euclideana. Este constituye el fundamento teórico para realizar las representaciones antes mencionadas, y en particular la tan familiar representación de un número en la base diez.

El lector posiblemente esté tan familiarizado con el sistema de numeración en base diez, que nunca ha sentido la necesidad de preguntarse si será posible trabajar con otras bases. En esta sección demostraremos que lo mismo que se hace en el sistema decimal se puede hacer con cualquier base $b > 1$.

4.3.1 Un poco sobre la división euclideana

Recordemos que por el lema 4.2.4, dados a y b números naturales, existen números naturales q y r tales que

$$a = bq + r, \quad 0 \leq r < b.$$

Este proceso de hallar q y r, se llama la división euclideana o algoritmo de la división. Los números q y r reciben el nombre de cociente y residuo respectivamente, y son únicos, de acuerdo con el teorema 4.3. ¿Se acuerda de la escuela primaria?

Ejemplo 4.3.1 *Si* $a = 145$ *y* $b = 15$, *tenemos* $a = b \cdot 9 + 10$, *así que* $q = 9$ *y* $r = 10$.

Ejemplo 4.3.2 *Si* $a = 177$ *y* $b = 14$, *se tiene* $a = b \cdot 12 + 9$, $0 \leq 9 < 14$.

Ejemplo 4.3.3 $154 = 14 \cdot 11 + 0$, $0 \leq 0 < 14$.

La unicidad de q y r la enunciamos y demostramos a continuación.

Teorema 4.3 *Sean* $a, b \in \mathbb{N}$, *con* $b > 0$. *Los números* q, $r \in \mathbb{N}$ *tales que*

$$a = bq + r, \quad 0 \leq r < b,$$

son únicos.

Demostración
Suponga que tenemos dos pares (q, r) y (q', r') tales que

$$a = bq + r = bq' + r', \text{ y } 0 \leq r < b, 0 \leq r' < b.$$

Sin perder generalidad podemos suponer que $r' \leq r$. Entonces $bq + r - r' = bq'$, lo que demuestra que $bq \leq bq'$, y luego $q \leq q'$. Ahora, si $q < q'$, se tendría $q' - q \geq 1$, de donde $b\,(q' - q) \geq b$, esto es

$$b \leq b\left(q' - q\right) = r - r' \leq r < b.$$

Esta contradicción demuestra que $q' = q$, y luego $r' = r$. □

4.3.2 Bases de numeración

¿Cómo escribir un número dado en un sistema de númeración de base b?
Para fijar ideas, pensemos por un momento en el caso del sistema de numeración de base diez o sistema decimal. Por ejemplo:

$$\begin{aligned} 4705 &= 4 \cdot 10^3 + 7 \cdot 10^2 + 0 \cdot 10 + 5, \\ 4806 &= 4 \cdot 10^3 + 8 \cdot 10^2 + 0 \cdot 10 + 6, \\ 36 &= 3 \cdot 10 + 6. \end{aligned}$$

Es decir, los números están representados por medio de potencias de 10. Es importante hacer notar, que en el sistema decimal se utilizan los símbolos: $0, 1, 2, \ldots, 9$ para representar cualquier número.
De manera análoga, cualquier otro número mayor que la unidad puede tomarse como base de un sistema de numeración; así si 7 es la base, un número expresado por 2453 representa el número $2 \cdot 7^3 + 4 \cdot 7^2 + 5 \cdot 7 + 3$. En este sistema no existe ningún dígito mayor que 6.

De manera general, en un sistema de numeración de base b, para representar los números se utilizan b símbolos. Aquí, b es cualquier natural mayor que 1.
Debe entenderse que, los símbolos o dígitos escogidos representan los primeros b números naturales, ordenados en sentido creciente.

$$0 < 1 < 2 < 3 < \ldots < b - 1.$$

Consideremos ahora un número natural cualquiera N.

1. Si $N < b$, existe un símbolo para representarlo. Por ejenplo supongamos que la base es $b = 8$, y $N = 5$. En este caso, el conjunto de símbolos que utilizamos es $\{0, 1, 2, \ldots, 7\}$, y claramente $N = 5$ es uno de ellos.

2. Si $N \geq b$, podemos utilizar la división euclideana de N por b, con lo cual obtenemos

   $$N = q_1 \cdot b + r_0; \quad 0 \leq r_0 < b, \quad q_1 \neq 0.$$

   Observe que como $r_0 < b$, entonces se puede representar con alguno de los símbolos del sistema.

   Si $q_1 < b$, también se podrá representar por uno de los símbolos del sistema. En este caso:

   $$N = q_1 b + r_0,$$

   y se usa la notación $N = (q_1 r_0)_b$ como represetación del número N en el sistema de base b.

Ejemplo 4.3.4 *En el sistema decimal,* $N = 27$ *significa:* $N = 2 \cdot 10 + 7$.

Ejemplo 4.3.5 *En el sistema de numeración de base* 3, $N = (21)_3$ *significa:* $N = 2 \cdot 3 + 1$.

La pregunta natural es: ¿Qué pasa si $q_1 \geq b$? En este caso, aplicaremos el algoritmo de la división a q_1 y b. En caso de ser necesario, se procede similarmente hasta obtener un cociente q_n que sea estrictamente menor que b.
En el caso en que se requiera efectuar la división euclideana de manera reiterada, se obtiene un esquema como el siguiente:

$$\begin{array}{r|lllll} & N & = q_1 b + r_0 & 0 \leq r_0 < b, & q_1 \neq 0, & q_1 \geq b \\ b & q_1 & = q_2 b + r_1 & 0 \leq r_1 < b, & q_2 \neq 0, & q_2 \geq b \\ b^2 & q_2 & = q_3 b + r_2 & 0 \leq r_2 < b, & q_3 \neq 0, & q_3 \geq b \\ \vdots & \vdots & \vdots & \vdots & \vdots & \\ b^{n-2} & q_{n-2} & = q_{n-1} b + r_{n-2} & 0 \leq r_{n-2} < b, & q_{n-1} \neq 0, & q_{n-1} \geq b \\ b^{n-1} & q_{n-1} & = q_n b + r_{n-1} & 0 \leq r_{n-1} < b, & q_n \neq 0\ , & q_n < b. \end{array}$$

Observe que multiplicando cada una de las igualdades por el entero indicado a la izquierda de la línea, se obtiene:

$$\begin{aligned} q_1 b &= q_2 b^2 + r_1 b \\ q_2 b^2 &= q_3 b^3 + r_2 b^2 \\ q_3 b^3 &= q_4 b^4 + r_3 b^3 \\ &\vdots \\ q_{n-2} b^{n-2} &= q_{n-1} b^{n-1} + r_{n-2} b^{n-2} \\ q_{n-1} b^{n-1} &= q_n b^n + r_{n-1} b^{n-1}, \end{aligned}$$

y sumándolas, resulta:

$$q_1 b + q_2 b^2 + \ldots + q_{n-1} b^{n-1} = (q_2 b^2 + \ldots + q_{n-1} b^{n-1} + q_n b^n) + (r_1 b + r_2 b^2 + \ldots + r_{n-2} b^{n-2} + r_{n-1} b^{n-1}).$$

Nótese que la expresión $q_2 b^2 + \ldots + q_{n-1} b^{n-1}$ aparece a ambos lados de la igualdad, y entonces cancelando se obtiene:

$$q_1 b = q_n b^n + r_1 b + r_2 b^2 + \ldots + r_{n-1} b^{n-1}.$$

Ahora, recordemos que $N = q_1 b + r_0$, es decir

$$N - r_0 = q_1 b = q_n b^n + r_{n-1} b^{n-1} + \ldots + r_1 b.$$

Despejando N obtenemos

$$N = q_n b^n + r_{n-1} b^{n-1} + \ldots + r_1 b + r_0.$$

Por convención escribimos

$$N = (q_n r_{n-1} r_{n-2} \ldots r_1 r_0)_b\,.$$

Observe que los números $q_n, r_{n-1}, r_{n-2}, \ldots, r_0$ son menores que b, y por lo tanto son representables por uno de los símbolos del sistema.

Ejemplo 4.3.6 *En el sistema de numeración de base* 4*, que tiene como símbolos* $0, 1, 2, 3$*, el símbolo* $(2011)_4$ *representa el número*

$$N = 2 \cdot 4^3 + 0 \cdot 4^2 + 1 \cdot 4 + 1 = 133.$$

En otras palabras, $N = (2011)_4 = (133)_{10}\,.$

Ejemplo 4.3.7 *En el sistema de numeración de base de* 7*, el número expresado por* $(2453)_7$ *es*

$$N = 2 \cdot 7^3 + 4 \cdot 7^2 + 5 \cdot 7 + 3,$$

o sea que $(2453)_7 = (920)_{10}$*. En este sistema no existe ningún dígito mayor que* 6*.*

Ejemplo 4.3.8 *Cuando* $b = 10$ *obtenemos la representación decimal usual, a la cual todos estamos acostumbrados. Los dígitos son* $0, 1, 2, \ldots, 9$*. Por ejemplo,* $345 = 3 \cdot 10^2 + 4 \cdot 10 + 5 = (345)_{10}$*. Desde luego, seguiremos con la costumbre de omitir el símbolo* $(\cdot)_{10}$ *en este caso.*

Ejemplo 4.3.9 *Dado el número* $N = 53$ *(en base diez), para representarlo en base* 4 *aplicamos el algoritmo de la división repetidamente, obteniendo*

$$\begin{array}{ll} 53 = 13 \cdot 4 + 1, & q_1 = 13, \quad r_0 = 1 \\ 13 = 3 \cdot 4 + 1, & q_2 = 3, \quad r_1 = 1. \end{array}$$

Como $q_2 = 3 < 4$*, paramos en este punto. Luego* $53 = (311)_4$*.*

Ejemplo 4.3.10 *Para expresar* $N = 100$ *en base 2, podemos dividir sucesivamente por 2. Sin embargo, es más rápido usar las potencias de 2 directamente: La mayor potencia de* 2 *que no excede a* $n = 100$ *es* $2^6 = 64$*, y dividiendo obtenemos:*

$$100 = 1 \cdot 64 + 36 = 1 \cdot 2^6 + 36.$$

Haciendo lo mismo con 36 *en vez de* 100 *obtenemos*

$$36 = 1 \cdot 32 + 4 = 1 \cdot 2^5 + 2^2,$$

de donde $100 = 1 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^2 = (1100100)_2$*.*

Comentarios

- Como los valores $r_0, q_1, r_1, q_2 \ldots$ se van obteniendo de manera única, al hacer las divisiones sucesivas, la representación que se obtiene para el número N, en un sistema de numeración de base b, es única.
- En un sistema de numeración de base b, se tiene que $b = 1 \cdot b + 0 = (10)_b$. Así, no importa cuál sea la base b, se obtiene que

$$N = q_n r_{n-1} \ldots r_0 = q_n \cdot (10)_b^n + r_{n-1} \cdot (10)_b^{n-1} + \cdots + r_0.$$

Ejemplo 4.3.11 *Representar* 475 *en base* 8

$$\begin{array}{rcl} N & = & 475 = 59 \cdot 8 + 3 = q_1 \cdot 8 + r_0 \\ q_1 & = & 59 = 7 \cdot 8 + 3 = q_2 \cdot 8 + r_1. \end{array}$$

Se observa que en la segunda división euclideana se obtiene $q_2 = 7 < 8$*. Luego:* $475 = (733)_8$*.*

Ejemplo 4.3.12 *Escribir* 325 *en base* 8. *Efectuando la división de* 325 *por* 8 *obtenemos:*

$$325 = 40 \cdot 8 + 5,$$

luego dividimos 40 *por* 8 *obteniendo* $40 = 5 \cdot 8 + 0$. *Entonces*

$$325 = 40 \cdot 8 + 5 = 5 \cdot 8^2 + 5,$$

lo que significa que $325 = [505]_8$.

Ejemplo 4.3.13 *Representar* 475 *en base* 2

$$\begin{array}{ll} 475 = 237 \cdot 2 + 1 & 29 = 14 \cdot 2 + 1 \\ 237 = 118 \cdot 2 + 1 & 14 = 7 \cdot 2 + 0 \\ 118 = 59 \cdot 2 + 0 & 7 = 3 \cdot 2 + 1 \\ 59 = 29 \cdot 2 + 1 & 3 = 1 \cdot 2 + 1. \end{array}$$

Luego $475 = (111\ 011\ 011)_2$.

Ejemplo 4.3.14 *Escribir* 1000 *en base* 2. *Veamos:*

$$\begin{array}{lcll} 1000 & = & 500 \cdot 2 + 0, & 31 = 15 \cdot 2 + 1, \\ 500 & = & 250 \cdot 2 + 0, & 15 = 7 \cdot 2 + 1, \\ 250 & = & 125 \cdot 2 + 0, & 7 = 3 \cdot 2 + 1 \\ 125 & = & 62 \cdot 2 + 1, & 3 = 1 \cdot 2 + 1. \\ 62 & = & 31 \cdot 2 + 0, & \end{array}$$

Luego $1000 = (1111101000)_2$. *También aquí puede procederse como en el ejemplo de* $N = 100$, *si recordamos bien las potencias de* 2 :

$$\begin{array}{rcl} 1000 & = & 512 + 488 \\ & = & 2^9 + 256 + 232 \\ & = & 2^9 + 2^8 + 128 + 104 \\ & = & 2^9 + 2^8 + 2^7 + 64 + 40 \\ & = & 2^9 + 2^8 + 2^7 + 2^6 + 32 + 8 \\ & = & 2^9 + 2^8 + 2^7 + 2^6 + 2^5 + 2^3. \end{array}$$

Para una base cualquiera b, hay algunos enteros cuya representación resulta muy sencilla.Veamos:

- $b = (10)_b$
- $b^2 = (100)_b$
- $b^4 = (10\ 000)_b$.

En general, b^n se representa, en base b, como un 1 seguido de n ceros. En particular

$$5^7 = (10000000)_5, \quad (16)^3 = (1000)_{16} = 4096 = 2^{12} = (1000000000000)_2.$$

Nota: Sean N y n dos enteros positivos, note que

$$\begin{aligned}\sum_{k=0}^{n-1}(N-1)N^k &= \sum_{k=0}^{n-1}N^{k+1} - \sum_{k=0}^{n-1}N^k \\ &= (N + N^2 + N^3 + \ldots + N^{n-1} + N^n) - (1 + N + N^2 + \ldots + N^{n-1}) \\ &= N^n - 1.\end{aligned}$$

Es decir

$$N^n - 1 = \sum_{k=0}^{n-1}(N-1)N^k.$$

Por lo tanto, la representación del entero $N^n - 1$, en base N es

$$N^n - 1 = (\theta\theta\ldots\theta)_N \tag{4.4}$$

donde θ (que representa a $N-1$) aparece n veces. Veamos algunos ejemplos de este resultado.

Ejemplo 4.3.15 *Tome $b = 5$ y $n = 7$. Entonces $5^7 - 1 = (4\ 444\ 444)_5$ (aquí θ es el símbolo 4).*

Ejemplo 4.3.16 *Tome $b = 8$ y $n = 6$, entonces: $8^6 - 1 = (777\ 777)_8$ (aquí θ es 7).*

¿Qué pasa cuando $b \geq 10$?

Consideremos el caso $b = 16$ (sistema de numeración en base 16), en este caso escogemos los símbolos:

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.$$

Es decir, usamos las letras A, B, C, D, E y F para representar los enteros $10, 11, 12, 13, 14$ y 15, respectivamente.

Ejemplo 4.3.17 $32 = (20)_{16}$, $79 = (4F)_{16}$, $(2EC1)_{16} = 2\cdot16^3+14\cdot16^2+12\cdot16+1 = 11\,969$.

Ejemplo 4.3.18 *Escribir* 506 *en base* 16. *Dividiendo sucesivamente obtenemos:*

$$\begin{aligned}506 &= 31 \cdot 16 + 10, \\ 31 &= 1 \cdot 16 + 15,\end{aligned}$$

de donde

$$506 = (1FA)_{16}\,.$$

Ejemplo 4.3.19 *Nótese que* $718 = 2 \cdot 16^2 + 12 \cdot 16 + 14$, *por lo tanto*

$$718 = (2CE)_{16}.$$

Ejemplo 4.3.20 *Tomando* $N = 16$ *y* $n = 9$, *en la fórmula (4.4) se tiene que*

$$(16)^9 - 1 = (FFFFFFFFF)_{16},$$

aquí θ *es el símbolo F.*

4.3.3 ¡De vuelta a la niñez!

Seguidamente, vamos a recordar la escuela primaria haciendo un poco de aritmética. Las operaciones aritméticas de suma, resta, multiplicación y división tienen las mismas reglas en cualquier base. La idea es partir del conocimiento que se tiene de estas operaciones en la base 10 y utilizarlas para operar en cualquier otro sistema de numeración. Es muy importante, eso sí, tener cuidado de utilizar correctamente las tablas de adición y multiplicación en la base correspondiente.

Comencemos con algunos ejemplos en base 2 (sistema binario). Las tablas de la suma y de la multiplicación en base 2 son las siguientes:

+	0	1
0	0	1
1	1	10

·	0	1
0	0	0
1	0	1

.

Ejemplo 4.3.21 *Efectuar la siguiente suma:* $(10011111)_2 + (11011101)_2$. *Veamos:*

$$\begin{array}{cccccccccc} & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ + & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ \hline 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \end{array}$$

Explicación: *Primero sumamos las unidades* $1 + 1 = 10$, *colocamos el* 0 *y llevamos el* 1 *a la segunda columna. En la segunda columna obtenemos que* $1 + 1 + 0 = 10$, *colocamos el cero y llevamos el* 1 *a la tercera columna, donde queda* $1 + 1 + 1 = 11$, *colocamos* 1 *y llevamos* 1 *a la cuarta columna. Se continúa de es manera hasta llegar a la última columna.*

Ejemplo 4.3.22 *Efectuar la resta siguiente* $(110001110)_2 - (11011101)_2$:

$$\begin{array}{cccccccccc} 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ - & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ \hline & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}$$

Explicación: *Como en la primera columna aparece* $0-1$, *tomamos "prestada" una "decena" de la segunda columna para obtener* $10 - 1 = 1$. *En la segunda columna queda entonces* $0 - 0 = 0$. *En la quinta columna se hace el mismo trato con la sexta, que a su vez debe pedir prestado a la sétima, y esta a la octava.*

Ejemplo 4.3.23 *Representar $N = 1000$ en base dos. Este ejemplo lo presentamos antes en forma directa. Podemos sin embargo hacerlo restando, dado que*

$$\begin{aligned} 1000 &= 1024 - 24 = 2^{10} - \left(2^4 + 2^3\right) \\ &= (10\,000\,000\,000)_2 - (11\,000)_2 = (1111101000)_2 \,. \end{aligned}$$

El lector puede realizar la resta indicada.

En base ocho, las tablas de la suma y la multiplicación son las siguientes. Invitamos al lector a comprobarlo:

+	1	2	3	4	5	6	7
1	2	3	4	5	6	7	10
2	3	4	5	6	7	10	11
3	4	5	6	7	10	11	12
4	5	6	7	10	11	12	13
5	6	7	10	11	12	13	14
6	7	10	11	12	13	14	15
7	10	11	12	13	14	15	16

·	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	10	12	14	16
3	3	6	11	14	17	22	25
4	4	10	14	20	24	30	34
5	5	12	17	24	31	36	43
6	6	14	22	30	36	44	52
7	7	16	25	34	43	52	61

Ejemplo 4.3.24 *Calcular* $(6733)_8 + (14\ 525)_8$:

$$\begin{array}{cccccc} + & 6 & 7 & 3 & 3 \\ 1 & 4 & 5 & 2 & 5 \\ \hline 2 & 3 & 4 & 6 & 0 \end{array}$$

Ejemplo 4.3.25 *Calcular* $(51026)_8 - (32137)_8$:

$$\begin{array}{ccccc} 5 & 1 & 0 & 2 & 6 \\ 3 & 2 & 1 & 3 & 7 \\ \hline 1 & 6 & 6 & 6 & 7 \end{array}$$

Ejemplo 4.3.26 *Calcular el producto* $(733)_8 \cdot (125)_8$:

$$\begin{array}{cccccc} & & & 7 & 3 & 3 \\ & & \times & 1 & 2 & 5 \\ \hline & & 4 & 5 & 0 & 7 \\ & 1 & 6 & 6 & 6 & \\ & 7 & 3 & 3 & & \\ \hline 1 & 1 & 6 & 6 & 6 & 7 \end{array}$$

Para el siguiente ejemplo, utilizamos las tablas de la suma y la muliplicación en base 16. Para el caso de la suma, bastará con la siguiente. Invitamos al lector a completarla.

+	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
5	6	7	8	9	A	B	C	D	E	F	10	11	12	13	14
6	7	8	9	A		C	D	E	F	10	11	12	13	14	15
7	8	9	A	B			E	F	10	11	12	13	14	15	16
8	9	A	B	C				10	11	12	13	14	15	16	17
9	A	B	C	D					12	13	14	15	16	17	18
A	B	C	D	E						14	15	16	17	18	19
B	C	D	E	F							16	17	18	19	1A
C	D	E	F	10								18	19	1A	1B
D	E	F	10	11									1A	1B	1C
E	F	10	11	12										1C	1D
F	10	11	12	13											1E

En el caso del producto, incluiremos un poco más de filas:

·	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	4													
3	6	9												
4	8	C	10											
5	A	F	14	19										
6	C	12	18	1E	24									
7	E	15	1C	23	2A	31								
8	10	18	20	28	30	38	40							
9	12	1B	24	2D	36	3F	48	51						
A	14	1E	28	32	3C	46	50	5A	64					
B	16	21	2C	37	42	4D	58	63	6E	79				
C	18	24	30	3C	48	54	60	6C	78	84	90			
D	1A	27	34	41	4E	5B	68	75	82	8F	9C	A9		
E	1C	2A	38	46	54	62	70	7E	8C	9A	A8	B6	C4	
F	1E	2D	3C	4B	5A	69	78	87	96	A5	B4	C3	D2	E1

Ejemplo 4.3.27 *Efectuar el producto indicado:* $(7A3)_{16} \cdot (82C)_{16}$

$$
\begin{array}{cccccc}
 & & & 7 & A & 3 \\
 & & \times & 8 & 2 & C \\
\hline
 & & 5 & B & A & 4 \\
 & & F & 4 & 6 & \\
3 & D & 1 & 8 & & \\
\hline
3 & E & 6 & 8 & 0 & 4
\end{array}
$$

$(7A3)_{16} \cdot (82C)_{16} = (3E6804)_{16}$

4.3.4 Algunos comentarios adicionales

Recordemos que para cualquier base $b > 1$, se tiene que $b = (10)_{b.}$ Por lo tanto si $N = (q_n r_{r-1} \dots r)_b$, entonces N también se puede escribir como

$$N = \left(q_n 10^n + r_{n-1}10^{n-1} + \dots + r_1 10 + r_0\right)_b .$$

Por otro lado, si $p < n$ se tiene

$$\begin{aligned} N &= (q_n b^n + r_{n-1}b^{n-1} + \dots + r_p b^p) + (r_{p-1}b^{p-1} + \dots + r_2 b^2 + r_1 b + r_0) \\ &= (q_n b^{n-p} + r_{n-1}b^{n-p-1} + \dots + r_p)b^p + R, \end{aligned}$$

donde

$$R = (r_{p-1} \dots r_1 r_0)_b.$$

Observe que $0 \leq R < b^p$, y por lo tanto R es el residuo de la división euclideana de N por b^p, y el cociente será

$$Q = q_n b^{n-p} + r_{n-1}b^{n-p-1} + \dots + r_p = (q_n r_{n-1} \dots r_p)_b$$

Lo anterior, se puede resumir en el siguiente resultado:

Teorema 4.4 *El resto de la división euclideana de N por b^p, en la base b, es el número formado por las p cifras de la derecha de la representación de N en base b. El cociente es el número formado por las $n - p$ cifras de la izquierda.*

Ejemplo 4.3.28 *Sea $N = (200\ 121\ 222)_3$. Entonces, al hacer la división euclideana de N por 3^4, se obtiene que:*

$$\begin{aligned} Q = (20012)_3 : &\quad \text{cociente} \\ R = (1222)_3 : &\quad \text{residuo.} \end{aligned}$$

Anteriormente, se discutió qué pasaba cuando la base b era mayor o igual a 10. Por ejemplo, si queremos expresar cantidades en la base 12 debemos elegir doce símbolos.

Ejemplo 4.3.29 *Sea $N = (498A7B4)_{12}$, donde A representa al 10 y B al 11. Al dividir N por 12^5 obtenemos cociente $(49)_{12}$ y resto $(8A7B4)_{12}$.*

4.3.5 Algoritmos de cálculo

En esta sección explicaremos el por qué de las técnicas que se usan en la escuela primaria para realizar las operaciones básicas. Tener estas técnicas bien claras, es algo fundamental para un docente de secundaria, pues de lo contrario no tendrá más que enseñar "recetas" a sus estudiantes.

Consideramos una base $b > 1$ fija, y omitiremos el símbolo $(\cdot)_b$ para simplificar notación.

La suma

Comencemos con un ejemplo en base 10. Queremos hacer la suma $6274+928$, así que primero agrupamos de acuerdo con las potencias de 10 que aparecen:

$$\begin{aligned} 6274 + 928 &= 6 \cdot 10^3 + (2+9) \cdot 10^2 + (7+2) \cdot 10 + (4+8) \\ &= 6 \cdot 10^3 + (2+9) \cdot 10^2 + (7+2) \cdot 10 + 12. \end{aligned}$$

El agrupar en potencias iguales de 10 corresponde a ubicar los números, uno debajo del otro, de modo que las unidades, decenas, etc, queden alineadas en columnas:

$$\begin{array}{cccc} 6 & 2 & 7 & 4 \\ + & 9 & 2 & 8 \\ \hline \end{array}$$

Como 12 no es uno de los dígitos, escribimos $12 = 10 + 2$, y entonces

$$6274 + 928 = 6 \cdot 10^3 + (2+9) \cdot 10^2 + (7+2+1) \cdot 10 + 2.$$

Esto corresponde a colocar el 2 en la casilla de las unidades, y "llevar" el 1 a la de las decenas:

$$\begin{array}{cccc} & & \overset{1}{} & \\ 6 & 2 & 7 & 4 \\ + & 9 & 2 & 8 \\ \hline & & & 2 \end{array}$$

Luego

$$\begin{aligned} 6274 + 928 &= 6 \cdot 10^3 + (2+9) \cdot 10^2 + 10 \cdot 10 + 2 \\ &= 6 \cdot 10^3 + (2+9+1) \cdot 10^2 + 0 \cdot 10 + 2, \end{aligned}$$

lo cual es equivalente a colocar el 0 en la casilla de las decenas, y llevar el 1 a la de las centenas:

$$\begin{array}{cccc} & \overset{1}{} & \overset{1}{} & \\ 6 & 2 & 7 & 4 \\ + & 9 & 2 & 8 \\ \hline & & 0 & 2 \end{array}$$

Finalmente

$$\begin{aligned} 6274 + 928 &= 6 \cdot 10^3 + 12 \cdot 10^2 + 0 \cdot 10 + 2 \\ &= (6+1) \cdot 10^3 + 2 \cdot 10^2 + 0 \cdot 10 + 2 \\ &= 7202, \end{aligned}$$

lo cual se ve así:

$$\begin{array}{cccc} {\scriptstyle 1} & {\scriptstyle 1} & {\scriptstyle 1} & \\ 6 & 2 & 7 & 4 \\ + & 9 & 2 & 8 \\ \hline 7 & 2 & 0 & 2 \end{array}$$

En general, consideremos dos números M y N que en base b se representan por:

$$M = p_m \dots p_0, \quad N = q_n \dots q_0.$$

Tenemos entonces $M = p_m \cdot b^m + \ldots + p_0$, y $N = q_m \cdot 10^m + \ldots + q_0$. Al sumar $M + N$ se hace uso de las propiedades de la suma (conmutatividad, asociatividad, etc.). Tenemos

$$M + N = (p_m b^m + \ldots + p_1 b) + (q_m b^m + \ldots + q_1 b) + p_0 + q_0.$$

Si $p_0 + q_0 < b$, tenemos que $r_0 = p_0 + q_0$ es el dígito de las unidades de $M + N$. En caso contrario tenemos $p_0 + q_0 = b + c$, donde $0 \leq c < b$, y tomamos $r_0 = c$. Obtenemos

$$M + N = \left(p_m b^m + \ldots + p_2 b^2\right) + \left(q_m b^m + \ldots + q_2 b^2\right) + (1 + p_1 + q_1)\, b + r_0.$$

Nótese que $p_0 + q_0$ se representa en base b como $(1r_0)_b$, y lo que hicimos equivale a colocar r_0 en la primera columna a la derecha, y llevar el 1 a la segunda:

$$\begin{array}{cccccc} & & & & {\scriptstyle 1} & \\ & \dots & p_2 & p_1 & p_0 \\ + & \dots & q_2 & q_1 & q_0 \\ \hline & & & & r_0 \end{array}$$

Luego hacemos el mismo análisis con $1 + p_1 + q_1$, y así continuamos hasta llegar a la última columna. El algoritmo se puede generalizar a más sumandos, con la direrencia que el dígito a "llevar" puede ser mayor que 1.

Ejemplo 4.3.30 *En base* 8, *sumar* $3245 + 467 + 674 + 56$. *Primero ubiquemos los números*

$$\begin{array}{cccc} 3 & 2 & 4 & 5 \\ & 4 & 6 & 7 \\ & 6 & 7 & 4 \\ + & & 5 & 6 \\ \hline \end{array}$$

Usando la tabla de la suma en base 8 *tenemos que* $5+7+4+6 = 26$. *Ponemos el* 6 *y llevamos el* 2 *a la siguiente columna. Luego hacemos* $2+4+6+7+5 = 30$, *ponemos el* 0 *en la segunda columna, y llevamos el* 3 *a la tercera. Es esta columna queda* $3+2+4+6 = 17$, *y en la cuarta nos que* $1+3 = 4$.

$$\begin{array}{cccc} {\scriptstyle 1} & {\scriptstyle 3} & {\scriptstyle 2} & \\ 3 & 2 & 4 & 5 \\ & 4 & 6 & 7 \\ & 6 & 7 & 4 \\ + & & 5 & 6 \\ \hline 4 & 7 & 0 & 6 \end{array}$$

La resta

Repasemos lo que uno hace en base 10. Cuando se quiere restar dos números naturales, lo ideal sería que todos los dígitos del primero sean mayores que los correspondientes del segundo. Por ejemplo, al efectuar la resta $6894-5472$, simplemente se resta dígito a dígito, obteniendo 1422. Dado que en general la situación no es tan fácil, hay que "pedir prestado". Pero, ¿qué significa esto? Por ejemplo, en la resta $385-29$ escribimos

$$385 - 29 = 3\cdot 10^2 + 8\cdot 10 + 5 - (2\cdot 10 + 9)\,.$$

Como no podemos hacer $5-9$, entonces escribimos

$$\begin{aligned} 385 - 29 &= 3\cdot 10^2 + 7\cdot 10 + 15 - (2\cdot 10 + 9) \\ &= 3\cdot 10^2 + 7\cdot 10 - 2\cdot 10 + 6. \end{aligned}$$

Esto es lo que uno expresa diciendo que "el 5 le pide prestado al 8". El resto de la operación es simple en este caso. La situación puede complicarse un poquito, como por ejemplo en $4253-367$, veamos:

$$\begin{aligned} 4253 - 367 &= 4\cdot 10^3 + 2\cdot 10^2 + 5\cdot 10 + 3 - \left(3\cdot 10^2 + 6\cdot 10 + 7\right) \\ &= 4\cdot 10^3 + (2-3)\cdot 10^2 + (5-6)\cdot 10 + (3-7) \\ &= 3\cdot 10^3 + (12-3)\cdot 10^2 + (5-6)\cdot 10 + (3-7) \\ &= 3\cdot 10^3 + (11-3)\cdot 10^2 + (15-6)\cdot 10 + (3-7) \\ &= 3\cdot 10^3 + (11-3)\cdot 10^2 + (14-6)\cdot 10 + (13-7) \\ &= 3886. \end{aligned}$$

Nótese que el 3 debe pedir prestado al 5, el cual primero debe recurrir al 2 por ayuda, y este último al 4.

$$\begin{array}{cccc} 4 & 2 & 5 & 3 \\ - & 3 & 6 & 7 \\ \hline \end{array} \rightarrow \begin{array}{cccc} 3 & {}_1 2 & 5 & 3 \\ - & 3 & 6 & 7 \\ \hline \end{array} \rightarrow \begin{array}{cccc} 3 & {}_1 1 & {}_1 5 & 3 \\ - & 3 & 6 & 7 \\ \hline \end{array} \rightarrow \begin{array}{cccc} 3 & {}_1 1 & {}_1 4 & {}_1 3 \\ - & 3 & 6 & 7 \\ \hline 3 & 8 & 8 & 6 \end{array}$$

Este es el mismo argumento que se utiliza en general, y no vale la pena ensuciar la presentación con una demostración rigurosa. Mejor veamos un ejemplo:

Ejemplo 4.3.31 *Realizar la resta* $3512 - 3477$, *en base* 8 :

$$\begin{array}{rrrrr} & 3 & 5 & 1 & 2 \\ - & 3 & 4 & 7 & 7 \\ \hline \end{array} \rightarrow \begin{array}{rrrrr} & 3 & 4 & {}_{1}1 & 2 \\ - & 3 & 4 & 7 & 7 \\ \hline \end{array} \rightarrow \begin{array}{rrrrr} & 3 & 4 & {}_{1}0 & {}_{1}2 \\ - & 3 & 4 & 7 & 7 \\ \hline \end{array} \rightarrow \begin{array}{rrrrr} & 3 & 4 & {}_{1}0 & {}_{1}2 \\ - & 3 & 4 & 7 & 7 \\ \hline & 0 & 0 & 1 & 3 \end{array}$$

La multiplicación

Dejamos al lector la tarea de hacer un análisis similar para el algoritmo de la multiplicación, tomando casos simples como el ejemplo 4.3.26.

La división

Empecemos con un ejemplo simple: Tratemos de dividir 659 entre 26. Tenemos

$$\begin{aligned} 659 &= 65 \cdot 10 + 9 = (26 \cdot 2 + 13) \cdot 10 + 9 \\ &= 26 \cdot 20 + 139 = 26 \cdot 20 + (26 \cdot 5 + 9) \\ &= 26 \cdot 25 + 9. \end{aligned}$$

¿Qué hicimos? Primero tomamos los dos primeros dígitos: 65, y dividimos por 26, obteniendo cociente 2 y resto 13. Luego "bajamos el 9" obteniendo 139, y dividimos este número por 26, obteniendo cociente 5 y resto 9. El 5 se coloca junto al 2 para obtener el cociente general 25.

$$\begin{array}{rrrr|l} & 6 & 5 & 9 & 26 \\ \cline{5-5} - & 5 & 2 & & 25 \\ & 1 & 3 & 9 & \\ - & 1 & 3 & 0 & \\ & & & 9 & \end{array}$$

En la práctica se pueden presentar situaciones especiales. Por ejemplo, en $2546 \div 34$ se deben tomar los tres primeros dígitos en vez de dos, dado que 25 es menor que 34, pero el principio es el mismo:

$$\begin{aligned} 2546 &= 254 \cdot 10 + 6 = (34 \cdot 7 + 16) \cdot 10 + 6 \\ &= 34 \cdot 70 + 166 = 34 \cdot 70 + 34 \cdot 4 + 30 \\ &= 34 \cdot 74 + 30. \end{aligned}$$

En la forma como se hace en primaria, esto se ve así:

$$\begin{array}{rcccc|l} & 2 & 5 & 4 & 6 & 34 \\ \cline{6-6} - & 2 & 3 & 8 & & 74 \\ & & 1 & 6 & 6 & \\ & - & 1 & 3 & 6 & \\ & & & 3 & 0 & \end{array}$$

Veamos qué pasa en otras bases:

Ejemplo 4.3.32 *Dividir* 11101010101 *entre* 10110111 *en base* 2 :

$$\begin{array}{rcccccccccc|l} & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & \textit{10110111} \\ \cline{12-12} - & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & & & & 1010 \\ & & & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & & \\ & & & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & & \\ & & & & & & 1 & 0 & 1 & 1 & 1 & 1 & \end{array}$$

Dado que 101111 *es menor que el divisor, obtenemos cociente* 1010 *y resto* 101111. *Nótese que en base* 2 *la división (al igual que las otras operaciones) es muy simple, primero porque las tablas de sumar y multiplicar son muy pequeñas, y segundo, como los dígitos que se van obteniendo en el cociente son siempre* 0 *ó* 1, *es muy fácil adivinarlos.*

4.3.6 Ejercicios

1. Escriba los números del 1 al 100 en base 2.
2. Represente:
   (a) 3680 en base 9.
   (b) 786 447 en base 16.
   (c) 1025 en base 2.
   (d) 133 en base 11.
3. Halle la representación en base 10 de los siguientes números:
   (a) $n = (1045)_8$
   (b) $n = (B1DF)_{16}$
   (c) $n = (1000001000001)_2$
   (d) $n = (121212)_3$
4. Realice las siguientes operaciones en la base dada, sin pasar a base 10.
   (a) $(11001011100)_2 + (101)_2$

(b) $(11001011100)_2 \cdot (101)_2$

(c) $(71A9)_{16} \cdot (12)_{16}$

(d) $(B1DF)_{16} + (84A)_{16}$

(e) $(7164)_8 - (643)_8$

(f) $(21222)_3 + (12121)_3$

5. Dado $a = (8764)_9$ y $b = 8$, halle q y r tales que $a = bq + r$ y $0 \leq r < b$. Haga la división en base 9, sin pasar a base 10.

6. ¿En cual base de numeración b, el número 182 se representa por $(222)_b$?

7. ¿En cual base de numeración b, el número 177 se representa por $(2301)_b$?

8. ¿En cual base el número $(212542)_6$ se representa como $(17486)_b$?

9. Halle r de modo que en base r se tenga $24^2 = 554$.

10. Demuestre que en cualquier base $b > 2$ el número representado por 121 es una cuadrado perfecto. Haga lo mismo con 144, en base $b > 4$.

11. Demuestre que si a un número natural de dos cifras, se le resta el número que resulta de invertir el orden de estas, la diferencia es divisible por 9.

12. Demuestre que si a un número natural de tres cifras, se le resta el número que resulta de invertir el orden de estas, la diferencia es divisible por 99.

13. Demuestre que si a un número natural de cuatro cifras, se le resta el número que resulta de invertir el orden de estas, y la diferencia es divisible por 999, entonces las dos cifras intermedias son iguales. Recíprocamentes, si un número natural de cuatro cifras tiene las dos cifras intermedias iguales, entonces al restarle el número que resulta de invertir el orden de estas, la diferencia es divisible por 999.

14. Determine todos los números naturales n de dos cifras que cumplen la siguiente propiedad: Si se invierten las cifras de n, el número resultante excede en 27 a n.

15. Determine los números de tres cifras que son múltiplos de 13, en cada uno de los cuales la cifra de las centenas es igual a la de las unidades.

16. Un número natural de se expresa con tres cifras en base 7. Además, al expresarlo en base 9 sus cifras son las mismas que en base 7, pero en orden inverso. Halle tal número.

17. Un número natural expresado en base b, posee un número par de cifras. Las dos cifras extremas son iguales, así como también los pares de cifras equidistantes de los extremos. Demuestre que el número dado es divisible por $b + 1$.

18. Sea n un número natural, y sea s la suma de las cifras de la expresión de n en base b. Demuestre que n es divisible por $b-1$ si y solo si s lo es.

19. Sea n un número natural, y sea m el número que resulta de invertir el orden de todas las cifras de n en base b. Demuestre que $n-m$ es divisible por $b-1$.

20. Determinar en qué base b se representa por 268 el número $(1012)_6$.

21. Cuando el número $(1204)_b$ se expresa en base decimal, se obtiene 179. Halle la base b.

22. Exprese el número $(21125)_7$ en el sistema de base 11.

Capítulo 5

Los Números Enteros

5.1 Introducción

En la enseñanza secundaria se introducen los números enteros a partir de los naturales, justificando su existencia con ideas de la vida real, como debe ser. Así, por ejemplo se habla de que -5 representa una deuda de 5 colones. La operación *suma* aparece así de manera natural: $-5+3$ representa el estado financiero de una persona que debe 5 colones y tiene tres en la bolsa. Si hace un abono con esos tres colones, quedará debiendo dos colones, y esto significa que $-5+3=-2$. También se puede hacer alusión aquí a la interpretación geométrica de los números enteros como puntos en una recta, donde n está ubicado a distancia n del origen, caminando hacia la derecha o la izquierda, dependiendo del signo de n.
La multiplicación aparece un poco más artificiosamente, pues al estudiante no le parece muy natural la ley de signos. ¿Por qué, por ejemplo, es $(-2)(-3)=6$?. Aquí se puede recurrir a la intuición, interpretando el signo menos "$-$" como un cambio de dirección, o de situación económica, etc. Pero en términos matemáticos, la razón es que queremos que se sigan cumpliendo todas las propiedades de la suma y la multiplicación, como la distributividad por ejemplo. Así, debe tenerse

$$0=(-2+2)\cdot 3=(-2)\cdot 3+2\cdot 3=(-2)\cdot 3+6,$$

de donde el único valor coherente de $-2\cdot 3$ es -6. Luego, usando esto debe tenerse

$$0=(-2)\cdot(-3+3)=(-2)\cdot(-3)+(-2)\cdot 3=-2\cdot(-3)+-6,$$

y consecuentemente $(-2)\cdot(-3)=6$. Este argumento se puede generalizar para justificar la ley de signos.
Pero, ¿cómo puede introducirse $\mathbb{Z}$ de una manera un poco más rigurosa, más allá de dibujar puntos sobre una recta, o de hablar de deudas? Un intento por hacer esto es el siguiente:

Dado que los enteros son en realidad números naturales antecedidos por un signo $+$ ó $-$, podemos pensar en estos como pares ordenados. Más precisamente, podemos definir

$$\mathbb{Z}:=(A\times\mathbb{N}^*)\cup\{0\},$$

donde A es un conjunto de dos elementos, los que denotaremos por $+$ y $-$. Esto es, $A = \{-, +\}$.
Ahora, los elementos no nulos de $\mathbb{Z}$ tienen forma $(-, n)$ ó $(+, n)$, con $n \in \mathbb{N}$, y usamos la notación $-n = (-, n)$, $+n = (+, n)$. Así, identificando el natural n con el par ordenado $(+, n)$, obtenemos $\mathbb{N} \subseteq \mathbb{Z}$.
Haciendo uso de las operaciones en $\mathbb{N}$, se definen las operaciones en $\mathbb{Z}$. Por ejemplo:

$$-3 + (-5) = -(3 + 5) = -8, \qquad -11 + 7 = -(11 - 7) = -4.$$

En general se define

$$(-n) + (-m) = -(n + m), \quad m + (-n) := \begin{cases} m - n & \text{si} \quad m \geq n \\ -(n - m) & \text{si} \quad m < n. \end{cases}$$

Similarmente se procede con la multiplicación. Luego debe demostrarse que las propiedades usuales (asociatividad, distributividad, etc.) son válidas en $\mathbb{Z}$.
Si bien es posible poner este método en un marco bastante riguroso, el estar considerando diferentes casos en cada paso, hace la exposición un poco agotadora. El método que expondremos a continuación es mucho más ágil en este sentido.

5.2 Construcción de $\mathbb{Z}$ como un conjunto cociente

Intuitivamente, un número entero es una resta de dos números naturales. Por ejemplo, $-3 = 4 - 7$, $-5 = 8 - 13$, etc. Es entonces natural pensar por ejemplo en -3 como el par ordenado $(4, 7)$, y similarmente, -5 como el par ordenado $(8, 13)$, etc. Pero existe una infinidad de pares ordenados de naturales que funcionan en la misma forma que lo hace $(4, 7)$. Por ejemplo, $1 - 4 = 9 - 12 = -3$. Si queremos una definición consistente de número entero, debemos identificar todos esos pares ordenados que "representan" a -3, y considerarlos como uno solo.
Siguiendo con la idea intuitiva, identificaremos (m, n) con (p, q) si $m - n = p - q$. Pero como todavía no podemos hablar de la resta, escribimos esto mejor como $m + q = n + p$.
Consideremos entonces la relación $\mathcal{R}$ definida en el conjunto $\mathbb{N} \times \mathbb{N}$ por

$$(m, n)\mathcal{R}(p, q) \Leftrightarrow m + q = n + p. \tag{5.1}$$

Dejamos al lector la tarea de demostrar que esta relación es de equivalencia (se hizo en ejemplos del capítulo 2). Se define

$$\mathbb{Z} = (\mathbb{N} \times \mathbb{N}) / \mathcal{R}.$$

Los elemento de $\mathbb{Z}$ son entonces clases de equivalencia, que llamaremos números enteros.

Ejemplo 5.2.1 *Sea* $u = [(8, 3)] \in \mathbb{Z}$. *Note que* $8 + 0 = 3 + 5$, *de donde* $(8, 3)\,\mathcal{R}(5, 0)$. *Esto demuestra que*

$$u = [(8, 3)] = [(5, 0)].$$

Ejemplo 5.2.2 *Considere* $z = [(3,5)] \in \mathbb{Z}$, *y note que como* $(3,5)\,\mathcal{R}(0,2)$, *tenemos* $z = [(0,2)]$.

Ejemplo 5.2.3 *Para cada* $m \in \mathbb{N}$ *se tiene* $[(m,m)] = [(0,0)]$

Los ejemplos anteriores ilustran el hecho que todo número entero se puede representar en la forma $[(m,0)]$ ó $[(0,n)]$. En efecto, si $z = [(p,q)] \in \mathbb{Z}$, tenemos tres posibilidades:

- Si $p = q$ entonce $z = [(p,p)] = [(0,0)]$.
- Si $p > q$ entonces existe un natural $m = p - q$ tal que $q + m = p$. Esto muestra que $(p,q)\,\mathcal{R}\,(m,0)$, así que $z = [(m,0)]$.
- Si $p < q$, existe un natural $n = q - p$ tal que $q = n + p$. Se tiene entonces $(p,q)\,\mathcal{R}\,(0,n)$, con lo que $z = [(0,n)]$.

Denotamos $\widehat{0} = [(0,0)]$, y para $n \in \mathbb{N}^*$ denotamos $+n = [(n,0)]$ y $-n = [(0,n)]$. Obtenemos así los enteros en su notación usual. Los elementos de la forma $-n$ se llaman enteros negativos, y los de la foma $+n$ se llaman enteros positivos.

Ejemplo 5.2.4 *El número entero* $[(6,4)] = [(2,0)]$ *se denota por* $+2$.

Ejemplo 5.2.5 *El número entero* $[(5,11)] = [(0,6)]$ *se denota por* -6.

Note que $[(m,0)] = [(0,n)]$ implica $m + n = 0$, y como $m, n \in \mathbb{N}$ se sigue que $m = n = 0$. En otras palabras, ningún entero es positivo y negativo a la vez.

El conjunto $\mathbb{Z}^+ = \{+n \in \mathbb{Z} : n \in \mathbb{N}^*\} \cup \{\widehat{0}\}$ se identifica con $\mathbb{N}$, obteniendo así $\mathbb{N} \subset \mathbb{Z}$. En otras palabras, identificamos al natural n con el entero $[(n,0)]$. Esta identificación tiene sentido puesto que la función

$$\varphi : \mathbb{N} \to \mathbb{Z}^+, \qquad \varphi(m) = [(m,0)]\,,\ \forall m \in \mathbb{N},$$

es biyectiva. Como veremos más adelante, esta función preserva las operaciones suma y producto (según la definición que daremos), y por lo tanto la identificación también tiene sentido desde un punto de vista algebraico.

5.2.1 Operaciones

Queremos ahora definir la suma y la multiplicación. Recordemos que al escribir $u = [(m,n)] \in \mathbb{Z}$, realmente estamos pensando en $u = m - n$. Entonces, si $v = [(p,q)]$, intuitivamente tendríamos

$$u + v = (m - n) + (p - q)\,,$$

y si las propiedades de la suma son lo que esperamos, esto nos lleva a $u+v = (m+p)-(n+q)$. Esto justifica la siguiente definición:

Definición 5.2.1 *Para u y v enteros, con $u = [(m,n)]$ y $v = [(p,q)]$, definimos*

$$u + v = [(m+p, n+q)].$$

Nótese que la definición se hace usando cualesquiera representantes de las clases involucradas. Para que esta definición sea coherente, no debe depender entonces de los representantes que se escojan. Antes de pasar a verificar esto, trataremos de aclararlo un poco:
Supóngase que decidimos definir una operación "$\circ$" por: $u \circ v = [(m+p, n)]$. Resulta que tomando $u = [(3,2)]$ y $v = [(1,0)]$ tenemos $u \circ v = [(4,2)]$. Pero note que también v se puede representar como $v = [(6,5)]$, y entonces, usando $(6,5)$ como representante de v obtendríamos $u \circ v = [(9,2)]$. Como $[(4,2)] \neq [(9,2)]$, esta definición no sería coherente..

Para verificar que la operación suma está bien definida en $\mathbb{Z}$, debemos probar entonces que al cambiar los representantes, ésta permanece invariante. Supongamos entonces que $u = [(m,n)] = [(m',n')]$ y $v = [(p,q)] = [(p',q')]$. Esto quiere decir que $m + n' = n + m'$ y $p + q' = q + p'$. Luego

$$m + n' + p + q' = n + m' + q + p',$$

lo que significa que

$$(m+p, n+q)\, \mathcal{R}\, \left(m' + p', n' + q'\right),$$

o equivalentemente, $[(m+p, n+q)] = [(m'+p', n'+q')]$. Entonces, efectivamente tenemos que la definición es idependiente del representante elegido.

Es un buen ejercicio para el lector, demostrar que la suma así definida es conmutativa, asociativa, tiene elemento neutro $\widehat{0} = [(0,0)]$, y que cada $a \in \mathbb{Z}$ tiene un inverso denotado por $-a$. Este inverso es único, y si $a = [(m,n)]$ entonces $-a = [(n,m)]$. En efecto, note que

$$[(n,m)] + [(m,n)] = [(n+m, n+m)] = \widehat{0}.$$

Note que en particular

$$[(m,0)] + [(p,0)] = [(m+p, 0)],$$

lo cual quiere decir que para números naturales, la suma sigue siendo la misma suma de naturales que conocíamos. Más precisamente,

$$\varphi(m) + \varphi(n) = \varphi\,(m+n),$$

donde $\varphi : \mathbb{N} \to \mathbb{Z}^+$ es la biyección que definimos arriba, y que identifica a estos dos conjuntos. La resta se define por

$$a - b = a + (-b),\ \forall a, b \in \mathbb{Z}.$$

En otras palabras, $a - b$ es el único entero x que satisface $b + x = a$. Note en particular que

$$a = b \Leftrightarrow a - b = 0.$$

Ahora, si $n, m \in \mathbb{N}$ tenemos

$$[(m,n)] = [(m,0)] + [(0,n)] = m + (-n) = m - n,$$

donde hemos usado la identificación $n \equiv \varphi(n)$. Así, la suma que acabamos de definir coincide con nuestra idea intuitiva que teníamos previamente.

La multiplicación se define de una manera un poco menos evidente. Tratemos primero de deducir cuál debe ser la definición. Dado que queremos distributividad, debemos pedir que se cumpla:

$$\begin{aligned} [(m,n)] \cdot [(p,q)] &= (m-n) \cdot (p-q) = mp - mq - np + nq \\ &= [(mp+nq, mq+np)] \end{aligned}$$

Lo anterior justifica la siguiente definición.

Definición 5.2.2 *Para $u = [(m,n)]$ y $v = [(p,q)]$ se define el producto $u \cdot v$ como*

$$u \cdot v = [(m,n)] \cdot [(p,q)] := [(mp+nq, mq+np)]\,.$$

Al igual que en el caso de la suma, se verifica que esta operación está bien definida, y que es asociativa, conmutativa, y tiene por neutro al entero $+1 = [(1,0)]$. Además, usando la distributividad de las operaciones en $\mathbb{N}$, no es difícil demostrar la distributividad en $\mathbb{Z}$. Todas estas propiedades juntas hacen de $\mathbb{Z}$ un *anillo conmutativo con unidad.*

5.2.2 Leyes de cancelación

La ley de cancelación de la suma es consecuencia directa de la estructura de anillo. Veamos:

- Para $a, b, c \in \mathbb{Z}$ se tiene $a + c = b + c \Rightarrow a = b$.

  En efecto, si $a + c = b + c$ tenemos

  $$a = a + (c + (-c)) = (a + c) + (-c) = (b + c) + (-c) = b + (c + (-c)) = b.$$

La ley de cancelación de la multiplicación no se deduce de la estructura de anillo, así que debemos usar directamente la construcción de $\mathbb{Z}$.

- Para $a, b \in \mathbb{Z}$ se tiene $ab = 0 \Rightarrow a = 0$ ó $b = 0$.

  En efecto, supongamos que $ab = 0$ y que $a \neq 0$. Hay dos posibilidades:

  Caso 1. Si $a = [(m,0)]$, con $m \in \mathbb{N}^*$, poniendo $b = [(p,q)]$ se obtiene $ab = [(mp, mq)]$. Dado que $ab = 0$ tenemos $mp = mq$, y por la ley de cancelación en $\mathbb{N}$ se sigue que $p = q$. Esto significa $b = 0$.

  Caso 2. Si $a = [(0,n)]$, con $n \in \mathbb{N}^*$, usamos que $(-a)b = 0$, y como $-a = [(n,0)]$, aplicamos el caso 1.

- Para $a, b, c \in \mathbb{Z}$, con $c \neq 0$ se tiene: $ac = bc \Rightarrow a = b$.

  En efecto, $ac = bc \Rightarrow (a - b) \cdot c = 0 \Rightarrow a - b = 0$ (pues $c \neq 0$) $\Rightarrow a = b$.

Nota: Las propiedades que acabamos de verificar, hacen de $(\mathbb{Z}, +, \cdot)$ un dominio de integridad.

5.2.3 Orden en $\mathbb{Z}$

A continuación nos dedicaremos a darle estructura de orden al anillo de los enteros.
Dados $a, b \in \mathbb{Z}$, diremos que a es menor que b si (geométricamente) a está ubicado a la izquierda de b, en la recta. Rigurosamente se tiene:

Definición 5.2.3 *Si $a, b \in \mathbb{Z}$, decimos que a es menor que b si $b - a \in \mathbb{N}^*$. En tal caso escribimos $a < b$. Cuando $b - a \in \mathbb{N}$ escribimos $a \leq b$ (a es menor o igual a b). Las relaciones $a \leq b$ y $a < b$ se escriben también $b \geq a$ y $b > a$, respectivamente.*

Nótese que la relación $\leq$ es una relación de orden. Más precisamente, esta relación tiene las siguientes propiedades:

1. Reflexividad: Para todo $a \in \mathbb{Z}$ se tiene $a \leq a$, dado que $a - a = 0 \in \mathbb{N}$.
2. Antisimetría: Si $a \leq b$ y $b \leq a$, entonces $a = b$. En efecto, si $b - a \in \mathbb{N}$ y $a - b \in \mathbb{N}$, dado que $(b - a) + (a - b) = 0$, obtenemos $a - b = 0$ (recuerde que en $\mathbb{N}$ no hay inversos).
3. Transitividad: Si $a \leq b$ y $b \leq c$, entonces $a \leq c$. Esto es claro del hecho que la suma de naturales es un natural. Esto es, dado que $b - a \in \mathbb{N}$ y $c - b \in \mathbb{N}$, se sigue que $c - a = (b - a) + (c - b) \in \mathbb{N}$.

Cuando $n \in \mathbb{N}^*$ tenemos por definición que $n > 0$, y viceversa. En tal caso decimos que n es un entero positivo. Cuando $n < 0$, decimos que n es negativo. Nótese que por definición del orden, esto significa que $-n$ es positivo.

Consideremos $m, n \in \mathbb{Z}$, y analicemos las siguientes tres posibilidades:

1. Si $m - n \in \mathbb{N}^*$, entonces $n < m$.
2. Si $-(m - n) \in \mathbb{N}^*$, entonmces $m < n$.
3. Si $m - n = 0$, entonces $m = n$.

Se concluye que dados $m, n \in \mathbb{Z}$, se cumple una y solamente una de las siguientes alternativas:

$$n < m, \quad n > m, \quad n = m.$$

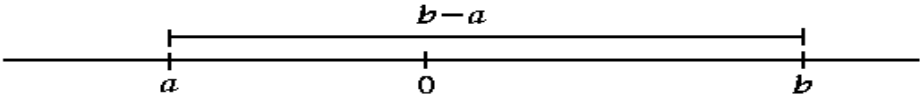
Esta es la llamada *ley de tricotomía.*

5.2.4 Representación geométrica

El entero $n > 0$ se puede representar en la recta numérica como un punto ubicado a distancia n, a la derecha del origen, mientras que si $n < 0$, lo representamos como un punto a distancia $-n$, hacia la izquierda del origen. A esa distancia la llamaremos *valor absoluto* de n, y la denotaremos por $|n|$. Definimos entonces

$$|n| = \begin{cases} n & \text{si } n \geq 0 \\ -n & \text{si } n < 0. \end{cases}$$

Si a y b son enteros, con $a < b$, entonces $b-a$ es la distancia entre los puntos correspondientes. Si no sabemos cual de los dos es mayor, podemos escribir eso como $|a - b|$.



Representación geométrica de la distancia, en el caso $a < 0 < b$.

Por ejemplo, la distancia entre los puntos correspondientes a 9 y 17 es

$$|17 - 9| = |9 - 17| = 8.$$

La distancia entre -4 y 5 es $|5 - (-4)| = |-4 - 5| = 9$.

5.2.5 El principio del buen orden visto en $\mathbb{Z}$

El principio del buen orden se puede extender a subconjuntos de $\mathbb{Z}$ que son acotados inferiormente, de acuerdo con la siguiente definición.

Definición 5.2.4 *Se dice que $A \subseteq \mathbb{Z}$ es acotado inferiormente si existe $m \in \mathbb{Z}$ tal que $m \leq n$, para todo $n \in A$. Tal m se llama cota inferior de A.*

Ejemplo 5.2.6 *El conjunto*

$$A = \left\{n^2 - 40n : n \in \mathbb{Z}\right\}$$

es acotado inferiormente en $\mathbb{Z}$. En efecto, $n^2 - 40n = (n-20)^2 - 400 \geq -400$, para todo $n \in \mathbb{Z}$. Entonces $m = -400$ es una cota inferior de A.

Lema 5.2.1 *(Generalización del buen orden) Si A es un subconjunto no vacío de $\mathbb{Z}$, acotado inferiormente, entonces A tiene primer elemento.*

Demostración
Sea m una cota inferior de A, y considere el conjunto

$$B = \{n - m : n \in A\}.$$

Como $n \geq m$ para cada $n \in A$, se tiene que $n - m \in \mathbb{N}$ para cada $n \in A$, así que $B \subseteq \mathbb{N}$. Además como existe al menos un $n \in A$, se tiene $B \neq \emptyset$. Por el principio del buen orden, B tiene primer elemento. Siendo n_0 el primer elemento de B, se concluye que $n_0 + m$ es el primer elemento de A. □

5.2.6 Ejercicios

1. Demuestre que la relación definida por (5.1), es de equivalencia en $\mathbb{N} \times \mathbb{N}$.
2. Demuestre que la buena definición de la multiplicación en $\mathbb{Z}$.
3. Demuestre las propiedades de anillo en $\mathbb{Z}$.
4. Demuestre que para todo $n \in \mathbb{Z}$ se tiene $n^2 \geq 0$.
5. Demuestre que para $n \in \mathbb{Z}$ no existe $m \in \mathbb{Z}$ tal que $n < m < n + 1$. Recuerde que no existe un natural entre 0 y 1.
6. Si $a, b \in \mathbb{Z}$ son tales que $ab = 1$, muestre que $a = b = \pm 1$.
7. En $\mathbb{Z}$ se define la relación $\mathcal{R}$ por:

$$n\mathcal{R}m \Leftrightarrow n - m \text{ es múltiplo de } 5.$$

   a. Demuestre que ésta es una relación de equivalencia.
   b. Demuestre que $\mathbb{Z}_5 = \mathbb{Z}/\mathcal{R}$ tiene exactamente 5 elementos.
   c. En $\mathbb{Z}_5$ defina las operaciones por

$$[n] + [m] = [n + m], \quad [n] \cdot [m] = [n \cdot m].$$

      Demuestre que están bien definidas.
   d. Demuestre que $\mathbb{Z}_5$ es un campo con estas operaciones (la suma y la multiplicación son asociativas, conmutativas, tienen neutro e inversos, y satisfacen la ley de distributividad).

8. En $\mathbb{Z}$ se define la relación $\mathcal{R}$ por:

$$n\mathcal{R}m \Leftrightarrow n - m \text{ es múltiplo de } 6.$$

   a. Demuestre que ésta es una relación de equivalencia.
   b. Demuestre que $\mathbb{Z}_6 = \mathbb{Z}/\mathcal{R}$ tiene exactamente 6 elementos.
   c. En $\mathbb{Z}_6$ defina las operaciones por

$$[n] + [m] = [n + m], \quad [n] \cdot [m] = [n \cdot m].$$

      Demuestre que están bien definidas.
   d. Demuestre que $\mathbb{Z}_6$ es un anillo conmutativo con unidad, pero no es un campo con estas operaciones.

9. Demuestre que para $a, b \in \mathbb{Z}$ se tiene:

(a) Si $a \geq 0$ y $b \geq 0$ entonces $ab \geq 0$.
(b) Si $a < 0$ y $b < 0$ entonces $ab > 0$.
(c) Si $a < 0$ y $b > 0$ entonces $ab < 0$.

10. Sean $a, b \in \mathbb{Z}$. Demuestre que:

(a) $a \leq b \Leftrightarrow -b \leq -a$.
(b) $a \leq b \Leftrightarrow ac \leq bc$, $\forall c > 0$.
(c) $a \leq b \Leftrightarrow bc \leq ac$, $\forall c < 0$.

11. Para $a, b \in \mathbb{Z}$, con $b > 0$, demuestre que existe $n \in \mathbb{N}$ tal que $a < bn$ (Arquimedianidad de $\mathbb{Z}$).

12. (**Algoritmo de la división en** $\mathbb{Z}$) Para $a, b \in \mathbb{Z}$, con $b > 0$, demuestre que existen $q, r \in \mathbb{Z}$ únicos, tales que
$$a = bq + r, \quad 0 \leq r < b.$$

13. Demuestre que para $n, m \in \mathbb{Z}$ se tiene

(a) $n = |n| \Leftrightarrow n \geq 0$
(b) $|n| \leq m \Leftrightarrow -m \leq n \leq m$
(c) $-|n| \leq n \leq |n|$
(d) $|n \cdot m| = |n| \cdot |m|$
(e) $|n|^2 = n^2$

14. Si $n^2 = m$ y $n \geq 0$, decimos que n es la raíz cuadrada de m, y escribimos $n = \sqrt{m}$.

(a) Demuestre que la raíz cuadrada es única, cuando existe.
(b) Para todo $n \in \mathbb{Z}$ se tiene $\sqrt{n^2} = |n|$.
(c) Si $n, m \in \mathbb{N}$ entonces
$$n \leq m \Leftrightarrow n^2 \leq m^2,$$
o sea que la función $f(n) = n^2$ es creciente en $\mathbb{N}$.
(d) Para $a, b \in \mathbb{Z}$ se tiene
$$|a| \leq |b| \Leftrightarrow a^2 \leq b^2.$$

15. Para $n, m \in \mathbb{N}$ demuestre que
$$|n + m|^2 = |n|^2 + 2nm + |m|^2.$$
Concluya que $|n + m|^2 \leq (|n| + |m|)^2$, y que por lo tanto $|n + m| \leq |n| + |m|$. Esta es la desigualdad triangular. Demuéstrela también directamente, considerando diferentes casos.

16. Sea $f : \mathbb{N} \to \mathbb{Z}$ definida por

$$f(n) = \begin{cases} \dfrac{n}{2} & \text{si } n \text{ es par} \\ -\dfrac{n+1}{2} & \text{si } n \text{ es impar.} \end{cases}$$

Demuestre que f es biyectiva, y dé una fórmula para su inversa.

5.3 Divisibilidad en $\mathbb{Z}$

Comenzaremos esta sección enunciando el algoritmo de la división en $\mathbb{Z}$. Haremos una demostración de la existencia utilizando la generalización del principio del buen orden. La unicidad la dejaremos de ejercicio.

Teorema 5.1 *(Algoritmo de la división) Sean $a, b \in \mathbb{Z}$, con $b \neq 0$. Entonces existen $q, r \in \mathbb{Z}$ únicos, tales que*

$$a = bq + r, \quad 0 \leq r < |b| .$$

Demostración
Comenzamos con el caso $b > 0$. Consideremos el conjunto

$$A = \{n \in \mathbb{Z} : bn > a\} .$$

Note que $|a|+1 \in A$, dado que $b(|a| + 1) \geq |a|+1 > a$.Esto demuestra que $A \neq \emptyset$. Además, es claro que $-|a|$ es una cota inferior de A (demuéstrelo como ejercicio). Por la generalización del principio del buen orden, se sigue que A tiene primer elemento. Si n_0 es tal elemento, se sigue que

$$b(n_0 - 1) \leq a < bn_0.$$

Tomando $q = n_0 - 1$, $r = a - bq$, se obtiene la existencia en el caso $b > 0$. El caso $b < 0$, y la unicidad se dejan como ejercicio. □

Nótese que bq es el mayor múltiplo de b que no sobrepasa a, y esta es la idea en que se basa la demostración.

Definición 5.3.1 *De acuerdo con la notación del teorema anterior, a q se le llama el cociente de la división euclideana de a por b, y a r se le llama el resto de dicha división.*

Ejemplo 5.3.1 *Si $a = -22$ y $b = 7$, se tiene $q = -4$, $r = 6$. En efecto, $bq+r = -28+6 = a$, y $0 \leq r = 6 < 7$.*

Ejemplo 5.3.2 *Si $a = 35$ y $b = -4$, se tiene $q = -8$ y $r = 3$.*

Cuando el resto es nulo, o sea cuando $r = 0$, decimos que b es divisor de a.

Definición 5.3.2 *Dados $m, n \in \mathbb{Z}$, decimos que n es divisor de m si existe $k \in \mathbb{Z}$ tal que $n \cdot k = m$. En tal caso se escribe $n \setminus m$, y el número k se denota también por $\frac{m}{n}$. Si n es divisor de m, también se dice que m es múltiplo de n (o divisible por n).*

Ejemplo 5.3.3 *El número 42 es múltiplo de 7, pues para $k = 6$ se tiene $7 \cdot k = 42$.*

Ejemplo 5.3.4 *El número 0 es múltiplo de todo número $a \in \mathbb{Z}$, pues $k = 0$ satisface $a \cdot k = 0$. Por otro lado, 0 no es divisor de ningún entero $b \neq 0$.*

Veamos algunas propiedades de la divisibilidad:

Propiedad 5.3.1 *Todo $a \in \mathbb{Z}$ es múltiplo de sí mismo, pues $a \cdot 1 = a$. Esto es, la relación $\setminus$ es reflexiva.*

Propiedad 5.3.2 *Para $a = 3$ y $b = -3$ tenemos $a \setminus b$ y $b \setminus a$, pero $a \neq b$. Entonces la relación $\setminus$ no es antisimétrica en $\mathbb{Z}$.*

Propiedad 5.3.3 *La relación $\setminus$ es transitiva. Esto es, si $a \setminus b$ y $b \setminus c$, entonces $a \setminus c$.*
En efecto, si $b = ak$ y $c = bl$, entonces $c = a(kl)$.

Propiedad 5.3.4 *Si $a \setminus b$, entonces $a \setminus (-b)$. También $(-a) \setminus b$, $(-a) \setminus (-b)$ y $|a| \setminus |b|$.*
En efecto, como a es divisor de b, existe $k \in \mathbb{Z}$ tal que $a \cdot k = b$. Luego

$$a \cdot (-k) = -b, \quad (-a) \cdot (-k) = b, \quad (-a) \cdot k = -b, \quad |a| \cdot |k| = |b| .$$

Propiedad 5.3.5 *Si a es divisor de $b \neq 0$, entonces $|a| \leq |b|$. En particular, si $a \setminus 1$ entonces $a = \pm 1$.*
Para ver esto, observemos que por la propiedad anterior se tiene $|a| \cdot k = |b|$, donde $k \geq 1$. Luego $|b| = |a| \cdot k \geq |a|$.

Propiedad 5.3.6 *Si a es divisor de b y c, entonces a es divisor de $b + c$ y $b - c$. Más generalmente, a es divisor de $bx + cy$, para todo par $x, y \in \mathbb{Z}$.*
Como a es divisor de b y c, existen $k, l \in \mathbb{Z}$ tales que $b = ak$, $c = al$. Luego

$$bx + cy = a \cdot (kx + ly) ,$$

de donde $bx + cy$ es múltiplo de a. Tomando $x = y = 1$ se obtiene que $a \setminus (b + c)$, y tomando $x = 1$, $y = -1$, se obtiene $a \setminus (b - c)$.

Propiedad 5.3.7 *Si a es divisor de b y $b + c$, entonces a es divisor de c.*
Esto es consecuencia de la propiedad anterior, pues $c = (b + c) - b$.

5.3.1 Divisor común máximo

Sean a y b enteros, no ambos nulos, y consideremos el conjunto de todos los divisores comunes de a y b. Este conjunto es finito por la propiedad 5.3.5. Entonces hay un divisor común que es mayor que todos los demás. A tal divisor lo llamaremos el divisor común máximo de a y b, y lo denotaremos por (a, b). Note que como 1 es siempre divisor de a y b, se tiene $(a, b) \geq 1$.

El símbolo $(0, 0)$ no tiene sentido en este contexto, puesto que todo entero es divisor de 0. Por este motivo, cuando escribimos (a, b), implícitamente estaremos suponiendo que a y b no son ambos nulos.

Ejemplo 5.3.5 *El máximo común divisor de* 18 *y* 12 *es* 6, *esto es* $(18, 12) = 6$. *Esto es evidente del hecho que los dos divisores más grandes de* 12 *son* 6 *y* 12, *y de ellos sólo el* 6 *es divisor de* 18.

Ejemplo 5.3.6 *Para calcular* $(45, 108)$ *podemos proceder de dos formas:*

- *Aplicamos el algoritmo de la división reiteradamente*

$$\begin{aligned} 108 &= 45 \cdot 2 + 18, \\ 45 &= 18 \cdot 2 + 9, \\ 18 &= 9 \cdot 2 + 0. \end{aligned}$$

  El MCD es el último resto no nulo. Entonces $(45, 108) = 9$.

- *Se escribe* $45 = 3^2 \cdot 5$, $108 = 2^2 \cdot 3^3$. *Como* $p = 3$ *es el único divisor común que es primo, se toma la potencia menor que aparece, esto es* $3^2 = 9$.

Más adelante justificaremos estos métodos.

Propiedad 5.3.8 *Para* a, b *enteros (no ambos nulos) tenemos* $(a, b) = (b, a)$.

Propiedad 5.3.9 *Para* $a, b \in \mathbb{Z}$ *tenemos:*

$$(a, b) = (-a, b) = (a, -b) = (-a, -b) = (|a|, |b|).$$

Esto es consecuencia de las propiedades de divisibilidad. Por ejemplo, los divisores comunes de a *y* b, *son los divisores comunes de* $-a$ *y* b, *y entonces el mayor de los divisores comunes de* a *y* b, *es el mayor de los divisores comunes de* $-a$ *y* b.

Propiedad 5.3.10 *Si* a *es divisor de* b, *entonces* $(a, b) = |a|$. *En particular* $(a, 0) = |a|$.
En efecto, por transitividad tenemos que todo divisor de a *es divisor de* b, *así que los divisores comunes de* a *y* b *son precisamente los divisores de* a. *Luego, el mayor de ellos es* $|a|$, *por la propiedad 5.3.5 de divisibilidad.*

Propiedad 5.3.11 *Si* $a = bq + r$, *entonces* $(a, b) = (b, r)$.
Para ver esto, note que por la propiedad 5.3.6 de divisibilidad, todo divisor de a *y* b, *es divisor de* $a - bq = r$, *y por lo tanto divisor común de* b *y* r. *Recíprocamente, todo divisor común de* b *y* r, *es divisor común de* a *y* b.

Esta propiedad nos da un algoritmo para hallar el máximo común divisor de dos números. Primero, por las propiedades podemos suponer $|a| > b > 0$. Si a es múltiplo de b obtenemos $(a, b) = b$. En caso contrario, aplicamos el algoritmo de la división repetidas veces hasta obtener resto cero, de la siguiente manera:

$$\begin{array}{rcll} a & = & bq_0 + r_0, & 0 < r_0 < b \\ b & = & r_0q_1 + r_1 & 0 < r_1 < r_0 \\ \vdots & \vdots & \vdots & \\ r_{n-2} & = & r_{n-1}q_n + r_n & 0 < r_n \leq r_{n-1} \\ r_{n-1} & = & r_nq_{n+1} + 0, & \end{array} \tag{5.2}$$

Note que el resto debe anularse eventualmente, pues $b > r_0 > r_1 > \ldots \geq 0$. Por la propiedad 5.3.11 se tiene

$$(a, b) = (b, r_0) = (r_0, r_1) = \cdots = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) = r_n,$$

la última igualdad por ser r_n divisor de r_{n-1}. Entonces (a, b) es el último resto que no es cero.

Ejemplo 5.3.7 *Hallar* $(434, 163)$

$$\begin{array}{rcl} 434 & = & 163 \cdot 2 + 108 \\ 163 & = & 108 \cdot 1 + 55 \\ 108 & = & 55 \cdot 1 + 53 \\ 55 & = & 53 \cdot 1 + 2 \\ 53 & = & 2 \cdot 26 + 1 \\ 2 & = & 1 \cdot 2 + 0 \end{array}$$

Entonces $(434, 163) = 1$.

Ejemplo 5.3.8 *Hallar* $(345, -715)$. *Primero usamos que* $(345, -715) = (715, 345)$. *Luego:*

$$\begin{array}{rcl} 715 & = & 345 \cdot 2 + 25 \\ 345 & = & 25 \cdot 13 + 20 \\ 25 & = & 20 \cdot 1 + 5 \\ 20 & = & 5 \cdot 4 + 0 \end{array}$$

Finalmente $(-715, 345) = 5$.

Este método nos permite además resolver ecuaciones *diofánticas.* Estas ecuaciones tienen la forma $ax + by = c$, donde a, b, c son enteros, y se buscan soluciones enteras. Por ejemplo, si queremos resolver la ecuación

$$-715x + 345y = 5,$$

despejamos sucesivamente en el algoritmo del ejemplo anterior para obtener:

$$\begin{aligned} 5 &= 25 - 20 \cdot 1 = 25 - (345 - 25 \cdot 13) \\ &= 25 \cdot 14 - 345 = (715 - 345 \cdot 2) \cdot 14 - 345 \\ &= -715 \cdot (-14) + 345 \cdot (-29) \\ &= -715x + 345y, \end{aligned}$$

donde $x = -14$, $y = -29$. En general, el mismo procedimiento demuestra que:

Lema 5.3.1 *Si $d = (a, b)$, existen $x, y \in \mathbb{Z}$ tales que $ax + by = d$.*

Este lema nos permite demostrar la siguiente caracterización del máximo común divisor:

Lema 5.3.2 *El entero $d = (a, b)$ satisface:*

1. *$d \backslash a$ y $d \backslash b$.*
2. *Si $d' \in \mathbb{Z}$ es tal que $d' \backslash a$ y $d' \backslash b$, entonces $d' \backslash d$.*

Demostración
La propiedad 1 se obtiene por definición. Ahora, si $d' \backslash a$ y $d' \backslash b$, entonces d' divide a cualquier entero de la forma $ax + by$, con $x, y \in \mathbb{Z}$. Luego, por el lema anterior se obtiene que $d' \backslash d$. □

El siguiente resultado es una ampliación del lema 5.3.1.

Lema 5.3.3 *Sean $a, b, c \in \mathbb{Z}$. Entonces la ecuación $ax + by = c$ tiene soluciones $x, y \in \mathbb{Z}$ si y sólo si c es múltiplo de $d = (a, b)$.*

Demostración:
Si la ecuación tiene solución, quiere decir que existen $x, y \in \mathbb{Z}$ tales que $ax + by = c$. Luego, como d es divisor de a y b, se sigue que es divisor de $ax + by = c$.
Recíprocamente, si c es mútiplo de d, tenemos $c = dk$, y por el lema 5.3.1 existen $x', y' \in \mathbb{Z}$ tales que $ax' + by' = d$. Luego $ax'k + by'k = dk = c$, de donde $x = x'k$, $y = y'k$ forman una solución. □

Ejemplo 5.3.9 *Hallar una solución x, y de la ecuación $434x + 163y = 3$. Del ejemplo 5.3.7 tenemos*

$$\begin{aligned} 1 = 53 - 2 \cdot 26 = 53 - (55 - 53) \cdot 26 = 53 \cdot 27 - 55 \cdot 26 \\ = (108 - 55 \cdot 1) \cdot 27 - 55 \cdot 26 = 108 \cdot 27 - 55 \cdot 53 \\ = 108 \cdot 27 - (163 - 108 \cdot 1) \cdot 53 = 108 \cdot 80 - 163 \cdot 53 \\ = (434 - 163 \cdot 2) \cdot 80 - 163 \cdot 53 = 434 \cdot 80 + 163 \cdot (-213). \end{aligned}$$

Multiplicando por 3, obtenemos que una solución está dada por $x = 240$, $y = -639$.

5.3.2 Números primos y primos entre sí

Definición 5.3.3 *Dos números enteros a y b se llaman primos entre sí (o primos relativos) si $(a, b) = 1$.*

Por ejemplo, 9 y 8 son primos entre sí, lo mismo que 11 y 20. De acuerdo con el lema 5.3.3, a y b son primos relativos si y sólo si se puede resolver la ecuación $ax + by = 1$. Una aplicación de este hecho nos da el siguiente lema.

Lema 5.3.4 *Si a y b son primos relativos, y si $a\backslash bc$, entonces $a\backslash c$.*

Demostración
Dado que existen $x, y \in \mathbb{Z}$ tales que $ax+by = 1$, tenemos $acx+bcy = c$. Ahora, evidentemente se tiene que a divide a ac, y por hipótesis también divide a bc. Luego a divide a $acx+bcy = c$. □

Definición 5.3.4 *Un número natural se llama primo si tiene exactamente dos divisores positivos. En otras palabras, $p \in \mathbb{N}$ es primo si $p > 1$ y sus únicos divisores positivos son 1 y p.*

Por ejemplo, son primos:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43.$$

Note que si p es primo entonces

$$(p, b) = \begin{cases} p & \text{si } p\backslash b \\ 1 & \text{si no.} \end{cases}$$

En lo que sigue preparamos la demostración del teorema fundamental de la aritmética.

Lema 5.3.5 *Todo entero $n \geq 2$ es primo o producto de primos.*

Demostración
Procedemos por inducción completa: Para $n = 2$ el resultado es cierto, pues es primo.
Asumiendo el resultado para $k = 2, 3, \ldots, n$, lo probaremos para $n+1$. Hay dos posibilidades:

- Si $n + 1$ es primo, no hay nada que demostrar.
- Si $n + 1$ no es primo, entonces por definición existe k tal que $2 \leq k \leq n$ y $k\backslash(n + 1)$. Esto es $n + 1 = kl$, donde también se tiene $2 \leq l \leq n$ (¿por qué?). Por hipótesis de inducción, k y l son primos o producto de primos, y consecuentemente $n+1$ es producto de primos. □

Lema 5.3.6 *Si p es primo y $p\backslash bc$, entonces $p\backslash b$ ó $p\backslash c$.*

Demostración
En efecto, si $p \backslash b$ no hay nada que demostrar. Si no, entonces $(p, b) = 1$, y por el lema 5.3.4 se tiene que $p \backslash c$.□

Nota: Si p y q son primos, y si $p \backslash q$, entonces $p = q$. De este hecho, y el lema anterior obtenemos el siguiente:

Lema 5.3.7 *Si $p, p_1, \ldots, p_n$ son primos, tales que p es divisor de $p_1 \cdot p_2 \cdot \ldots \cdot p_n$, entonces $p = p_i$, para algún $i \in \{1, \ldots, n\}$.*

Demostración
Haremos la prueba por inducción en n. Para $n = 1$ tenemos que $p \backslash p_1$, y como ambos son primos obtenemos $p = p_1$. Ahora, si el resultado es cierto para n, supongamos que p divide a

$$p_1 \cdot p_2 \cdot \ldots \cdot p_{n+1} = (p_1 \cdot p_2 \cdot \ldots \cdot p_n) \cdot p_{n+1}.$$

Por el lema anterior tenemos que $p \backslash (p_1 \cdot p_2 \cdot \ldots \cdot p_n)$ ó $p \backslash p_{n+1}$.

- Si $p \backslash p_{n+1}$ entonces $p = p_{n+1}$, pues ambos son primos.
- Si $p \backslash (p_1 \cdot p_2 \cdot \ldots \cdot p_n)$, entonces por hipótesis de inducción se sigue que $p = p_i$, para algún $i \in \{1, \ldots, n\}$.

Luego $p = p_i$, para algún $i \in \{1, \ldots, n+1\}$. □

Ahora podemos demostrar el *Teorema Fundamental de la Aritmética.*

Teorema 5.2 *Para todo $n \in \mathbb{N}$, $n \geq 2$, existe un natural $k \in \mathbb{N}$ único, y k primos $p_1, \ldots, p_k$ únicos tales que $n = p_1 \cdot \ldots \cdot p_k$ y $p_1 \leq p_2 \leq \ldots \leq p_k$.*

Demostración
Para la existencia usamos inducción completa:

- Para $n = 2$ tome $k = 1$ y $p_1 = 2$.
- Para el paso inductivo, sea p_1 el menor primo que divide a n, el cual existe por el lema 5.3.5 y el principio del buen orden. Tenemos $n = p_1 \cdot m$, donde $m < n$. Por hipótesis de inducción completa, existen $l \in \mathbb{N}$ y $q_1, \ldots, q_l$ primos tales $m = q_1 \cdot \ldots \cdot q_l$, y $q_1 \leq \ldots \leq q_l$. Definiendo $k = l + 1$, y $p_2 = q_1, \ldots, p_{l+1} = q_l$, obtenemos

$$n = p_1 \cdot m = p_1 \cdot \ldots \cdot p_k \quad \text{y} \quad p_1 \leq p_2 \leq \ldots \leq p_k.$$

La unicidad es consecuencia del lema anterior, y se deja como ejercicio. □

El lema siguiente permite explotar el teorema anterior a la hora de calcular el MCD de dos números enteros.

Lema 5.3.8 *Si $m > 0$ se tiene $(am, bm) = (a, b)\, m$. Si además m es divisor de a y b, entonces*

$$\left(\frac{a}{m}, \frac{b}{m}\right) = \frac{(a, b)}{m}.$$

Demostración
Para la primera parte, una forma es multiplicar por m el algoritmo (5.2) para hallar (a, b). Recordemos que $d = (a, b)$ es el último resto que no es 0. Luego dm es el último resto que no es cero en el algoritmo aplicado a am y bm, con lo que $dm = (am, bm)$. Otra forma es usar los lemas 5.3.2 y 5.3.3 (hágalo como ejercicio).

Para la segunda parte, aplicamos la primera cambiando a por $\dfrac{a}{m}$ y b por $\dfrac{b}{m}$, obteniendo

$$(a, b) = \left(\frac{a}{m}m, \frac{b}{m}m\right) = \left(\frac{a}{m}, \frac{b}{m}\right) m,$$

y luego divida a ambos lados por m. □

Nota: En particular, si $d = (a, b)$ se tiene:

$$\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

Note además que por el lema 5.3.5, $(a, b) = 1$ si y solo si a y b no tienen divisores primos en común.

Ejemplo 5.3.10 *Observe que $2520 = 2^3 3^2 5 \cdot 7$, mientras que $1950 = 2 \cdot 3 \cdot 5^2 13$. Entonces*

$$(2520, 1950) = 2 \cdot 3 \cdot 5 \cdot \left(2^2 3 \cdot 7, 5 \cdot 13\right) = 2 \cdot 3 \cdot 5 = 30,$$

dado que $2^2 \cdot 3 \cdot 7$ y $5 \cdot 13$ no tienen divisores primos en común.

Ejemplo 5.3.11 *En el caso de $1145\,375 = 5^3 7^2 11 \cdot 17$, y de $359\,975 = 5^2 \cdot 7 \cdot 11^2 \cdot 17$, tenemos*

$$(1145\,375, 359\,975) = 5^2 \cdot 7 \cdot 11 \cdot 17 = 32725.$$

En general, (m, n) es el producto de los primos que dividen a ambos m y n, elevados a la menor potencia con la que aparecen en la descomposición de m ó n.

5.3.3 El múltiplo común mínimo

Sean $a, b \in \mathbb{N}^*$, y sea $m \in \mathbb{N}^*$ un múltiplo común de a y b. Tenemos entonces

$$m = ak = bl, \text{ donde } k, l \in \mathbb{N}^*.$$

Si $d = (a, b)$ tenemos $a = pd$, $b = qd$, donde por el lema 5.3.8 se tiene $(p, q) = \dfrac{(a, b)}{d} = 1$. Luego

$$pdk = ak = m = bl = dql,$$

y por la ley de cancelación se tiene $pk = ql$. Entonces q divide a pk, y como $(p, q) = 1$ obtenemos que $q \backslash k$. Escribamos entonces $k = qt$, y observemos que

$$m = ak = aqt = \frac{ab}{d}t.$$

Esto demuestra que todo múltiplo común de a y b es múltiplo del número

$$[a, b] := \frac{ab}{d} = aq = bp.$$

Entonces $[a, b]$ es el múltiplo común positivo más pequeño de a y b, y es llamado el múltiplo común mínimo de a y b.
En general, para $a, b \in \mathbb{Z}^*$, el menor múltiplo común positivo de a y b es

$$[a, b] := \frac{|ab|}{d} = [|a|, |b|].$$

Note que si a y b son primos relativos, entonces $[a, b] = |ab|$. A veces se usa la abreviación MCM para *mínimo común múltiplo.*

Ejemplo 5.3.12 *Para hallar el MCM de* 48 *y* 360, *primero observamos que* $48 = 2^4 3$, $360 = 2^3 3^2 5$, *de donde* $(48, 360) = 2^3 \cdot 3 = 24$. *Luego*

$$[48, 360] = \frac{48 \cdot 360}{24} = 720.$$

Note que equivalentemente, se toman todos los primos que dividen a 48 *o* 360, *elevados a la potencia mayor con la que aparecen. Esto es*

$$[48, 360] = 2^4 \cdot 3^2 \cdot 5 = 720.$$

Ejemplo 5.3.13 *Tomando* $a = 82798848 = 2^8 3^5 11^3$ *y* $b = 81\,057\,226\,635\,000 = 2^3 3^3 5^4 7^3 11^2 17 \cdot 23 \cdot 37$, *tenemos que*

$$(a, b) = 2^3 \cdot 3^3 \cdot 11^2 = 26\,136, \quad [a, b] = \frac{ab}{26136} = 256\,789\,293\,979\,680\,000.$$

5.3.4 Ejercicios

1. Complete los detalles en la demostración del teorema 5.1.

2. Para $n \in \mathbb{N}$, demuestre que el menor divisor de n, mayor que 1, es un primo.

3. Demuestre que para un número compuesto $n \in \mathbb{N}$, el menor divisor primo de n satisface $p^2 \leq n$. Demuestre que 787 es primo.

4. Use el ejercicio anterior para hallar todos los primos entre 300 y 400.

5. Sean $a, b \in \mathbb{Z}$ no ambos nulos. Demuestre que (a, b) es el menor natural de la forma $ax + by$, con $x, y \in \mathbb{Z}$.

6. Sean $a, b \in \mathbb{N}$, primos relativos.

   (a) Demuestre que a^2 y b^2 son primos relativos. Recuerde que si un primo divide a a^2, entonces divide a a.

   (b) En general, demuestre que a^k y b^k son primos relativos, para todo $k \in \mathbb{N}$.

7. Demuestre que:

   (a) Todo número impar tiene la forma $4m + 1$ ó $4m + 3$.

   (b) El producto de números de la forma $4m + 1$ es de la forma $4m + 1$.

   (c) Si $p_1, \ldots, p_k$ son primos de la forma $4m+3$, entonces $4p_1 \cdots p_k - 1$ tiene un divisor primo de la forma $4m + 3$, el cual es distinto de $p_1, \ldots, p_k$.

   (d) Existe una cantidad infinita de primos de la forma $4m + 3$.

8. Demuestre que:

   (a) Los primos mayores que 3 tienen la forma $6m + 1$ ó $6m + 5$.

   (b) El producto de números de la forma $6m + 1$ es de la forma $6m + 1$.

   (c) Si $p_1, \ldots, p_k$ son primos de la forma $6m+5$, entonces $6p_1 \cdots p_k - 1$ tiene un divisor primo de la forma $6m + 5$, el cual es distinto de $p_1, \ldots, p_k$.

   (d) Existe una cantidad infinita de primos de la forma $6m + 5$.

9. Halle $(6188, 4709)$ de dos formas: usando el algoritmo de la división, y usando la descomposición en factores primos.

10. Para $a_1, \ldots, a_n$ enteros, no todos nulos, se define el máximo común divisor $(a_1, \ldots, a_n)$, como el mayor divisor común de todos los a_i. Halle $(81719, 52003, 33649, 30107)$.

11. Si $a, b \in \mathbb{Z}^*$ y $m > 0$, muestre que $[am, bm] = [a, b]\, m$. Si además m es divisor común de a y b, entonces
$$\left[\frac{a}{m}, \frac{b}{m}\right] = \frac{[a, b]}{m}.$$

12. Para $c \neq 0$ muestre que $(ac, bc) = (a, b)\,|c|$.

13. Si $(a, b) = 1$, y si a y b son divisores de c, entonces ab es divisor de c.

14. Sean $a, b \in \mathbb{Z}^*$. Demuestre que

   (a) $[a, b] = [b, a] = [-a, b] = [-a, -b]$

(b) Si $a > 0$ entonces $[a, b] = a \Leftrightarrow b \backslash a$

(c) $[a, b] = (a, b) \Leftrightarrow a = b$.

15. Para $a, b, c \in \mathbb{Z}^*$, muestre que $[[a, b], c] = [a, [b, c]]$.

16. Sean $a, b, c \in \mathbb{Z}$ tales que $a \backslash b + c$ y $a \backslash b - c$. Demuestre que $a \backslash 2b$.

17. Halle el MCD y el MCM de las siguientes parejas de números

(a) 300 y 396

(b) 10780 y 7280

(c) 715 y 3215

18. Halle soluciones $(x, y) \in \mathbb{Z}^2$ si existen, para las siguientes ecuaciones

(a) $125x + 80y = 5$,

(b) $77x + 49y = 11$,

(c) $39x - 52y = 13$,

(d) $134x + 1256y = 18$.

Capítulo 6

Los Números Racionales

6.1 Introducción

Recordemos la forma en que se introducen las fracciones en la escuela primaria, como una necesidad de expresar cantidades no enteras, como media naranja, tres cuartas partes de un litro, etc. Así aparecen expresiones como $\frac{1}{2}$, $\frac{2}{3}$, $\frac{3}{7}$, que representan la mitad, las dos terceras partes y las tres sétimas partes de la unidad, respectivamente. Con frecuencia encontramos expresiones como $\frac{1}{2}$, $\frac{2}{4}$, $\frac{3}{6}$, las cuales representan la misma cantidad (la mitad de la unidad, en este caso), y a las que llamamos fracciones equivalentes. Formalmente decimos:

$$\frac{m}{n} \sim \frac{p}{q} \Leftrightarrow m \cdot q = n \cdot p.$$

En este capítulo echamos mano a este y otros conceptos básicos de la teoría de fracciones, para definir los números racionales, y darles estructura de campo ordenado, a partir de la esrtructura de los números enteros. Conforme avancemos nos daremos cuenta de que hay pocas cosas nuevas en esta construcción, y de que en realidad se trata de ponerle nombre a una serie de conceptos y resultados que conocíamos y usábamos desde muy temprana edad.

6.2 Construcción

Consideremos el conjunto $\mathbb{Z} \times \mathbb{Z}^*$ de pares ordenados de números enteros, con segunda componente no nula. Haciendo la identificación de (a, b) con $\frac{a}{b}$, este conjunto corresponde al conjunto de las fracciones.

Basados en la definición que conocemos de equivalencia de fracciones, definimos la relación $\mathcal{R}$ en el conjunto $\mathbb{Z} \times \mathbb{Z}^*$ así:

$$(m, n)\mathcal{R}(p, q) \Leftrightarrow mq = np.$$

Demostremos que $\mathcal{R}$ es una relación de equivalencia.

- Dado que $mn = nm$, tenemos que $(m,n)\,\mathcal{R}(m,n)$. Esto muestra la reflexividad.
- Si $(m,n)\mathcal{R}(p,q)$ entonces $mq = np$. Esto es lo mismo que $pn = qm$, lo que implica $(p,q)\mathcal{R}(m,n)$. Entonces $\mathcal{R}$ es simétrica.
- Para la transitividad, suponga que $(m,n)\mathcal{R}(p,q)$ y $(p,q)\mathcal{R}(r,s)$. Esto significa que $mq = np$ y $ps = qr$. Luego $mqps = npqr$, y por la ley de cancelación en $\mathbb{Z}$ se sigue que $ms = nr$, o sea $(m,n)\mathcal{R}(r,s)$.

El conjunto cociente $\mathbb{Z} \times \mathbb{Z}^*/\mathcal{R}$, formado por todas las clases de equivalencia que genera la relación $\mathcal{R}$, se denota por $\mathbb{Q}$ y se llama el conjunto de los números racionales. Esto es

$$\mathbb{Q} := (\mathbb{Z} \times \mathbb{Z}^*)\,/\mathcal{R}.$$

Note que con esta definición, un número racional $[(a,b)]$ será la clase de equivalencia de la fracción (a,b), y se denotará también como $\frac{a}{b}$. Es decir, el racional denotado por $\frac{a}{b}$ es el conjunto de todas las fracciones que están relacionadas, mediante la relación $\mathcal{R}$, con la fracción (a,b). Por ejemplo:

$$\begin{aligned}\frac{3}{4} &= \{(a,b) \in \mathbb{Z} \times \mathbb{Z}^* : (3,4)\,\mathcal{R}\,(a,b)\} \\ &= \{(a,b) \in \mathbb{Z} \times \mathbb{Z}^* : 3b = 4a\} \\ &= \{\ldots, (-3,-4), (3,4), (6,8), (9,12), \ldots\}.\end{aligned}$$

Es importante notar que para todo $a \in \mathbb{Z}$ y todo $b, k \in \mathbb{Z}^*$ se tiene

$$\frac{0}{b} = \frac{0}{1}, \qquad \frac{b}{b} = \frac{1}{1}, \qquad \frac{a}{b} = \frac{ak}{bk}.$$

En efecto, basta observar que $(0,b)\,\mathcal{R}\,(0,1)$, $(b,b)\,\mathcal{R}\,(1,1)$ y $(a,b)\,\mathcal{R}\,(ak,bk)$. Es importante tener presente que por la definición misma de la relación $\mathcal{R}$ se tiene

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc.$$

6.2.1 Multiplicación en $\mathbb{Q}$

Recordemos primero la multiplicación de fracciones

$$(a,b) \odot (c,d) = (ac, bd).$$

Note que $bd \neq 0$ pues $b \neq 0$ y $d \neq 0$. Resulta sencillo probar que la relación de equivalencia $\mathcal{R}$ es compatible con esta multiplicación. En efecto, si $(a,b)\,\mathcal{R}\,(a',b')$ y $(c,d)\,\mathcal{R}\,(c',d')$, entonces $ab' = a'b$ y $cd' = c'd$, de donde $ab'cd' = a'bc'd$, lo que significa $(ac,bd)\,\mathcal{R}\,(a'c',b'd')$, esto es

$$(a,b) \odot (c,d)\,\mathcal{R}\,\left(a',b'\right) \odot \left(c',d'\right).$$

Esto permite definir la multiplicación en $\mathbb{Q}$, de la manera siguiente:

$$\frac{a}{b} \odot \frac{c}{d} = \frac{ac}{bd}.$$

Por ejemplo:

$$\frac{2}{5} \odot \frac{1}{2} = \frac{2 \cdot 1}{5 \cdot 2} = \frac{2}{10} = \frac{1}{5}.$$

Un cálculo sencillo, permite comprobar que la multiplicación definida sobre $\mathbb{Q}$ es:

1. Conmutativa: $\frac{a}{b} \odot \frac{c}{d} = \frac{c}{d} \odot \frac{a}{b}$.
2. Asociativa: $\left(\frac{a}{b} \odot \frac{c}{d}\right) \odot \frac{m}{n} = \frac{a}{b} \odot \left(\frac{c}{d} \odot \frac{m}{n}\right)$

   Además se tiene:
3. El producto o multiplicación tiene por elemento neutro al racional

$$\mathbf{1} = \frac{1}{1}.$$

4. El racional $\mathbf{0} = \frac{0}{1}$ es absorvente con respecto a la multiplicación. En efecto, para cualquier racional $\frac{a}{b}$ se tiene

$$\frac{a}{b} \odot \mathbf{0} = \frac{a}{b} \odot \frac{0}{1} = \frac{a \cdot 0}{b \cdot 1} = \frac{0}{b} = \frac{0}{1} = \mathbf{0}.$$

5. Si $a \neq 0$, $\frac{a}{b}$ tiene como inverso multiplicativo a $\frac{b}{a}$. En efecto, nótese que

$$\frac{b}{a} \odot \frac{a}{b} = \frac{ba}{ab} = \frac{ab}{ab} = \frac{1}{1} = \mathbf{1}.$$

   Denotaremos entonces

$$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}, \text{ para } \frac{a}{b} \neq \mathbf{0}.$$

6. El inverso multiplicativo es único. Es decir, el único racional r que satisface $\frac{a}{b} \odot r = \mathbf{1}$ es $\frac{b}{a}$. Para demostrar esto supongamos que efectivamente se tiene $\frac{a}{b} \odot r = \mathbf{1}$. Entonces multiplicando por $\frac{b}{a}$ se obtiene

$$\frac{b}{a} = \frac{b}{a} \odot \mathbf{1} = \frac{b}{a} \odot \left(\frac{a}{b} \odot r\right) = \left(\frac{b}{a} \odot \frac{a}{b}\right) \odot r = \mathbf{1} \odot r = r.$$

6.2.2 $\mathbb{Z}$ visto como una parte de $\mathbb{Q}$

Sea $\mathbb{Z}'$ el subconjunto de $\mathbb{Q}$ definido de la manera siguiente:

$$\mathbb{Z}' := \left\{ \tfrac{a}{1} : a \in \mathbb{Z} \right\},$$

Consideremos la función

$$\begin{array}{ccc} \varphi : \mathbb{Z} & \to & \mathbb{Z}' \\ a & \mapsto & \frac{a}{1} \end{array}$$

Note que φ es sobreyectiva, por la definición misma de $\mathbb{Z}'$. Además φ es inyectiva dado que

$$\frac{a}{1} = \frac{a'}{1} \Rightarrow (a,1)\,\mathcal{R}\,(a',1) \Rightarrow a = a'.$$

Además

$$\varphi(ab) = \frac{ab}{1} = \frac{a}{1} \odot \frac{b}{1} = \varphi(a) \odot \varphi(b).$$

Así, φ es un "isomorfismo" de $\mathbb{Z}$ en $\mathbb{Z}'$ que nos permite identificar el racional $\frac{a}{1}$ con el entero a y consecuentemente identificamos a $\mathbb{Z}$ con $\mathbb{Z}'$. Es decir, φ nos permite identificar $\mathbb{Z}$ con una parte $\mathbb{Z}'$ de $\mathbb{Q}$, y de esta manera la multiplicación en $\mathbb{Q}$ se puede ver como una prolongación de la multiplicación en $\mathbb{Z}$:

$$\forall a, b \in \mathbb{Z}, \quad a \odot b = ab.$$

Lo mismo ocurre con la suma, como veremos más adelante.
Puesto que la multiplicación de $\mathbb{Z}$ es la restricción de la multiplicación en $\mathbb{Q}$, no hay peligro de confusión y usaremos $\cdot$ en vez de $\odot$.

6.2.3 La división

Dados dos racionales $\frac{a}{b}$ y $\frac{c}{d} \neq 0$, existe un único racional r tal que $\frac{c}{d} \cdot r = \frac{a}{b}$. En efecto, suponiendo que ese es el caso debe tenerse

$$r = r \cdot 1 = r \cdot \frac{c}{d} \cdot \frac{d}{c} = \frac{a}{b} \cdot \frac{d}{c} = \frac{a}{b} \cdot \left(\frac{c}{d}\right)^{-1}.$$

Esto demuestra que efectivamente existe tal r, y que es único. Esto nos sugiere la siguiente definición.

Definición 6.2.1 *Para $\frac{a}{b} \in \mathbb{Q}$ y $\frac{c}{d} \in \mathbb{Q}^*$ se define la división del primero por el segundo así:*

$$\frac{a}{b} \div \frac{c}{d} = \frac{a}{b} \cdot \left(\frac{c}{d}\right)^{-1} = \frac{ad}{bc}.$$

Por ejemplo se tiene

$$\frac{2}{5} \div \frac{-4}{9} = \frac{2 \cdot 9}{5 \cdot (-4)} = \frac{18}{-20} = \frac{-9}{10}.$$

Note que si $r = \dfrac{a}{b}$ es un racional arbitrario, entonces se puede escribir

$$r = \frac{a}{1} \cdot \frac{1}{b} = \frac{a}{1} \cdot \left(\frac{b}{1}\right)^{-1}.$$

Recordando la identificación que hemos hecho de $\frac{a}{1}$ con a tenemos

$$\frac{a}{b} = ab^{-1} = a \div b,$$

así que todo número racional es el cociente de dos enteros.

6.2.4 Representación canónica

Recordemos que

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc.$$

En particular, para $k \in \mathbb{Z}^*$ se tiene $\dfrac{ak}{bk} = \dfrac{a}{b}$, dado que $akb = bka$. Tomando $k = -1$ se obtiene $\dfrac{a}{b} = \dfrac{-a}{-b}$. Esto permite siempre obtener un representante $\dfrac{a}{b}$ con $b > 0$. En efecto, si $r = \dfrac{a}{b} \in \mathbb{Q}$, y si $b < 0$, escribimos $r = \dfrac{-a}{-b}$, donde el denominador es ahora $-b > 0$.
Por otro lado, si d es el máximo común divisor entre a y b, tenemos que $a = dm$, $b = dn$, con $m, n \in \mathbb{Z}$, $n > 0$. Luego

$$\frac{a}{b} = \frac{md}{nd} = \frac{m}{n},$$

y recordemos que m y n resultan ser primos relativos. Esto significa que todo número racional se puede representar por una fracción, cuyo numerador y denominador son primos relativos.

Definición 6.2.2 *Diremos que un racional $r = \dfrac{m}{n}$ está escrito en su forma canónica reducida, si $n > 0$ y m y n son primos relativos.*

Por ejemplo, los racionales

$$\frac{3}{5}, \frac{1}{20}, \frac{-72}{175}, \frac{-125}{49}, \frac{561}{455}$$

están escritos en forma canónica reducida. Por otro lado, los racionales

$$\frac{4}{-3}, \frac{105}{72}, \frac{-7}{-11}, \frac{1024}{1026}$$

no están escritos en su forma canónica reducida.

6.2.5 Definición de la suma en $\mathbb{Q}$

El lector probablemente conoce la definición de la suma en $\mathbb{Q}$. Pero, ¿por qué se define la suma así y no de otra manera? Tratemos de hallar una respuesta. Dado que esperamos que $\mathbb{Q}$ sea un campo, debemos tener distributividad de la multiplicación con respecto a la suma. Como además $b \cdot b^{-1} = 1$ debemos tener

$$\frac{a}{b} + \frac{c}{d} = ab^{-1} + cd^{-1} = ab^{-1}dd^{-1} + cd^{-1}bb^{-1} = (ad + bc)\,(bd)^{-1}\,.$$

Ahora, definimos la suma $\oplus$ sobre $\mathbb{Q}$ de la manera siguiente:

$$\frac{a}{b} \oplus \frac{c}{d} = \frac{ad + bc}{bd}.$$

Para que esta definición sea coherente, no debe depender del representante que se escoja. Para verificar que ese es el caso, supongamos que $u = \dfrac{m}{n} = \dfrac{m'}{n'}$ y $v = \dfrac{p}{q} = \dfrac{p'}{q'}$. Entonces $mn' = nm'$ y $pq' = qp'$, de donde

$$(mq + np)\,n'q' = mn' \cdot qq' + nn' \cdot pq' = nm' \cdot qq' + nn' \cdot qp' = nq\left(m'q' + n'p'\right),$$

lo que demuestra que

$$\frac{mq + np}{nq} = \frac{m'q' + n'p'}{n'q'},$$

y la definición es independiente del representante elegido.

Esta suma puede verse como una prolongación de la suma en $\mathbb{Z}$: si $a, c \in \mathbb{Z}$,

$$a \oplus c = \frac{a}{1} \oplus \frac{c}{1} = \frac{a \cdot 1 + 1 \cdot c}{1} = a + c.$$

Por esto, al igual que en el caso de la multiplicación, usaremos $+$ en vez de $\oplus$.

6.2.6 Propiedades de la suma en $\mathbb{Q}$

1. La suma es conmutativa.
2. La suma es asociativa.
3. 0 es elemento neutro de la suma.
4. $\dfrac{-a}{b}$ es el inverso de $\dfrac{a}{b}$ para la suma. Es decir, $-\frac{a}{b} = \frac{-a}{b}$.

Se deja al lector la tarea de demostrar estas propiedades.

6.2.7 $\mathbb{Q}$ es un campo

Además de las propiedades anteriores, tenemos la distributividad de la multiplicación con respecto a la suma:

$$\frac{m}{n}\cdot\left(\frac{a}{b}+\frac{c}{d}\right)=\frac{m}{n}\cdot\frac{a}{b}+\frac{m}{n}\cdot\frac{c}{d}.$$

Esto puede verificarse sin mucha dificultad. Entonces $\mathbb{Q}$ es anillo conmutativo con unidad. Como además todo elemento diferente de 0 tiene inverso multiplicativo, $\mathbb{Q}$ es un *campo*.

6.2.8 Leyes de cancelación en $\mathbb{Q}$

Las leyes de cancelación aquí son consecuencia directa de la estructura de campo. Veamos:

- Para $a,b,c\in\mathbb{Q}$ se tiene $a+c=b+c\Rightarrow a=b$.

  En efecto, si $a+c=b+c$ tenemos

  $$\begin{aligned} a &= a+0=a+(c+(-c))\\ &= (a+c)+(-c)\\ &= (b+c)+(-c)\\ &= b+(c+(-c))=b. \end{aligned}$$

  Similarmente,

- Para $a,b,c\in\mathbb{Q}$, con $c\neq 0$, se tiene $ac=bc\Rightarrow a=b$. En particular, al igual que en $\mathbb{Z}$ se tiene

  $$ab=0\Leftrightarrow (a=0 \text{ ó } b=0).$$

  Ejercicio: Demuéstrelo.

6.2.9 Orden y valor absoluto en $\mathbb{Q}$

Centrémos nuestra atención en la estructura de orden del campo de los racionales. Diremos que un racional r es positivo si se puede representar como una fracción $\dfrac{m}{n}$, donde ambos m y n son enteros positivos. Por ejemplo, $r=\dfrac{-4}{-5}$ es positivo, pues se puede representar como $r=\dfrac{4}{5}$. Por otro lado, el racional $\frac{-2}{3}$ no es positivo, pues si $\frac{-2}{3}=\frac{m}{n}$, se sigue que $-2n=3m$, lo que muestra que m y n tienen signos opuestos. En general $r=\frac{a}{b}$ es positivo cuando, y solo cuando a y b tienen el mismo signo.

Dados $u,v\in\mathbb{Q}$, diremos que u es menor que v si $v-u$ es positivo. En tal caso escribimos $u<v$, o también $v>u$ (v es mayor que u). Por ejemplo, nótese que $\frac{4}{3}-\frac{5}{4}=\frac{1}{12}$ es positivo, y por lo tanto

$$\frac{5}{4}<\frac{4}{3}.$$

En general, tomemos $u = \dfrac{p}{q}$ y $v = \dfrac{m}{n}$ en su forma canónica. En particular se tendrá $qn > 0$. Entonces $v - u = \dfrac{mq - np}{qn}$ es positivo si y solo si el numerador lo es, esto es:

$$u < v \Leftrightarrow mq - np > 0 \Leftrightarrow np < mq.$$

Entonces, otra manera de dar la definición del orden estricto es la siguiente:

$$\frac{p}{q} < \frac{m}{n} \Leftrightarrow pn < qm,$$

donde se asume que los denominadores son positivos.

Se define la relación $\leq$ por:

$$u \leq v \Leftrightarrow pn \leq qm,$$

esto es, si $u < v$ ó $u = v$. Note que

$$u \leq v \Leftrightarrow v - u \in \mathbb{Q}^+.$$

Por ejemplo, $\dfrac{2}{3} \leq \dfrac{3}{4}$ pues $2 \cdot 4 = 8 \leq 9 = 3 \cdot 3$. Se le deja al lector la tarea de demostrar que esta relación es de orden.

Definición 6.2.3 *El* valor absoluto *de* $u = \dfrac{m}{n}$ *se define por* $|u| = \dfrac{|m|}{|n|}$. *Es decir*

$$|u| = \begin{cases} u & si\ u \geq 0 \\ -u & si\ u < 0. \end{cases}$$

Dados $u = \dfrac{m}{n}$ y $v = \dfrac{p}{q}$ en $\mathbb{Q}$, hay tres posibilidades:

1. Si $mq > np$ tenemos $u > v$,
2. Si $mq < np$ se tiene $u < v$,
3. Si $mq = np$ entonces $u = v$.

Entonces el orden en $\mathbb{Q}$ satisface la *ley de tricotomía,* y por lo tanto $(\mathbb{Q}, +, \cdot, \leq)$ es un campo totalmente ordenado.

El lema siguiente demuestra que con este orden $\mathbb{Q}$ es arquimediano.

Lema 6.2.1 *dados* a *y* b *en* $\mathbb{Q}$, *con* $b > 0$, *existe un natural* n *tal que* $a < bn$.

Demostración
Si $a \leq 0$ basta tomar $n = 1$.
Si $a > 0$, expresemos en forma canónica $a = \dfrac{m}{k}$, $b = \dfrac{p}{q}$. Como $k \geq 1$ y $p \geq 1$ se tiene

$$a \leq m < m + 1 \leq (m + 1)\, p = b\,(m + 1)\, q,$$

y entonces podemos tomar $n = (m + 1)\, q$. □

Al igual que en $\mathbb{Z}$ se define la distancia entre los racionales a y b por:

$$d(a, b) = |a - b|\,.$$

6.2.10 Densidad del orden en $\mathbb{Q}$

Dados $a, b \in \mathbb{Q}$, con $a < b$, existe al menos un racional r tal que $a < r < b$. En efecto, tomando $r = \frac{1}{2}\,(a + b)$ tenemos $b - r = r - a = \dfrac{1}{2}\,(b - a) > 0$, así que $a < r < b$. De hecho note que r está ubicado en el punto medio de a y b en la recta numérica.
Nótese que el argumento se puede repetir, tomando ahora a y r (o r y b) en vez de a y b. Se obtiene así por inducción que entre dos números racionales existe una infinidad de otros números racionales.

6.2.11 Parte entera

Sea $x = \dfrac{m}{n} \in \mathbb{Q}$, en su forma canónica. Por el algoritmo de la división, existen únicos $q, r \in \mathbb{Z}$ tales que

$$m = qn + r, \quad 0 \leq r < n.$$

Tenemos entonces

$$x = \frac{m}{n} = \frac{qn + r}{n} = q + \frac{r}{n},$$

y en particular $q \leq a = q + \dfrac{r}{n} < q + 1$. La siguiente definición se basa en esta observación.

Definición 6.2.4 *Dado el racional x, al único entero q que satisface $q \leq x < q + 1$, se le llama la parte entera de x, y se denota por $q = [\![x]\!]$.*

6.3 Sobre la no completitud de $\mathbb{Q}$

Los números racionales se pueden representar en una recta *numérica,* de la siguiente manera. Dado $\dfrac{m}{n} \in \mathbb{Q}$, en forma canónica, partimos de la representación geométrica de $\mathbb{N}$, subdividiendo cada unidad en n partes iguales, y luego contando $|m|$ de estas partes a partir del origen, hacia la derecha o la izquierda dependiendo del signo de m.
Así, todo racional tiene asociado un punto sobre la recta, y surge la siguiente pregunta: ¿Tendrá todo punto de la recta un racional asociado? La respuesta es no, como lo muestra el siguiente lema:

Lema 6.3.1 *No existe un racional r tal que $r^2 = 2$.*

Demostración
Suponga que sí existe tal r, y tomemos su representación canónica $r = \frac{a}{b}$. Tenemos entonces que a y b son primos relativos, y por el ejercicio 6 del capítulo anterior se sigue que a^2 y b^2 lo son. Dado que $a^2 = 2b^2$, se sigue que $\left(a^2, b^2\right) = b^2$, de donde $b = 1$. Pero entonces r sería natural, y eso es imposible. □

Esto demuestra que efectivamente los racionales dejan huecos en la recta, pues según el teorema de Pitágoras, hay un punto sobre la recta cuya distancia al origen debería ser $\sqrt{2}$. Un argumento similar se usa para demostrar que, para $p \in \mathbb{N}$ no existe un racional r tal que $r^2 = p$, a menos que p sea cuadrado perfecto.

6.4 Potenciación en $\mathbb{Q}$

El problema de cómo definir la función exponencial es central en matemática, en particular a nivel de enseñanza. Empezando con la definición más simple

$$a^n = \underbrace{a \cdot a \cdots a}_{n \text{ veces}}, \quad \text{para } a > 0,\ n \in \mathbb{N},$$

ya tenemos un pequeño problema de rigurosidad. Esto tal vez no sea tan grave pues intuitivamente "todo el mundo" sabe lo que significa "n veces". Además, no es difícil corregir el problema usando recurrencia. Podemos definir:

$$a^1 = a, \quad a^{n+1} = a^n \cdot a, \quad \forall n \in \mathbb{N}.$$

Las siguientes propiedades son válidas para $a, b \in \mathbb{Q}$, $a, b > 0$.

1. $a^m \cdot a^n = a^{m+n}$, $\forall n, m \in \mathbb{N}$.
2. $(a^n)^m = a^{n \cdot m}$, $\forall n, m \in \mathbb{N}$.
3. $\frac{a^n}{a^m} = a^{n-m}$, $n > m$.
4. $(ab)^n = a^n \cdot b^n$, $\forall n \in \mathbb{N}$.
5. $\left(\frac{a}{b}\right)^n = \frac{a^n}{b^n}$, $\forall n \in \mathbb{N}$.

Como ejemplo demostremos la propiedad **1**: Aquí otra vez se puede apelar a la intuición y decir que

$$a^m \cdot a^n = \underbrace{a \cdot a \cdots a}_{m \text{ veces}} \cdot \underbrace{a \cdot a \cdots a}_{n \text{ veces}} = \underbrace{a \cdot a \cdots a}_{m+n \text{ veces}}$$

Pero si se quiere ser riguroso, se debe usar el principio de inducción otra vez. Dejamos m fijo y aplicamos inducción sobre n.

- Para $n = 1$, tenemos $a^m \cdot a^n = a^m \cdot a = a^{m+1}$ por definición.
- En el paso inductivo tenemos como hipótesis $a^m \cdot a^n = a^{m+n}$, y entonces

$$a^m \cdot a^{n+1} = a^m \cdot (a^n \cdot a) = (a^m \cdot a^n) \cdot a = a^{m+n} \cdot a = a^{(m+n)+1} = a^{m+(n+1)}.$$

La segunda igualdad se trata similarmente, mientras que la tercera se puede demostrar usando la primera. En efecto, como $n - m \in \mathbb{N}$ tenemos

$$a^{n-m} \cdot a^m = a^{(n-m)+m} = a^n,$$

y luego dividimos por a^m.

Estas identidades nos dan una idea de lo que sigue, pues queremos que sean válidas en general, sin restricciones en n y m. Entonces, si queremos que la tercera sea válida con $n = m$ debemos tener

$$a^0 = a^{n-n} = \frac{a^n}{a^n} = 1.$$

Debemos definir entonces $a^0 := 1$. Nótese que no hemos demostrado que $a^0 = 1$, sólo hemos justificado por qué definirlo así.
Luego, al tomar $n = 0$ y $m \in \mathbb{N}$ justificamos la definición

$$a^{-m} := \frac{1}{a^m}, \quad \forall m \in \mathbb{N}.$$

Con esto tenemos definido a^z, para $a \in \mathbb{Q}_*^+$ y cualquier $z \in \mathbb{Z}$.

En este punto debemos demostrar que las propiedades **1**,...,**5** siguen siendo válidas para todo $n, m \in \mathbb{Z}$. Por ejemplo, si $n < 0$ y $m > 0$, tenemos $n = -p$, con $p \in \mathbb{N}$, y entonces

$$(a^n)^m = \left(a^{-p}\right)^m = \left(\frac{1}{a^p}\right)^m = \frac{1^m}{(a^p)^m} = \frac{1}{a^{pm}} = a^{-pm} = a^{nm},$$

donde usamos las propiedades **2** y **5** para $p, m \in \mathbb{N}$.

6.5 Ejercicios

1. Demuestre las propiedades de la suma en $\mathbb{Q}$.
2. Demuestre que la multiplicación está bien definido en $\mathbb{Q}$.
3. Demuestre las propiedades de la multiplicación en $\mathbb{Q}$.
4. Demuestre que para todo $a \in \mathbb{Q}$ se tiene $a^2 \geq 0$.
5. Demuestre que para $a \in \mathbb{Q} \backslash \mathbb{Z}$ existe $m \in \mathbb{Z}$ tal que $a < m < a + 1$.

6. Para $a, b \in \mathbb{Q}$ muestre que $a^2 + b^2 \geq 2ab$.

7. Sean $a, b \in \mathbb{Q}$, del mismo signo. Demuestre que $\dfrac{a}{b} + \dfrac{b}{a} \geq 2$. En particular $a + \dfrac{1}{a} \geq 2$, para todo $a \in \mathbb{Q}_*^+$.

8. Demuestre que para $a, b \in \mathbb{Q}$ se tiene:

   (a) Si $a \geq 0$ y $b \geq 0$ entonces $ab \geq 0$.
   (b) Si $a < 0$ y $b < 0$ entonces $ab > 0$.
   (c) Si $a < 0$ y $b > 0$ entonces $ab < 0$.

9. Sean $a, b \in \mathbb{Q}$. Demuestre que:

   (a) $a \leq b \Leftrightarrow -b \leq -a$.
   (b) $a \leq b \Leftrightarrow ac \leq bc$, $\forall c > 0$.
   (c) $a \leq b \Leftrightarrow bc \leq ac$, $\forall c < 0$.

10. Demuestre que para $a, b \in \mathbb{Q}$ se tiene

    (a) $a = |a| \Leftrightarrow a \geq 0$
    (b) $|a| \leq b \Leftrightarrow -b \leq a \leq b$
    (c) $-|a| \leq a \leq |a|$
    (d) $|a \cdot b| = |a| \cdot |b|$
    (e) $|a|^2 = a^2$

11. Si $a^2 = b$ y $a \geq 0$, decimos que a es la raíz cuadrada de b, y escribimos $a = \sqrt{b}$.

    (a) Demuestre que la raíz cuadrada es única, cuando existe.
    (b) Para todo $a \in \mathbb{Q}$ se tiene $\sqrt{a^2} = |a|$.
    (c) Si $a, b \in \mathbb{Q}^+$ entonces
    $$a \leq b \Leftrightarrow a^2 \leq b^2,$$
    o sea que la función $f(x) = x^2$ es creciente en $\mathbb{Q}$.
    (d) Demuestre que si p es primo, entonces no tiene raírz cuadrada en $\mathbb{Q}$.

12. Demuestre la desigualdad triangular en $\mathbb{Q}$.

13. Sea $f : \mathbb{N} \times \mathbb{N} \to \mathbb{Z}$ definida por $f(m, n) = 2^m 3^n$. Demuestre que f es inyectiva, pero no sobreyectiva. Entonces $\mathbb{N} \times \mathbb{N}$ y $\mathbb{N}$ tienen la misma cantidad de elementos.

14. Sea $g : \mathbb{N} \times \mathbb{N}^* \to \mathbb{Q}^+$ definida por $g(m,n) = \dfrac{m}{n}$. Demuestre que g es sobreyectiva pero no inyectiva.

15. Sean $a, b \in \mathbb{Q}$. Entonces existe un único $x \in \mathbb{Q}$ tal e $a + x = b$. El número $b + (-a)$, se denota usualmente como $b - a$. Para $b = 0$, esto demuestra en particular que el inverso de a es único.

16. Sean $a, b \in \mathbb{Q}$, $a \neq 0$. Entonces existe un único número racional y tal que $ay = b$.

    Usualmente el número $b \cdot a^{-1}$ se denota por $\frac{b}{a}$. Con $b = 1$, esto demuestra que el inverso multiplicativo de a es único.

17. Si $x \in \mathbb{Q}$ es tal que $ax = a$ para algún $a \neq 0$, muestre que $x = 1$.

18. Para todo $a \in \mathbb{Q}$, $-(-a) = a$.

19. Para todos a y b en $\mathbb{Q}$, se tiene que $-(a + b) = (-a) + (-b)$.

20. Para todo $a \in \mathbb{Q}$, $a \cdot 0 = 0 \cdot a = 0$. Esta propiedad se conoce como la propiedad absorbente del cero.

21. Sean a y b dos números racionales. Entoces $a \cdot b = 0$ si y sólo si $a = 0$ o $b = 0$.

22. Para todo $a \in \mathbb{Q}$, $a \neq 0$, se tiene que $\left(a^{-1}\right)^{-1} = a$.

23. Para todos $a, b \in \mathbb{Q}$, $a \neq 0 \neq b$, se tiene que $(ab)^{-1} = a^{-1}b^{-1}$.

24. Sean $a, b \in \mathbb{Q}$. Entonces:

    $$\text{(i)}\ a(-b) = -(ab)$$
    $$\text{(ii)}\ (-a)b = -(ab)$$
    $$\text{(iii)}\ (-a)(-b) = ab$$

    Este resultado se conoce como la ley de los signos. Concluya que $(-1) \cdot a = -a$.

25. Para todos $a, b \in \mathbb{Q}$, $b \neq 0$, se tiene que $\frac{a}{b} = 0 \Leftrightarrow a = 0$.

26. Si $a > 0 \Rightarrow a^{-1} > 0$.

27. Si $ac \leq bc$ y $c > 0$, entonces $a \leq b$.

28. Si $a \leq b$ y $c < 0$, entonces $b \leq a$.

29. $a > b > 0 \Rightarrow \frac{1}{b} > \frac{1}{a}$.

30. $a > 1 \Rightarrow a^2 > a$.

31. $0 < a < 1 \Rightarrow a > a^2$.

32. Demuestrepor inducción las propiedades de la potenciación en $\mathbb{Q}$, con exponentes naturales. Deduzca dichas propiedades para exponentes enteros.

33. Demuestre que para todo $n \in \mathbb{N}$ tal que $n \geq 9$ se tiene $\left(\frac{3}{2}\right)^n > 4n$.

6.6 Representación de racionales en diferentes bases

Hemos visto que cada racional es al fin un cociente de dos números enteros, cuyo denominador es diferente de 0. O lo que es lo mismo, todo racional podrá expresarse siempre por $\frac{p}{q}$, con $p, q \in \mathbb{Z}$ y $q \neq 0$, o cualquiera de sus fracciones equivalentes. Note que, sin embargo, la representación canónica es única.

Sabemos que dado un sistema de numeración de base $b > 1$, todo entero positivo p se puede expresar según las potencias sucesivas de b, es decir:

$$p = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0, \tag{6.1}$$

donde los coeficientes $a_k, a_{k-1}, \ldots, a_1, a_0$ son naturales estrictamente menores que b, y para los cuales ya el sistema cuenta con símbolos para representarlos. Puesto que la forma polinómica (6.1) está determinada unívocamente por los coeficientes $a_k, \ldots, a_0$, resulta claro que estos son suficientes para hacer una representación única del entero p. Por esta razón, se acostumbra escribir:

$$p = a_k a_{k-1} \ldots a_1 a_0$$

que a veces se llama *expresión cifrada* de p en base b.

Por ejemplo, si la base es diez, cuando escribinmos $a = 3248$, estamos indicando que los números representados por los símbolos $3, 2, 4$ y 8 son los coeficientes de la forma polinómica cuyo valor numérico es a. Así, $a = 3 \cdot 10^3 + 2 \cdot 10^2 + 4 \cdot 10 + 8$ y su expresión cifrada es 3248.

En adelante, vamos a representar los racionales en su forma canónica. Es decir, cuando escribamos $\frac{p}{q}$ asumiremos que $(p, q) = 1$ y $q > 0$.

Consideremos el racional $\frac{m}{n}$. Utilizando el algoritmo de la división, obtenemos:

$$m = qn + r,\ 0 \leq r < n,$$

es decir:

$$\frac{m}{n} = q + \frac{r}{n},\ 0 \leq \frac{r}{n} < 1.$$

El número q se llama la parte entera del racional $\frac{m}{n}$. Si denotamos la parte entera de $\frac{m}{n}$ por $[\![\frac{m}{n}]\!]$, se tiene que:

$$[\![\tfrac{m}{n}]\!] \leq \tfrac{m}{n} < [\![\tfrac{m}{n}]\!] + 1,$$

pues $\frac{r}{n} < 1$, y se ve claramente que :

$$\frac{r}{n} = \frac{m}{n} - q = \frac{m}{n} - [\![\frac{m}{n}]\!].$$

Es claro que todo racional queda determinado unívocamente por su parte entera y su parte fraccionaria $\frac{r}{n}$.

Puesto que ya sabemos representar enteros en cualquier sistema de numeración de base $b > 1$, el problema de representar racionales en un sistema de base b se reduce al problema de estudiar la representación de los racionales en $[0, 1[$.

Vamos a estudiar el caso más sencillo, el caso de los números $b-$ádicos, cuando $b = 10$.

Definición 6.6.1 *Sea $b \geq 2$. Se dice que un racional x es un número $b-$ádico si existe $k \in \mathbb{N}$ y un entero a tal que*

$$x = \frac{a}{b^k}$$

Ejemplo 6.6.1 *Los números $\frac{1}{2}, \frac{7^3}{4}, -\frac{19}{2^{10}}$ son números diádicos ($b = 2$). Los números $\frac{3}{10}$, $\frac{14}{10^5}$ son $b-$ádicos, con $b = 10$.*

6.6.1 Una partición de $\mathbb{Q}$

Trabajaremos con una base de numeración b. Definimos los siguientes subconjuntos de $\mathbb{Q}$:

- $\mathbb{Q}_d$ está formado por aquellos racionales no nulos que, al expresarlos en su forma canónica, los divisores primos de su denominador son todos divisores primos de b. Por ejemplo, si el sistema es el sistema decimal, cuya base 10 tiene por divisores primos, solamente al 2 y al 5, el número racional $\frac{3}{250} = \frac{3}{2 \cdot 5^3}$ pertenece a $\mathbb{Q}_d$, mientras que $\frac{5}{21}$ no pertenece a $\mathbb{Q}_d$.

- $\mathbb{Q}_p$ está formado por los racionales no nulos que no pertenecen a $\mathbb{Q}_d$. Es decir, si r se expresa en forma canónica como $\frac{m}{n}$, entonces $r \in \mathbb{Q}_p$ si n contiene al memos un divisor que no es divisor de b. Por ejemplo, en el sistema decimal,

  $$\frac{1}{6} = \frac{1}{2 \cdot 3} \in \mathbb{Q}_p,$$

  puesto que $n = 6$ contiene como divisor al 3, que no es divisor de 10.

Resulta inmediato que

$$\mathbb{Q}_d \neq \emptyset,\ \mathbb{Q}_p \neq \emptyset,\ \mathbb{Q}_d \cap \mathbb{Q}_p = \emptyset,\ \text{y}\ \mathbb{Q}^* = \mathbb{Q}_d \cup \mathbb{Q}_p.$$

Es decir, los conjuntos $\mathbb{Q}_d$ y $\mathbb{Q}_p$ forman una partición de $\mathbb{Q}^*$.

Seguidamente, estudiaremos con más detalle los conjuntos $\mathbb{Q}_d$ y $\mathbb{Q}_p$ para el caso del sistema de numeración de base 10. Sin embargo, es fácil percatarse que los resultados que obtendremos no dependen de la base escogida y que, por lo tanto, se pueden generalizar a cualquier base b.

6.6.2 El subconjunto $\mathbb{Q}_d$

Sea $\frac{m}{n} \in \mathbb{Q}_d$, entonces: $n = 2^\alpha \cdot 5^\beta$, donde $\alpha, \beta \in \mathbb{N}$. Note que:

- Si $\alpha = \beta$, entonces $n = 2^\alpha \cdot 5^\alpha = (10)^\alpha$, y $\dfrac{m}{n} = \dfrac{m}{10^\alpha}$.
- Si $\alpha > \beta$, multiplicando m y n por $5^{\alpha-\beta}$ se obtiene:

$$\frac{m}{n} = \frac{m \cdot 5^{\alpha-\beta}}{2^\alpha \cdot 5^\beta \cdot 5^{\alpha-\beta}} = \frac{k}{2^\alpha \cdot 5^\alpha} = \frac{k}{10^\alpha}, \text{ con } k = m \cdot 5^{\alpha-\beta}.$$

- Si $\alpha < \beta$, multiplicando m y n por $2^{\beta-\alpha}$ se obtiene:

$$\frac{m}{n} = \frac{m \cdot 2^{\beta-\alpha}}{2^\alpha \cdot 5^\beta \cdot 2^{\beta-\alpha}} = \frac{k}{2^\beta \cdot 5^\beta} = \frac{k}{10^\beta}, \text{ con } k = m \cdot 2^{\beta-\alpha}.$$

Es decir, en cualquier caso el racional $\dfrac{m}{n}$ puede expresarse mediante una fracción equivalente cuyo denominador es una potencia de 10. Es decir,

$$\frac{m}{n} \in \mathbb{Q}_d \text{ si y solo sí } \frac{m}{n} = \frac{a}{10^k}, \text{ para algún } k \in \mathbb{N}.$$

Este hecho, permite dar la siguiente definicion.

Definición 6.6.2 *Se llama fracción decimal a todo racional perteneciente a $\mathbb{Q}_d$, es decir a todo racional que pueda expresarse mediante una fracción equivalente cuyo denominador sea una potencia natural de* 10.

Entonces son equivalentes:

- $\dfrac{m}{n}$ es una fracción decimal
- $\dfrac{m}{n} \in \mathbb{Q}_d$
- Existen $a \in \mathbb{Z}$ y $k \in \mathbb{N}$ tales que $\dfrac{m}{n} = \dfrac{a}{10^k}$.

Note que la notación $\mathbb{Q}_d$ tiene su razón de ser en el hecho que es el conjunto de todos los racionales que son fracciones decimales.

6.6.3 Acerca de la expresión decimal de los racionales de $\mathbb{Q}_d$

Sea r un racional perteneciente a $\mathbb{Q}_d$, es decir r es una fracción decimal y por lo tanto podrá expresarse como $r = \dfrac{a}{10^n}$.
Ahora, a es un entero y se puede representar en base 10 como :

$$a = u_k \cdot 10^k + u_{k-1} \cdot 10^{k-1} + \cdots + u_1 \cdot 10 + u_0,$$

o en su forma cifrada:

$$a = u_k u_{k-1} \ldots u_1 u_0.$$

Luego

$$r = \frac{a}{10^n} = \frac{u_k \cdot 10^k + u_{k-1} \cdot 10^{k-1} + \cdots + u_1 \cdot 10 + u_0}{10^n}.$$

Note que aquí, k puede ser mayor, menor o igual que el natural n.

Veamos qué pasa cuando $k > n$

$$r = u_k \cdot \frac{10^k}{10^n} + u_{k-1} \cdot \frac{10^{k-1}}{10^n} + \cdots + u_n \cdot \frac{10^n}{10^n} + u_{n-1} \cdot \frac{10^{n-1}}{10^n} + \cdots + u_1 \cdot \frac{10}{10^n} + \frac{u_0}{10^n},$$

y utilizando las leyes de potencias se obtiene:

$$r = u_k \cdot 10^{k-n} + u_{k-1} \cdot 10^{k-n-1} + \cdots + u^n + u_{n-1} \cdot 10^{-1} + \cdots + u_1 \cdot 10^{1-n} + u_0 \cdot 10^{-n}.$$

Observemos que esta última expresión, tiene a primera vista el aspecto de un polinomio evaluado en $x = 10$. Sin embargo, una observación más atenta nos permite ver la presencia de potencias negativas de 10. En algunas ocaciones la expresión se denomina forma pseudo polinómica, para destacar el hecho que tiene una parte polinómica y otra que no lo es.
Esquemáticamente

$$r = \underbrace{\underbrace{u_k \cdot 10^{k-n} + u_{k-1} \cdot 10^{k-n-1} + \cdots + u_n}_{\text{parte polinómica}} + \underbrace{u_{n-1} \cdot 10^{-1} + \cdots + u_1 \cdot 10^{1-n} + u_0 \cdot 10^{-n}}_{\text{parte no polinómica}}}_{\text{forma pseudo-polinómica}}$$

Introducimos la notación

$$r = \frac{a}{10^n} = u_k u_{k-1} \ldots u_n \underbrace{,}_{\text{coma decimal}} u_{n-1} \ldots u_1 u_0$$

donde los coeficientes desde u_k a u_n son los coeficientes de la forma polinómica y los u_{n-1} hasta u_0 corresponden a la parte no polinómica.

Aquí hacemos la siguiente convención: introducimos el símbolo "," llamado la coma decimal, para separar los coeficientes de la forma polinómica, de los coeficientes de la forma no polinómica.

Con esta convención, resulta:

$$r = u_k u_{k-1} \dots u_n, u_{n-1} \dots u_1 u_0.$$

A las cifras $u_k, u_{k-1}, \dots, u_n$ las llamamos cifras enteras, y las cifras $\underbrace{u_{n-1} \dots u_1 u_0}_{n \text{ cifras}}$ las llamamos decimales, y la expresión

$$u_k u_{k-1} \dots u_n, u_{n-1} \dots u_1 u_0$$

se le llama la expansión decimal (o expresión racional) del racional r.

El razonamiento anterior se hizo para $k > n$; sin embargo, nada impide hacer el mismo razonamiento para $k = n$ y $k < n$. Para $k = n$, resultará una situación similar solamente que habrá una sola cifra entera, y para el caso $k < n$ podrá completarse la forma polinómica que expresa a con las potencias $10^n, 10^{n-1}, \dots, 10^{k+1}$, con coeficientes nulos.
Caso $k = n$:

$$\begin{aligned} r &= \frac{a}{10^n} = \frac{u_n \cdot 10^n + u_{n-1} \cdot 10^{n-1} + \dots + u_1 \cdot 10 + u_0}{10^n} \\ &= u_n + u_{n-1} \cdot 10^{-1} + \dots + u_1 \cdot 10^{1-n} + u_0 10^{-n}, \end{aligned}$$

así que la expresión decimal del raciona r resulta ser:

$$r = \frac{a}{10^n} = u_n, u_{n-1} \dots . u_1 u_0.$$

Caso $k < n$:

$$\begin{aligned} r &= \frac{a}{10^n} = \frac{u_k \cdot 10^k + u_{k-1} \cdot 10^{k-1} + \dots + u_1 \cdot 10 + u_0}{10^n} \\ &= \frac{0 \cdot 10^n + 0 \cdot 10^{n-1} + \dots + u_k 10^k + u_{k-1} 10^{k-1} + \dots + u_1 \cdot 10 + u_0}{10^n} \\ &= 0 \cdot 1 + 0 \cdot 10^{-1} + \dots + 0 \cdot 10^{k+1-n} + u_k \cdot 10^{k-n} + \dots + u_1 \cdot 10^{1-n} + u_0 10^{-n} \\ r &= \frac{a}{10^n} = 0, \underbrace{0 \dots 0}_{n-k-1 \text{ ceros}} u_k u_{k-1} \dots u_1 u_0. \end{aligned}$$

Todo lo anterior, puede resumirse en el siguiente resultado:

Teorema 6.1 *Todo número racional perteneciente a $\mathbb{Q}_d$, es decir toda fracción decimal, puede representarse por su expresión decimal separando mediante una coma decimal n cifras, contadas de derecha a izquierda, en la representación de a, completando con ceros si fuera necesario.*

Ejemplo 6.6.2 *Sea $r = \frac{19}{8}$. Claramente $8 = 2^3 \cdot 5^0$, y entonces $r \in \mathbb{Q}_d$. Luego*

$$r = \frac{19}{8} = \frac{19 \cdot 5^3}{2^3 \cdot 5^3} = \frac{2375}{10^3},$$

y la expresión decimal de r será:

$$r = \frac{19}{8} = 2,375.$$

Ejemplo 6.6.3 *Sea* $r = \frac{19}{200}$. *Observe que* $200 = 2^3 \cdot 5^2$, *y consecuentemente* $r \in \mathbb{Q}_d$. *Luego*

$$r = \frac{19}{200} = \frac{19}{2^3 \cdot 5^2} = \frac{19 \cdot 5}{2^3 \cdot 5^3} = \frac{95}{10^3}$$

y la expresión decimal de r será

$$\frac{19}{200} = 0,095.$$

Ejemplo 6.6.4 *Sea* $r = \frac{3}{1250}$. *Puesto que* $1250 = 2 \cdot 5^4$, *se tiene* $r \in \mathbb{Q}_d$. *Luego*

$$r = \frac{3}{2 \cdot 5^4} = \frac{3 \cdot 2^3}{2^4 \cdot 5^4} = \frac{24}{10^4} = 0,0024$$

Un comentario

La nominación *números decimales,* es una forma un tanto convencional para referirse a los números del conjunto $\mathbb{Q}_d$. Note que si, por ejemplo, escribimos $x = 23,148$ simplemente nos estamos refiriendo al número racional: $\frac{23148}{10^3}$. Veamos unos ejemplos adicionales.

Ejemplo 6.6.5 *Considere el racional* $\frac{1352}{625}$. *Determinar si este número pertenece al conjunto* $\mathbb{Q}_d$. *En caso afirmativo encuentre la expresión decimal.*
Note que: $625 = 5^4 \cdot 2^0$, *y por lo tanto* $\dfrac{1352}{625} \in \mathbb{Q}_d$. *Luego*

$$\frac{1352}{625} = \frac{1352}{5^4 \cdot 2^0} = \frac{1352 \cdot 2^4}{5^4 \cdot 2^4} = \frac{(1352)(16)}{(10)^4} = \frac{21632}{10^4},$$

y la expresión decimal será

$$\frac{1352}{325} = 2,1632.$$

Ejemplo 6.6.6 *Considere la expresión decimal* $x = 0,012$. *Escribir la fracción irreducible que tiene esa forma decimal*

$$0,012 = \frac{12}{10^3} = \frac{3}{250}.$$

6.6.4 De regreso al conjunto de los racionales $\mathbb{Q}_p$

Si volvemos la vista, por un momento, al conjunto de los racionales $\mathbb{Q}_d$, nos percatamos que cada racional $r \in \mathbb{Q}_d$ lo hemos podido expresar en forma decimal con un número finito de cifras decimales. Las pregunta natural es si esta propiedad seguirá siendo válida para los racionales pertenecientes a $\mathbb{Q}_p$. Desafortunadamente la respuesta es no.

En efecto, sea $r \in \mathbb{Q}_p$ y supongamos que lo podemos expresar con un número finito de cifras decimales. Es decir, supongamos que existen $u_k, u_{k-1}, ..., u_0$ tales que:

$$r = u_k u_{k-1} \dots u_n, u_{n-1} \dots u_1 u_0.$$

En tal caso se tiene

$$r = \frac{u_k u_{k-1} \dots u_n u_{n-1} \dots u_1 u_0}{10^n},$$

y resulta que $r \in \mathbb{Q}_d$. Pero esto es imposible, dado que $\mathbb{Q}_p \cap \mathbb{Q}_d = \emptyset$.
De esta forma, los racionales que pertenecen a $\mathbb{Q}_p$, en caso de tener una expresión decimal, ésta deberá contener un número infinito de cifras decimales.

6.6.5 Unas palabras sobre la división en $\mathbb{Q}$

Consideremos un racional $\frac{a}{b}$. Recordemos que este racional expresa el cociente entre los enteros a y b, con $b \neq 0$. Nuestro propósito será encontrar una expresión decimal para este cociente.
Para los enteros a y b sólo existen dos alternativas:

- a es múltiplo de b, ó
- a no es múltiplo de b.

Si ocurre lo primero, es decir si a es un múltiplo de b, existe un entero q tal que:

$$a = b \cdot q,$$

y por lo tanto

$$\frac{a}{b} = q = \frac{q}{10^0},$$

resultando que $\frac{a}{b} \in \mathbb{Q}_d$.
Si ocurre la segunda alternativa, es decir si a no es múltiplo de b, por el algoritmo de la división existen q y r enteros únicos, tales que

$$a = bq + r, \text{ con } 0 \leq r < b.$$

¿Que hacer en caso de que a no sea múltiplo de b?
Un posible camino, es intentar dividir r por b, pero como $r < b$, al efectuar esta división se obtiene cociente igual a cero y resto igual a r, lo que no conducirá a ningún lado.
Vamos a introducir lo que se llama el primer paso de la división decimal de a por b. Este procedimiento consiste en dividir el resto de la división, previamente multiplicando po 10, por el denominador b.
Entonces, para $10 \cdot r$ y b hay dos alternativas:

- $10 \cdot r$ es múltiplo de b

- $10 \cdot r$ no es múltiplo de b

Si se da la primera alternativa, existe $q_1 \in \mathbb{Z}$ tal que:

$$10r = q_1 b,$$

y en este caso $r = b \cdot \frac{q_1}{10}$, y remplazando se obtiene:

$$a = bq + r = bq + b \cdot \frac{q_1}{10} = b\left(q + \frac{q_1}{10}\right).$$

Es decir

$$\frac{a}{b} = q + \frac{q_1}{10}.$$

En este caso, $\frac{a}{b}$ es una fracción decimal y en consecuencia $\frac{a}{b} \in \mathbb{Q}_d$. Además, la expresión decimal será

$$\frac{a}{b} = q, q_1.$$

En caso de darse la segunda alternativa, es decir que $10r$ no sea múltiplo de b, existen $q_1 \in \mathbb{Z}$ y $r_1 \in \mathbb{Z}$ tales que:

$$10r = bq_1 + r_1,\ 0 < r_1 < b.$$

Note que $0 \leq q_1 \leq 9$, y se tiene:

$$r = b \cdot \frac{q_1}{10} + \frac{r_1}{10}.$$

Reemplazando en la expresión para a, se tiene:

$$\begin{aligned} a &= bq + b \cdot \frac{q_1}{10} + \frac{r_1}{10} = b\left(q + \frac{q_1}{10}\right) + \frac{r_1}{10} \\ \frac{a}{b} &= q + \frac{q_1}{10} + \frac{r_1}{10b} = q, q_1 + \frac{r_1}{10b} \end{aligned}$$

y a partir de aquí reiteramos el procedimiento anterior que es lo que se llama comnúmente segundo paso de la división decimal de a por b. Es decir, vamos a dividir $10r_1$ por b.

Nuevamente, para $10r_1$ y b, existen dos alternativas:

- $10r_1$ es múltiplo de b,
- $10r_1$ no es múltiplo de b.

Si ocurre la primera alternativa, es decir si $10r_1$ es múltiplo de b, se tiene que:

$$10r_1 = q_2 b,$$

lo que implica que $r_1 = b \cdot \frac{q_2}{10}$ y se obtiene:

$$\frac{a}{b} = q + \frac{q_1}{10} + \frac{q_2}{10^2} = q, q_1 q_2$$

Note que $0 \leq q_2 \leq 9$.
Si lo que se da es la segunda alternativa, es decir si $10r_1$ no es múltiplo de b, se tiene que existen $q_2 \in \mathbb{Z}$ y $r_2 \in \mathbb{Z}$ tales que

$$10r_1 = bq_2 + r_2,\ 0 < r_2 < b.$$

Luego:

$$r_1 = b \cdot \frac{q_2}{10} + \frac{r_2}{10},$$

y remplazando:

$$\frac{a}{b} = q + \frac{q_1}{10} + \frac{q_2}{10^2} + \frac{r_2}{10^2 b}.$$

Antes de seguir reiterando los pasos de la división decimal, vamos a tratar de sacar algunas conclusiones.
Después de todo esto, uno podrá preguntarse: ¿ Qué es la división decimal en $\mathbb{Q}$?
Para nosotros, división decimal en $\mathbb{Q}$ es el procedimiento que se puede aplicar a todo racional $\frac{a}{b}$ y que se reduce a dividir a por b y sucesivamente los restos no nulos, previamente multiplicados por 10. Vamos a decir que los cocientes $q_1, q_2, ...$ que se obtienen en las diferentes etapas de la división decimal de a po b, así como los restos $r_1, r_2, ...$, se denominan cocientes y restos decimales parciales.
En el paso n-ésimo de la división decimal de a por b, se presentan dos alternativas posibles:

- $10r_{n-1}$ es múltiplo de b, ó
- $10r_{n-1}$ no es múltiplo de b.

Supongamos que se da el primer caso; es decir el resto $r_n = 0$. Entonces, el racional $\frac{a}{b} \in \mathbb{Q}_d$.
En efecto, razonando de manera análoga al paso uno y al paso dos, se tiene:

$$a = b\left(\underbrace{q, q_1 q_2 ... q_n}_{\text{n cifras}}\right)$$

lo que implica que

$$\frac{a}{b} = q, q_1 q_2 \ldots q_n$$

y entonces $\frac{a}{b} \in \mathbb{Q}_d$. Por lo tanto, podemos afirmar:
Si la división decimal de a por b, tiene un número finito de pasos, o sea si finaliza al obtener un resto nulo a los n pasos, entonces $\frac{a}{b}$ es una fracción decimal y puede expresarse en forma decimal de la manera siguiente: su parte entera es el cociente entre a y b y las cifras decimales son los sucesivos cocientes parciales obtenidos en los n pasos de la división decimal.

Ejemplo 6.6.7 *Consideremos el racional* $\frac{4357}{125}$. *Tenemos*

$$4357 = 125 \cdot 34 + 107,$$

así que $a = 4357$, $b = 125$, $q = 34$ *y* $r = 107$. *Primer paso de la división decimal:*

$$10r = 1070 = 125 \cdot 8 + 70,$$

de donde $q_1 = 8$ *y* $r_1 = 70$. *Segundo paso de la división decimal:*

$$10r_1 = 700 = 125 \cdot 5 + 75,$$

y entonces $q_2 = 5$, $r_2 = 75$. *Tercer paso de la división decimal:*

$$10r_2 = 750 = 125 \cdot 6 + 0,$$

y obtenemos $q_3 = 6$, $r_3 = 0$. *Obtenemos, entonces, que:*

$$\frac{4357}{125} = 34,856 = \frac{34856}{10^3}, \text{ y consecuentemente } \frac{4357}{125} \in \mathbb{Q}_d.$$

Este procedimiento que acabamos de realizar, ¿No le recuerda la escuela? Claro! Se trata del conocido mecanismo de bajar ceros que nos enseñó la niña.

		$\lfloor b$
a		
r	$\times 10$	$q, q_1 q_{2\ldots}$
r_1	$\times 10$	
r_2	$\times 10$	
r_3	$\times 10$	

Ahora, resulta totalmente natural preguntarse ¿Puede la división decimal de a por b tener un número infinito de pasos? Es decir ¿Puede darse el caso en que esta división no termine? Para tener idea del problema, consideramos el racional $\frac{1}{3}$. Observe que esta división no termina pues en cada paso, se obtiene un resto igual a 1. Sin embargo, números racionales como $\frac{1}{3}$ tienen la propiedad de que los cocientes parciales son todos iguales a tres. Es decir, hay una cantidad infinita de cocientes parciales, pero estos se repiten periódicamente.
Ahora: ¿Será cierto que una división decimal infinita los cocientes parciales se repiten con alguna periodicidad?
Veremos a continuación que, afortunadamente, la respuesta es afirmativa.
Consideremos las siguientes desigualdades:

$$\begin{aligned} a &= bq + r \text{ ; con } 0 < r < b \\ 10r &= bq_1 + r_1 \text{ ; con } 0 < r_1 < b \\ 10r_1 &= bq_2 + r_2 \text{ ; con } 0 < r_2 < b \\ \vdots &\quad \vdots \qquad\qquad\qquad \vdots \end{aligned}$$

Todos los restos parciales son mayores que 0 pero menores que el denominador b.
Por lo tanto, si efectuamos la división de manera indefinida, los restos:

$$r_1, r_2, \ldots, r_n, \ldots$$

deben ser positivos y menores que b.

$$0 < r_i < b, \text{ con } i = 1, 2, 3, ...$$

Sin embargo existen $b-1$ enteros positivos menores que b (los números comprendidos entre 1 y $b-1$); es decir, los r_i tienen un número finito de valores posibles a tomar y como hay un número infinito de restos, necesariamente estos restos deben repetirse a partir de cierto momento. Supongamos, por ejemplo, que el resto del paso n; denotado por r_n, es el mismo que el del paso k anterior a n; es decir $r_n = r_k$.
De aquí resulta que:

$$q_{n+1} = q_{k+1},$$

y los cocientes parciales comienzan a repetirse a partir de q_{n+1}, y esto origina un período cuyas cifras son los cocientes parciales q_{k+1} desde hasta q_n. En tal caso se denota:

$$\frac{a}{b} = q, q_1 ... q_k \overline{q_{k+1} \ldots q_n}$$

Desde luego que, el cociente q_{k+1}(primera cifra del período) puede coincidir con q_1 si el resto que se repite coincide con r. En este caso, el período de los cocientes parciales comienza inmediatamente después de la coma decimal.
Resumimos:

> Si la división de a por b da un número infinito de cocientes parciales, estos necesariamente se repiten de manera periódica. El período puede comenzar inmediatamente después de la *coma decimal,* o luego de un número finito de cifras.

Ejemplo 6.6.8 *Considere el racional* $\frac{23}{27}$*, dividiendo:*

$$\begin{array}{rl|l} 23 & & 27 \\ \cline{3-3} 23 & \times 10 & 0,851 \\ 14 & \times 10 & \\ 5 & \times 10 & \\ 23 & & \end{array}$$

Como $r_3 = r$*, resulta que* $q_4 = q_1$*, de donde resulta que el cociente parcial siguiente valdrá* 8*, y* 851 *será el período. Notación* $\frac{23}{27} = 0, \overline{851}$*, lo cual significa que:* $\frac{23}{27} = 0,851851851\ldots$.

Ejemplo 6.6.9 *Considere ahora el racional* $\frac{4177}{33300}$. *Efectuando la división decimal, se tiene:*

$$\begin{array}{rl} 4177 & \big| \; 33300 \\ \cline{2-2} 4177 \times 10 & 0,12543 \\ 8470 \times 10 & \\ 18100 \times 10 & \\ 14500 \times 10 & \\ 11800 \times 10 & \\ 18100 & \end{array}$$

Claramente, $r_2 = r_5$ y consecuentemente $q_6 = q_3$, o sea $q_6 = 5$ y el período resulta ser: 543, siendo la parte no periódica las cifras $1, 2$, las cuales dicho sea de paso no volverán a aparecer como cocientes parciales. Así:

$$\frac{4177}{33300} = 0,12\overline{543}.$$

Cuando el período comienza inmediatamente después de la *coma decimal*, se llama forma periódica pura, y a las otras se les llama formas periódicas mixtas.

6.6.6 Ejercicios

1. Halle las expansiones decimales de $\frac{3}{5}$, $\frac{9}{11}$, $\frac{129}{7}$, $\frac{1234}{9999}$, $\frac{37}{90}$, $\frac{1}{31}$, $\frac{1}{37}$, $\frac{1}{49}$.

2. En cada caso, halle el número racional correspondiente a la expansión decimal dada:

   0.00001111, 4.323232, $4.\overline{32}$, $-1.\overline{9}$, 0.6667, $0.\overline{6}$, $0.\overline{123456789}$, $0.\overline{1232345}$

3. Demuestre que si $a \in \mathbb{Q}$ tiene expansión decimal $q, a_1 a_2 \ldots$, entonces para cada $n \in \mathbb{N}$ se tiene

   $$q + \frac{a_1}{10} + \ldots + \frac{a_n}{10^n} \leq a < q + \frac{a_1}{10} + \ldots + \frac{a_n}{10^n} + \frac{1}{10^n}.$$

4. Halle la expansión decimal de

   $$\frac{10^{n+1} - 1}{9 \cdot 10^n} = \frac{\left(\frac{1}{10}\right)^{n+1} - 1}{\frac{1}{10} - 1}.$$

   Recuerde que:

   $$1 + r + \ldots + r^n = \frac{r^{n+1} - 1}{r - 1}.$$

5. Si r es un racional positivo, demuestre que existe $n \in \mathbb{N}$ tal que $\frac{1}{n} < r$.

6. Para todo racional x, $[\![x]\!]$ denota su parte entera

(a) Demostrar que $[\![x+y]\!] \geq [\![x]\!] + [\![y]\!]$
¿que podemos decir de la diferencia? $[\![x+y]\!] - ([\![x]\!] + [\![y]\!])$

(b) Demostrar que $[\![x-y]\!] \leq [\![x]\!] - [\![y]\!]$

¿que podemos decir de la diferencia? $[\![x]\!] - [\![y]\!] - [\![x-y]\!]$

(c) Sea $n \in \mathbb{N}^*$. Demostrar que

$$\left[\!\left[\frac{[\![nx]\!]}{n} \right]\!\right] = [\![x]\!], \quad \text{y} \quad \sum_{n=0}^{n-1} \left[\!\left[x + \tfrac{k}{n} \right]\!\right] = [\![nx]\!].$$

7. ¿Cuáles de los siguientes números racionales son decimales?

$$\frac{17}{675}, \quad \frac{5}{160}, \quad \frac{12}{425}, \quad \frac{1}{4700}, \quad \frac{3}{10240}, \quad \frac{21}{150}.$$

8. Determinar los $n \in \mathbb{N}$ tales que $\frac{17n}{6}$ sea un número decimal.

9. Sean x , y números racionales que satisfacen la ecuación: $x + y = \frac{1}{4}$. Demostrar que x e y son números decimales.

10. Sean a , b , c , d , e , f números b-ádicos. Encontrar una condición necesaria y suficiente para que los racionales x, y que satisfacen las ecuaciones: $ax + by = e$ y $cx + dy = f$ sean números b-ádicos.

11. Encontrar los números k para los cuales existen dos cifras, a y b , tales que la suma de los numeros racionales reprensetados, en numeración decimal, por " a, b " y " b, a " sea k .

12. Comparar estos dos números racionales: $4 + \frac{2}{18} + \frac{15}{18^2} + \frac{3}{18^3}$ y $4 + \frac{1}{6} + \frac{1}{18^3}$

13. Determinar los números racionales reprensetados por la fracción de denominador positivo menor que 10 y cuya aproximación decimal de orden 1 es 3,4.

14. Sea $x \in \mathbb{Q}$ tal que $0 \leq x \leq 1$ y sea $y = 1 - x$.

(a) Demuestre que si x no es un número decimal, entonces y tampoco es un número decimal.
Sea $\frac{a_n}{10^n}$ la aproximación decimal de orden n de x . ¿Cuál es la aproximacion decimal de orden n de y ?
Demostrar que la suma de dos cifras del mismo rango en la reprensetación decimal de x e y es 9.

(b) Si x es un númera decimal. ¿Como se modifican los resultados de la pregunta anterior?

15. Sea b un entero mayor que 2.

    (a) Sea a un entero tal que $0 < a < b - 1$. Encontrar la representación ilimitada, en base b, del número racional $\frac{a}{b-1}$.
    Use el resultado anterior para encontrar la expansión decimal (repesentación ilimitada en base 10) del racional $\frac{5}{9}$.

    (b) Sea $\alpha \in \mathbb{N}^*$. ¿Cómo se pasa del desarrollo ilimitado de un número racional en base b^α a su desarrollo ilimitado en base b ?

    (c) Sean a y a' dos enteros tales que $0 \leq a \leq b - 1$ y $0 \leq a' \leq b - 1$; sea x el entero representado en base b por aa'. Encontrar la representación ilimitada (desarrollo ilimitado) en base b del número $\frac{x}{b^2-1}$.
    Sugerencia: $\frac{1}{b^2-1} = \frac{1}{b^2(1-\frac{1}{b^2})} = \frac{1}{b^2} \cdot \frac{1}{1-\frac{1}{b^2}}$ y utilice el hecho de que

    $$\frac{1}{1-t^2} = 1 + t^2 + t^4 + t^6 \ldots$$

    (d) Generalice el resultado de la pregunta c) y use la generalización para encontrar la expansión decimal (desarrollo ilimitado en base 10) del racional $\frac{4512}{9999}$.

16. Sea r un número racional cuya representación canónica está dada por: $\frac{a}{d_1 d_2}$, donde d_1 y d_2 son mayores que 1 y primos relativos.

    (a) Demostrar que existen enteros p y q tales que: $\frac{a}{d_1 d_2} = \frac{p}{d_1} + \frac{q}{d_2}$.

    (b) Demostrar que existe una infinidad de tales descomposiciones.

    (c) Demostrar que existen enteros e, v_1, v_2 tales que: $\frac{a}{d_1 d_2} = e + \frac{v_1}{d_1} + \frac{v_2}{d_2}$, con $0 < v_1 < d_1$ y $0 < v_2 < d_2$.

    (d) Demostrar que e es único, luego que v_1 y v_2 también son únicos.

    (e) Efectuar esta descomposición para $a = 11, d_1 = 2, d_2 = 3$.

17. Sea $\frac{a}{d_1 d_2 \ldots d_n}$ la representación canónica de un racional dado, donde los d_i son mayores que 1 y primos relativos dos a dos. Demostrar que existen enteros $e, v_1, v_2, \ldots, v_n$ únicos tales que: $\frac{a}{d_1 d_2 \ldots d_n} = e + \frac{v_1}{d_1} + \frac{v_2}{d_2} + \ldots + \frac{v_n}{d_n}, 0 < v_1 < d_1, 0 < v_2 < d_2, \ldots, 0 < v_n < d_n$.

18. Demuestre que todo número b-ádico positivo y menor que 1, es igual a la suma de números b-ádicos de la forma $\frac{a}{b^k}$ con $k > 0$ y $0 < a < b$. Demostrar que esta descomposición es única.

19. Demostrar que todo número racional es la suma de un entero y números de la forma $\frac{a}{p^k}$, donde p es primo, $0 < a < p$ *y* k es entero positivo. Demostrar que esta descomposición es única. Efectuar esta descomposición para el racional $\frac{36}{45}$.

20. Sea a y b dos números naturales.

(a) Para x un natural cualquiera, comparar los números racionales $\frac{a}{b}$ y $\frac{a+x}{b+x}$.

(b) Demostrar que para todo racional positivo h, existe un entero N tal que $x >$

$$N \Rightarrow \left| \frac{a+x}{b+x} - 1 \right| < h$$

21. Sea x un racional no nulo. Encontrar los números racionales y tales que $x \cdot y$ y $\frac{\frac{1}{y}}{x}$ sean enteros.

22. Sean a, b, c, d enteros naturales tales que $a < b < c$ y $\frac{a}{b} = \frac{c}{d}$.

    (a) Comparar c y d.

    (b) Comparar $a + d$ y $b + c$.

23. Encontrar los número naturales n tales que $\frac{12n+96}{n+4}$ sea un entero.

24. Sea a, b, c enteros positivos. Demostrar que si $|b - ac| \geq c$, existe al menos un natural n tal que $\frac{an+b}{n+c}$ es entero.

25. Demostrar que cualesquiera que sean a, b, c existen al menos dos naturales n tales que $\frac{an+b}{n-c}$ es entero. ¿Bajo qué condición se puede afirmar que existee únicamente dos?

26. Sea $n \in \mathbb{N}$ encontrar expresiones simples para las sumas:

$$S_n = \sum_{p=1}^{n} \frac{1}{p\,(p+1)}, \quad T_n = \sum_{p=1}^{n} \frac{1}{p\,(p+2)}.$$

    Denotando $E = \{S_n : n \in \mathbb{N}\}$, $F = \{T_n : n \in \mathbb{N}\}$, demostrar que E y F son dos subconjuntos acotados superiormente de $\mathbb{Q}$.

27. Sean a y b enteros que satisfacen $0 < a < b$. Demostrar que existe un entero positivo q, único, tal que : $\frac{1}{q+1} < \frac{a}{b} \leq \frac{1}{q}$, y que $\frac{a}{b} - \frac{1}{q+1}$ se escribe en la forma $\frac{u}{v}$, con u y v enteros positivos que verifican $u < a$ y $v > b$.

28. Sean n y k enteros positivos, escribir el número racional $\frac{n}{n!(k+1)}$ como la diferencia de dos racionales representados por fracciones de numerador 1.

29. Demostrar que todo número racional positivo es la suma de un número natural y un número finito de racionales positivos representedos por fracciones de numerador 1. Escriba bajo esta forma el racional $\frac{31}{18}$.

30. Dados dos naturales n y k, demostrar que $\frac{n}{n!(k+1)}$ es la suma de n racionales representados por fracciones de numerador 1 y denominador de la forma $p!(k_p + 1)$, donde $0 \leq p \leq n-1$ y los k_p son enteros positivos. Demostrar que si $p < p'$ entonces k_p divide a $k_{p'}$

31. Comprobar que cada uno de los siguientes números es un racional:
    a) $r = \sqrt[3]{20 + 14\sqrt{2}} + \sqrt[3]{20 - 14\sqrt{2}}$.
    b) $r = \sqrt{2}\left(\sqrt[4]{7 + 4\sqrt{3}} - \sqrt[4]{7 - 4\sqrt{3}}\right)$

Capítulo 7

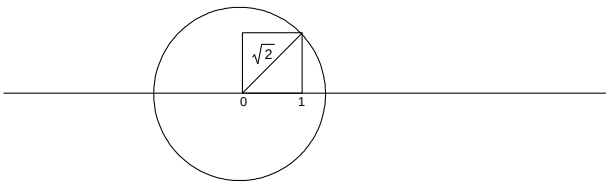
El paso de los racionales a los reales

El lector probablemente esté familiarizado con el conjunto de números reales como campo totalmente ordenado, y posiblemente su estudio de este sistema numérico haya sido hasta el momento axiomático. Es importante tener claro que mientras no se hable de *completitud*, no podemos realmente diferenciar los campos ordenados $\mathbb{Q}$ y $\mathbb{R}$. Es decir, las propiedades algebraicas y de orden, o axiomas de campo y de orden, que se enuncian comúnmente, son satisfechas tanto por el conjunto de los racionales como por el de los reales. Nuestro primer objetivo en el presente capítulo es entender qué significa la completitud, y cómo hacer para expresarla de una manera analítica.

7.1 Incompletitud de $\mathbb{Q}$

7.1.1 Incompletitud geométrica

Tal vez el hecho más conocido de la incompletitud de los números racionales, es su incapacidad para "llenar" la recta numérica, como lo demuestra el teorema de pitágoras. Tomemos por ejemplo un cuadrado de lado 1. Si los números racionales han de servir para representar la medida de cualquier segmento de recta, la medida de la diagonal debería ser cierto racional r, y por el teorema de pitágoras se tendría $r^2 = 1^2 + 1^2 = 2$. Sin embargo, el lema 6.3.1 demuestra que no existe tal r.
Esto demuestra que efectivamente hay puntos sobre la recta numérica que no corresponden a números racionales.



El mismo argumento demuestra el siguiente lema.

Lema 7.1.1 *Si $n \in \mathbb{N}$ no es cuadrado perfecto, entonces no existe $r \in \mathbb{Q}$ tal que $r^2 = n$.*

Prueba
Suponga que sí existe tal r, y tomemos su representación canónica $r = \dfrac{a}{b}$. Tenemos entonces que a y b son primos relativos, y por el ejercicio 6 del capítulo anterior se sigue que a^2 y b^2 lo son. Dado que $a^2 = nb^2$, se sigue que $\left(a^2, b^2\right) = b^2$, de donde $b = 1$. Pero entonces r sería natural, lo que contradice la hipótesis. □

7.1.2 Otras evidencias de la incompletitud de los racionales

Con el estudio de las expansiones de números racionales, se demuestra que todo número racional tiene una expansión decimal de la forma

$$a_0, a_1 a_2 \ldots a_n \ldots \tag{7.1}$$

donde a_0 es un número entero y $a_n \in \{0, 1, \ldots, 9\}$ para cada $n \geq 1$.
Surge aquí la pregunta: ¿Será cierto que toda expresión de este tipo tiene asociado un número racional? La respuesta es negativa, dado que la expansión de un racional es siempre periódica. Por ejemplo:

$$\begin{aligned} \tfrac{5}{3} &= 1,666\ldots = 1,\overline{6} \\ \tfrac{1}{7} &= 0,\ 142\,857\,142\,857\ldots = 0,\ \overline{142\,857} \end{aligned}$$

En general, si $r \in \mathbb{Q}$ tiene expansión $a_0, a_1 a_2 \ldots$, entonces existen $n, p \in \mathbb{N}$ tales que $a_{k+p} = a_k$ para todo $k \geq n$.
Como consecuencia, existen muchas expansiones que no corresponden a números racionales. Por ejemplo:

$$0,10100100010000100000\ldots$$

En esta expansión aparece un *"uno"* seguido de cierta cantidad de ceros que se va incrementando sucesivamente, y consecuentemente no es periódica. Otro ejemplo lo podemos obtener si definimos $a_0 = 0$, $a_n = 3$ para n primo, y $a_n = 5$ en los demás casos. Obtenemos una expansión que comienza así:

$$0,5335335553535553535\ldots$$

De hecho, esto sugiere una manera de definir los números reales, como expresiones formales del tipo (7.1).

7.1.3 Versión analítica de la incompletitud de $\mathbb{Q}$

Pensemos en un punto P sobre la recta "numérica". Es intuitivamente claro que este punto determina dos conjuntos de racionales: El conjunto A de racionales que se ubican a la izquierda de P, y el conjunto B de los que se ubican a la derecha. Tales conjuntos satisfacen:

$$\text{Para cada } x \in A \text{ y cada } y \in B \text{ se tiene } x \leq y. \qquad (A \text{ y } B \text{ adyacentes})$$

Ejemplo 7.1.1 *Si P es el punto que corresponde al número* 3, *se obtiene:*

$$A = \{x \in \mathbb{Q} : x < 3\} \ y \ \ B = \{x \in \mathbb{Q} : x > 3\}$$

Ejemplo 7.1.2 *Si P es el conjunto que corresponde a la diagonal de un cuadrado de lado* 1, *entonces*

$$A = \mathbb{Q}^- \cup \{x \in \mathbb{Q}^+ : x^2 < 2\}, \qquad B = \{x \in \mathbb{Q}^+ : x^2 > 2\}.$$

En el primer ejemplo, existe un racional $r = 3$ tal que $x \leq 3 \leq y$ para cada $x \in A$ y cada $y \in B$. En el segundo caso, no existe tal r, pues de existir no sería difícil demostrar que $r^2 = 2$, y esto es imposible como se ha demostrado. La diferencia entre $\mathbb{Q}$ y $\mathbb{R}$ radica, específicamente, en que en $\mathbb{R}$ siempre es posible hallar un α tal que $x \leq \alpha \leq y$ para cada $x \in A$ y cada $y \in B$.

7.2 Axiomatización de los números reales

Las ideas de la sección anterior nos convencen de que es posible efectuar la construcción de $\mathbb{R}$ a partir de $\mathbb{Q}$, y nos muestran cómo la intuición geométrica ayuda a elaborar conceptos de una manera rigurosa. Una construcción detallada de $\mathbb{R}$ apartir de $\mathbb{Q}$ se hace en los anexos.

En lo que sigue, se hará una presentación axiomática del conjunto de los números reales. Asumiremos la existencia de un conjunto, cuyos elementos llamamos números reales. Suponemos, además, que este conjunto está dotado de dos operaciones internas -una suma y una multiplicación- y de una relación de orden " $\leq$ "; que cumplen con tres grupos de axiomas que describiremos a continuación.

1. Axiomas de campo,
2. Axiomas de orden,
3. Axiomas de completitud o axioma del extremo superior.

7.2.1 Axiomas de campo

Las operaciones suma y multiplicación cumplen los siguientes axiomas:

Axioma 7.2.1 *La operación suma es cerrada. Es decir, para $a, b \in \mathbb{R}$ se tiene $a + b \in \mathbb{R}$. Esta propiedad nos garantiza que*

$$\begin{array}{rcl} + : \mathbb{R} \times \mathbb{R} & \rightarrow & \mathbb{R} \\ (a, b) & \rightarrow & a + b \end{array}$$

Axioma 7.2.2 *Para todos a, $b \in \mathbb{R}$, se cumple: $a + b = b + a$.*
Esta propiedad se llama conmutatividad de la suma.

Axioma 7.2.3 *Para todos a, b, c en $\mathbb{R}$, se cumple:*

$$a + (b + c) = (a + b) + c.$$

Esta propiedad se conoce como la asociatividad de la suma.

Axioma 7.2.4 *Existe $0 \in \mathbb{R}$ tal que*

$$a + 0 = 0 + a = a, \ \forall a \in \mathbb{R}.$$

Esta propiedad se le conoce como la existencia del neutro aditivo.

Axioma 7.2.5 *Para todo $a \in \mathbb{R}$, existe $-a \in \mathbb{R}$ tal que*

$$a + (-a) = (-a) + a = 0.$$

El elemento $-a$ se llama el inverso aditivo de a.

Axioma 7.2.6 *La multiplicación es cerrada. Es decir, para $a, b \in \mathbb{R}$ se tiene $a \cdot b \in \mathbb{R}$. Esta propiedad nos garantiza que*

$$\begin{array}{rcl} \cdot : \mathbb{R} \times \mathbb{R} & \rightarrow & \mathbb{R} \\ (a, b) & \rightarrow & a \cdot b \end{array}$$

Axioma 7.2.7 *Para todos $a, b \in \mathbb{R}$, se tiene que*

$$a \cdot b = b \cdot a.$$

Esta propiedad se llama la conmutatividad del producto o multiplicación.

Axioma 7.2.8 *Para todos a, b y c en $\mathbb{R}$, se tiene que*

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

Propiedad que se conoce con el nombre de asociatividad del producto.

Axioma 7.2.9 *Existe $1 \in \mathbb{R}$, $1 \neq 0$, tal que*

$$1 \cdot a = a \cdot 1 = a, \ \forall a \in \mathbb{R}.$$

Esta se conoce como la existencia del neutro multiplicativo. El hecho de que $1 \neq 0$ nos garantiza $\mathbb{R} \neq \{0\}$.

Axioma 7.2.10 *Para todo $a \in \mathbb{R}$, $a \neq 0$, existe $a^{-1} \in \mathbb{R}$ tal que*

$$a \cdot a^{-1} = a^{-1} \cdot a = 1.$$

Esta propiedad se conoce como la existencia del inverso multiplicativo para los números reales diferentes del 0.

Axioma 7.2.11 *Para todos a, b, c en $\mathbb{R}$, se cumple:*

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

Esta es la propiedad de distributividad de la multiplicación con respecto a la suma.

De los axiomas de campo que acabamos de enunciar, se pueden deducir todas las "leyes usuales" del algebra elemental de números reales. A continuación, se enuncian estas leyes y se demuestran algunas de ellas.

Teorema 7.1 *Los elementos 0 y 1 son únicos. Es decir, 0 es el único neutro de la suma, y 1 es el único neutro de la multiplicación.*

Demostración
Demostraremos la unicidad del cero, y dejamos la del uno como ejercicio. Supongamos que $0' \in \mathbb{R}$ es otro neutro de la suma, lo cual quiere decir que $a + 0' = a$ para todo $a \in \mathbb{R}$. Entonces tenemos

$$\begin{array}{rcll} 0' & = & 0+0' & \text{(por ser 0 un neutro)} \\ & = & 0 & \text{(por ser } 0' \text{ un neutro). } \square \end{array}$$

Teorema 7.2 *(Ley de cancelación de la suma) Sean a, b y c números reales cualesquiera. Si $a + c = b + c$, entonces $a = b$.*

Demostración
Si $a + c = b + c$, sumando el inverso aditivo de a en ambos lados de la igualdad, se tiene

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

de donde por la asociatividad de la suma resulta

$$a+(c+(-c)) = b+(c+(-c))\,.$$

Es decir $a + 0 = b + 0$, y el resultado se sigue por el axioma 7.2.4. $\square$

El argumento anterior se puede resumir como sigue:

$$a = a+0 = (a+c)+(-c) = (b+c)+(-c) = b+0 = b.$$

El lector puede demostrar en forma similar la ley de cancelación de la multiplicación.

Teorema 7.3 *(Ley de cancelación de la multiplicación) Sean a, b y c números reales cualesquiera, con $c \neq 0$. Si $a \cdot c = b \cdot c$, entonces $a = b$.*

Puede ilustrar en un ejemplo que la hipótesis c es imprescindible.

Teorema 7.4 *Sean $a, b \in \mathbb{R}$. Entonces existe un único $x \in \mathbb{R}$ tal que $x + a = b$. En particular, el inverso de a es único.*

Demostración
Tomando $x = b + (-a)$ se tiene

$$x + a = b + (-a) + a = b + 0 = b.$$

Para la unicidad, supongamos que existe otro número real x' que también cumple: $x' + a = b$. Entonces $x' + a = x + a$, y por la ley de cancelación de la suma se sigue que $x' = x$. Finalmente, aplicando esto con $b = 0$ se tiene que existe un único x tal que $x + a = 0$, demostrando la unicidad del inverso de a. □

Teorema 7.5 *Sean $a, b \in \mathbb{R}$, con $a \neq 0$. Entonces existe un único número real y tal que $ay = b$. En particular, el recíproco de a es único.*

Demostración
En efecto, basta tomar $y = b \cdot a^{-1}$. Los detalles son análogos del teorema anterior, y se dejan de ejercicio. □

Teorema 7.6 *Para todo $a \in \mathbb{R}$ se tiene $-(-a) = a$. Además, si $a, b \in \mathbb{R}$ tenemos*

$$-(a + b) = (-a) + (-b).$$

Demostración
Note que $-(-a)$ significa *el inverso aditivo de* $-a$. Como $-a + a = 0$, la unicidad del inverso aditivo de $-a$ demuestra que $a = -(-a)$.
Para la segunda parte, observe que por la asociatividad y conmutatividad se tiene

$$((-a) + (-b)) + (a + b) = -a + (-b + b) + a = -a + a = 0,$$

y por la unicidad del inverso se tiene que $(-a) + (-b) = -(a + b)$. □

Similarmente se demuestra el siguiente teorema.

Teorema 7.7 *Para todo $a \neq 0$ se tiene $\left(a^{-1}\right)^{-1} = a$. Además, si $a \neq 0 \neq b$ entonces*

$$(ab)^{-1} = a^{-1}b^{-1}.$$

Teorema 7.8 *(Propiedad absorvente del cero) Para todo $a \in \mathbb{R}$, $a \cdot 0 = 0 \cdot a = 0$.*

Demostración
Sabemos que $0 + 1 = 1$, y entonces

$$a = a \cdot 1 = a(0 + 1) = a \cdot 0 + a \cdot 1 = a \cdot 0 + a,$$

y por la ley de cancelación de la suma resulta $a \cdot 0 = 0$. □

Teorema 7.9 *Sean a y b dos números reales. Entoces $a \cdot b = 0$ sii $a = 0$ ó $b = 0$*

Demostración
Si $a = 0$ o $b = 0$, por la absorvencia del cero se obtiene $a \cdot b = 0$.

Recíprocamente, supongamos que $a \cdot b = 0$ y demostremos que $a = 0$ ó $b = 0$. Si $a = 0$ no hay nada que demostrar. Si $a \neq 0$, por la ley de cancelación del producto se obtiene $b = 0$. □

La propiedad anterior indica que en $\mathbb{R}$ no existen divisores de cero. Por otro lado, note que como una consecuencia inmediata de la propiedad anterior, se obtiene el siguiente resultado:

$$\text{Si } a, b \in \mathbb{R}, \text{ entonces } a \neq 0 \neq b \Leftrightarrow ab \neq 0.$$

El siguiente resultado es una manera de escribir la ley de signos.

Teorema 7.10 *Sean $a, b \in \mathbb{R}$. Entonces:*

$$(\ i\ )\ a(-b) = -(ab)$$

$$(\ ii\ )\ (-a)b = -(ab)$$

$$(\ iii\ )\ (-a)(-b) = ab$$

Demostración
Vamos a demostrar la parte (i). Las partes (ii) y (iii), se dejan como ejercicio para el lector. Tenemos

$$a(-b) + ab = a[(-b) + b] = a \cdot 0 = 0.$$

Es decir, el número $a(-b)$ también es el inverso aditivo de ab, y por la unicidad $a(-b) = -(ab)$, y esto es lo que se quería demostrar. □

Como consecuancia de la ley de los signos, es inmediato que $(-1) \cdot a = -a$. En efecto,

$$(-1) \cdot a = -(1 \cdot a) = -a.$$

7.2.2 Cálculo de cocientes

Si a y b son números reales, $b \neq 0$, entonces el número ab^{-1} lo escribimos como $\dfrac{a}{b}$, y a este número real lo llamamos el cociente de a por b. Note que:

$$\frac{a}{1} = a. \qquad \text{Si } a \neq 0, \text{ entonces } \frac{a}{a} = 1.$$

Teorema 7.11 *Sean a, b, c y d números reales, $b \neq 0$ y $d \neq 0$, entonces*

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \qquad \frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd}.$$

Demostración

$$\begin{aligned}\frac{a}{b}\cdot\frac{c}{d} &= (ab^{-1})\cdot(cd^{-1})\\ &= ac\cdot(b^{-1}d^{-1})\\ &= ac\cdot(bd)^{-1}\\ &= \frac{ac}{bd}.\end{aligned}$$

Por otro lado

$$\begin{aligned}\frac{a}{b}+\frac{c}{d} &= ab^{-1}+cd^{-1}\\ &= a\cdot\left(dd^{-1}\right)\cdot b^{-1}+c\cdot\left(bb^{-1}\right)\cdot d^{-1}\\ &= ad\cdot(bd)^{-1}+cb\cdot(bd)^{-1}\\ &= (ad+cb)\cdot(bd)^{-1}=\frac{ad+cb}{bd}.\ \square\end{aligned}$$

Teorema 7.12 *Para todos $a, b \in \mathbb{R}$, $b \neq 0$, se tiene que $\frac{a}{b} = 0 \Leftrightarrow a = 0$.*

Este resultado es una consecuencia inmediata del hecho que $\mathbb{R}$ no posee divisores de cero. Note que si $a \neq 0$, entonces

$$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a},$$

dado que

$$\left(\frac{a}{b}\right)^{-1} = \left(ab^{-1}\right)^{-1} = a^{-1}\left(b^{-1}\right)^{-1} = a^{-1}b = \frac{b}{a}.$$

7.2.3 Axiomas de orden

Se acepta la existencia de un subconjunto $P \subset \mathbb{R}$ (el conjunto de los números reales positivos) que cumple las siguientes propiedades

Axioma 7.2.12 *Si $a \in P$ y $b \in P$, entonces $a + b \in P$.*

Axioma 7.2.13 *Si $a \in P$ y $b \in P$, entonces $ab \in P$.*

Axioma 7.2.14 *Para todo $a \in \mathbb{R}$, si $a \neq 0$, entonces $a \in P$ o bien $-a \in P$. Además $0 \notin P$.*

Los elementos del conjunto P los llamaremos números reales positivos. Al conjunto $P \cup \{0\}$ lo denotaremos por $\mathbb{R}^+$. Si un número no es positivo ni cero, decimos que es negativo. Esto es, a es negativo si $-a$ es positivo.

Definición 7.2.1 *Dados $a, b \in \mathbb{R}$, ponemos $a \geq b$ (se lee "a mayor o igual que b ") si $a - b \in \mathbb{R}^+$. Ponemos $b \leq a$ si $a \geq b$. Ponemos $a > b$ si $a - b \in P$ (o sea, si $a \geq b$ y $a \neq b$), y $b < a$ si $a > b$. Note que $a \geq 0$ sii $a \in \mathbb{R}^+$, y que $a > 0$ sii a es positivo.*

A partir de aquí, se demuestran todas las leyes que rigen el comportamiento de las desigualdades. Veamos algunas de ellas.

Teorema 7.13 *Si $a \in \mathbb{R}$, entonces a y $-a$ no pueden ser ambos positivos.*

Demostración
En efecto, si ambos fueran positivos, entonces por el axioma 7.2.12 se tendría $0 = -a + a \in P$, lo cual contradice el axioma 7.2.14. □

Teorema 7.14 *El "uno" es positivo. Esto es:* $1 > 0$.

Demostración
Por el axioma 7.2.14, sabemos que $1 \in P$ ó $-1 \in P$. Si 1 no fuera positivo, entonces -1 sería positivo, y por el axioma 7.2.13, se tendría que $(-1)(-1)$ es positivo. Pero sabemos que $(-1)(-1) = 1$, y entonces se contradice el teorema anterior. En consecuencia, el 1 es positivo. □

Observación: Note que del axioma 7.2.12 se concluye que:

$$a \geq 0, b \geq 0 \Rightarrow a + b \geq 0.$$

Teorema 7.15 *La relación $\leq$ es de orden total en $\mathbb{R}$.*

Demostración
Por definición se tiene que $a \leq a$ para cada $a \in \mathbb{R}$, y esto es la reflexividad.
Para la antisimetría, supongamos que $a \leq b$ y $b \leq a$. Entonces $b - a \geq 0$ y $a - b \geq 0$. Si a y b fueran distintos, se tendría $x = b - a \neq 0$, pero entonces x y $-x$ serían ambos positivos. Esta contradicción nos permite concluir que $a = b$.
Finalmente, si $a \leq b$ y $b \leq c$, se tiene $b - a \geq 0$ y $c - b \geq 0$, y por la observación anterior:

$$a - c = (a - b) + (b - c) \geq 0,$$

de donde resulta que $a \geq c$. Esto demuestra la transitividad. □

Teorema 7.16 *(Compatibilidad del orden con la suma) Sean a, b, c en $\mathbb{R}$. Entonces*

$$a \geq b \Leftrightarrow a + c \geq b + c.$$

Demostración
En efecto

$$(a + c) - (b + c) = (a + c) + (-b + (-c)) = a + (c + (-c)) + (-b) = a + (-b) = a - b,$$

de donde $a - b \in \mathbb{R}^+$ si y solo si $(a + c) - (b + c) \in \mathbb{R}^+$. □

Teorema 7.17 *(Compatibilidad del orden con el producto) Sean a, b, c en $\mathbb{R}$. Si $a \leq b$ y $c > 0$, entonces $ac \leq bc$. También, si $a < b$ y $c > 0$, entonces $ac < bc$.*

Demostración
En efecto, de las hipótesis se tiene que $b - a \geq 0$ y $c > 0$, de donde $c\,(b - a) \geq 0$, esto es $cb - ca \geq 0$. Consecuentemente $ac \leq bc$. □

El siguiente teorema establece la ley de signos, y se deja como ejercicio:

Teorema 7.18 *Sean $a, b, c \in \mathbb{R}$. Entonces*

1. *Si $a > 0$ y $b < 0$, se tiene $ab < 0$.*
2. *Si $a < 0$ y $b < 0$, se tiene $ab > 0$*

Si multiplicamos ambos lados de una desigualdad por un número negativo, entonces la desigualdad se invierte. El siguiente teorema expresa este hecho, y su demostración se deja como ejercicio.

Teorema 7.19 *Si $a \leq b$ y $c < 0$, entonces $bc \leq ac$*

Finalmente, el lector puede verificar las propiedades siguientes.

Teorema 7.20 *Sean $a, b, c \in \mathbb{R}$. Entonces*

1. $a > 0 \Rightarrow a^{-1} > 0$
2. $a > b > 0 \Rightarrow \dfrac{1}{b} > \dfrac{1}{a}$
3. $a^2 + b^2 \geq 2ab$
4. $a > 1 \Rightarrow a^2 > a$
5. $0 < a < 1 \Rightarrow a > a^2$.

Los axiomas de orden, nos permiten introducir la noción de intervalos en $\mathbb{R}$.
Sean a y b números reales tales que $a < b$. Denotamos por $]a, b[$ al conjunto de todos los números reales comprendidos entre a y b. Es decir,

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

Dicho conjunto se llama intervalo abierto con extremos a y b. Análogamente,

$$[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$$

se llama intervalo cerrado de extremos a y b;

$$[a,b[= \{x \in \mathbb{R} : a \leq x < b\}$$

$$]a,b] = \{x \in \mathbb{R} : a < x \leq b\}$$

se llaman intervalos semiabiertos y finalmente, se tienen los intervalos no acotados de la forma:

$$]a,+\infty[= \{x \in \mathbb{R} : x > a\}$$

$$[a,+\infty[= \{x \in \mathbb{R} : x \geq a\}$$

$$]-\infty,a] = \{x \in \mathbb{R} : x \leq a\}$$

$$]-\infty,a[= \{x \in \mathbb{R} : x < a\}.$$

De manera más general decimos que un conjunto $I \subset \mathbb{R}$ es un intervalo de $\mathbb{R}$ si:

$$\text{para cada } x, y \in I, \text{ con } x \leq y, \text{ se tiene que } [x,y] \subseteq I.$$

Ejemplo 7.2.1 *El conjunto* $A = [2,3[\cup\{5\}$ *no es un intervalo, ya que* $2 \in A$, $5 \in A$, *y* $[2,5]$ *no es subconjunto de* A.

Ejemplo 7.2.2 $\mathbb{R}^*$ *no es un intervalo, pues* $-1 \in \mathbb{R}^*$, $1 \in \mathbb{R}^*$, *y* $[-1,1]$ *no es subconjunto de* $\mathbb{R}^*$.

Ejemplo 7.2.3 *El conjunto* $A = \left\{x \in \mathbb{R}^+ : x^2 > 2\right\}$ *sí es intervalo. En efecto, si* $a, b \in A$, *se sigue que* $a > 0$ *y* $a^2 > 2$. *Luego, para cada* $x \in [a,b]$ *se tiene*

$$x^2 - a^2 = (x-a)(x+a) \geq 0,$$

de donde $x^2 \geq a^2 > 2$, *así que* $x \in A$. *Esto demuestra que* $[a,b] \subseteq A$.

7.2.4 Valor Absoluto

El valor absoluto de un número real x se denota $|x|$, y se define como el mayor de los números x y $-x$. Es decir

$$|x| = \max(x,-x).$$

Equivalentemente,

$$|x| = \begin{cases} x & \text{si } x \geq 0 \\ -x & \text{si } x < 0. \end{cases}$$

Geométricamente, $|x|$ es la distancia del origen al punto representado por x en la recta numérica. Similarmente, $|x-y|$ es la distancia entre los puntos representados por x e y, en la recta numérica. Observe que una consecuencia inmediata de la definición es el hecho que

$$|x| = |y| \Leftrightarrow (x = y \ \text{ ó } \ x = -y)$$

A continuación exponemos algunos resultados importantes acerca del valor absoluto. Para comenzar observe que $|-x| = |x|$. Además, es evidente que $x \leq |x|$ y $-x \leq |x|$. De esto se concluye el siguiente teorema.

Teorema 7.21 *Para todo número real x, se tiene que*

$$-|x| \leq x \leq |x|\,.$$

El lector puede también intentar una demostración considerando los caso $x \geq 0$ y $x < 0$ por separado. Como una consecuencia del resultado anterior, se obtiene que:

Teorema 7.22 *Si $a \geq 0$, entonces*

$$|x| \leq a \Leftrightarrow -a \leq x \leq a$$

Demostración
Debemos demostrar que el lado izquierdo implica el lado derecho, y viceversa. Supongamos primero que $|x| \leq a$ y demostremos que $-a \leq x \leq a$. Primero, por el teorema anterior

$$x \leq |x| \leq a. \tag{7.2}$$

y por el mismo teorema

$$-a \leq -|x| \leq x. \tag{7.3}$$

Combinando los resultados (7.2) y (7.3), resulta

$$-a \leq x \leq a.$$

Recíprocamente, supongamos que $-a \leq x \leq a$. Entonces $x \leq a$ y $-x \leq a$. Como $|x|$ es igual a x o $-x$, obtenemos $|x| \leq a$. □

Teorema 7.23 *Para $a, b \in \mathbb{R}$ tenemos que $a^2 < b^2$ si y sólo si $|a| < |b|$.*

Demostración
El resultado se obtiene de manera directa del hecho que

$$b^2 - a^2 = |b|^2 - |a|^2 = (|b| + |a|)\,(|b| - |a|)\,.$$

Dado que $|b| + |a|$ es siempre positivo (a menos que $a = b = 0$), el lado izquierdo es positivo si y sólo si $|b| - |a|$ lo es. □

Nota: Observe que de igual manera se demuestra que $a^2 \leq b^2$ si y sólo si $|a| \leq |b|$.

Teorema 7.24 *Para cualesquiera números reales x e y, se cumple:*

(a) $|x| = 0 \Leftrightarrow x = 0$

(b) $|xy| = |x|\ |y|$

(c) $|x + y| \leq |x| + |y|$

El resultado (c) se conoce con el nombre de desigualdad triangular.

Demostración
Las partes (a) y (b) se dejan como ejercicio.
Demostremos la parte (c): Sabemos que

$$-|x| \leq x, \qquad -|y| \leq y.$$

Sumando estas desigualdades, se obtiene:

$$-(|x| + |y|) \leq x + y. \tag{7.4}$$

Análogamente, de las desigualdades

$$x \leq |x|, \quad y \leq |y|$$

resulta que

$$x + y \leq |x| + |y|. \tag{7.5}$$

Luego, combinando (7.4) y (7.5) obtenemos

$$-(|x| + |y|) \leq x + y \leq |x| + |y|,$$

lo cual, por el teorema 22, es equivalente a

$$|x + y| \leq |x| + |y|.$$

Otra manera de probar la desigualdad triangular es la siguiente: Observe que

$$\begin{aligned}(a+b)^2 &= a^2 + 2ab + b^2 \\ &\leq a^2 + 2|a| \cdot |b| + b^2 \\ &= |a|^2 + 2|a| \cdot |b| + |b|^2 \\ &= (|a| + |b|)^2,\end{aligned}$$

y por el teorema 7.23 se sigue que $|a + b| \leq |a| + |b|$. □

7.2.5 Una copia de $\mathbb{Q}$

Hasta el momento $\mathbb{R}$ es simplemente un campo ordenado, es decir que en principio no hay diferencia con el campo de los racionales que conocemos. De hecho, se puede demostrar que $\mathbb{R}$ contiene una copia de $\mathbb{Q}$, como procedemos a explicar.
Primero se puede definir una copia del conjunto $\mathbb{N}$ de los números naturales como el menor subconjunto inductivo de $\mathbb{R}$.
Para concretar esto, diremos primero que un subconjunto A de $\mathbb{R}$ se llama inductivo si satisface las propiedades

(a) $0 \in A$.

(b) $x \in A \Rightarrow x + 1 \in A$.

Así por ejemplo $\mathbb{R}$ mismo es inductivo, y $\mathbb{R}^+$ también es inductivo. El intervalo $]0, \infty[$ no es inductivo, pues no satisface la propiedad (a). Por otro lado, el conjunto $\mathbb{R} - \{5\}$ no es inductivo pues no satisface la propiedad (b), ya que $4 \in \mathbb{R} - \{5\}$, pero $4 + 1 = 5 \notin \mathbb{R} - \{5\}$.

Podemos ahora considerar la familia $\mathcal{I}$ de todos los subconjuntos inductivos de $\mathbb{R}$. Entonces tenemos, por ejemplo que $\mathbb{R} \in \mathcal{I}$, $[0, \infty[\in \mathcal{I}$. Definimos $\mathbb{N}$ como la intersección de todos los subconjuntos inductivos de $\mathbb{R}$, esto es

$$\mathbb{N} = \bigcap_{A \in \mathcal{I}} A.$$

Como $0 \in A$, para todo $A \in \mathcal{I}$, tenemos por definición que $0 \in \mathbb{N}$, y entonces $\mathbb{N}$ satisface la propiedad (a). Además, si $x \in \mathbb{N}$ tenemos que $x \in A$ para cualquier conjunto inductivo A, y por lo tanto $x + 1 \in A$. Luego, como esto es cierto para todo $A \in \mathcal{I}$, tenemos que $x + 1 \in \mathbb{N}$, con lo que $\mathbb{N}$ satisface la propiedad (b). Concluimos entonces que $\mathbb{N}$ es también inductivo.

Ahora, como $\mathbb{N}$ está contenido en cualquier conjunto inductivo, concluimos que $\mathbb{N}$ es el conjunto inductivo más pequeño. Esto es en realidad el principio de inducción, y los otros axiomas de Peano se satisfacen trivialmente, usando la función sucesor $n^* = n + 1$.

Hemos construido así una copia de $\mathbb{N}$ dentro del campo $\mathbb{R}$. Luego se define una copia de $\mathbb{Z}$ así:

$$\mathbb{Z} = \mathbb{N} \cup \{x \in \mathbb{R} : -x \in \mathbb{N}\} = \{x \in \mathbb{R} : |x| \in \mathbb{N}\},$$

y finalmente una copia de $\mathbb{Q}$:

$$\mathbb{Q} = \left\{ \frac{a}{b} : a \in \mathbb{Z},\ b \in \mathbb{Z}^* \right\}.$$

Es evidente del teorema 7.11 que las operaciones de $\mathbb{R}$ son cerradas en $\mathbb{Q}$, y que coinciden con las operaciones definidas en la construcción clásica de este campo a partir del anillo de los números enteros. En consecuencia, en lo que sigue usaremos esta copia de $\mathbb{Q}$, obteniendo como resultado $\mathbb{Q} \subseteq \mathbb{R}$.

7.2.6 Ejercicios

1. En las demostraciones anteriores hicimos uso del hecho, más o menos obvio, que $a^2 = |a|^2$. Demuestre este hecho con todo detalle.

2. Si $a < b$ y $c > d$, demuestre que $a - c < b - d$.

3. Demuestre usando solo los axiomas de campo que para $a, b \in \mathbb{R}$ se tiene:

$$a(-b) = -(ab), \quad (-a)b = -(ab), \quad (-a)(-b) = ab.$$

4. Demuestre los teoremas 7.18, 7.19 y 7.20.

5. Si $n \in \mathbb{N}$ y $x, y \in \mathbb{R}$, demuestre que

$$x^n - y^n = (x-y)\left(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}\right).$$

6. Demuestre que para cada $n \in \mathbb{N}^*$, la función $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = x^n$, es estrictamente creciente en $\mathbb{R}^+$.

7. Concluya que la función $g : \mathbb{R}^+ \to \mathbb{R}$, definida por $f(x) = x^n$, es inyectiva (para cualquier $n \in \mathbb{N}^*$).

8. Halle todos los números reales x que satisfacen cada una de las siguientes inecuaciones:

a.) $3 + x^2 < 7$	e.)$3 - x^2 < 3$
b.)$x^2 + 4x + 3 \geq 0$	f.) $\left(x^2 - 4\right)\left(x^2 - 9\right) > 0$
c.)$\dfrac{1}{x} + \dfrac{1}{1-x} > 0$	g.) $(x+1)\left(x^2 - 4\right) < 0$
d.)$\dfrac{x-1}{x+1} > 0$	h.) $(x-1)(x+3)(2x+3) > 0$.

9. Resuelva cada una de las siguientes ecuaciones e inecuaciones:

$\lvert x-2\rvert = 5$,	$\lvert x^2 - 1\rvert > 3$,
$\lvert x+1\rvert < 3$,	$\lvert x^2 + 3x + 2\rvert > 0$,
$\lvert x+1\rvert + \lvert x-2\rvert > 1$,	$\lvert x^2 + 3x + 2\rvert > 1$,
$\lvert x-1\rvert - \lvert x+1\rvert < 1$,	$\lvert x^2 + 3x + 2\rvert \geq \frac{1}{4}$.

10. Demuestre que para $x, y, z \in \mathbb{R}$ se tiene:

    (a) $|xy| = |x||y|$
    (b) $\left|\dfrac{1}{x}\right| = \dfrac{1}{|x|}$, para $x \neq 0$
    (c) $\left|\frac{x}{y}\right| = \frac{|x|}{|y|}$, si $y \neq 0$
    (d) $|x - y| \leq |x| + |y|$
    (e) $|x| - |y| \leq |x - y|$
    (f) $\big|\,|x| - |y|\,\big| \leq |x - y|$
    (g) $|x + y + z| \leq |x| + |y| + |z|$.

11. Se define $\max(a, b)$ como el mayor de los números a y b. En otras palabras,

$$\max(a,b) = \begin{cases} a & \text{si } a \geq b, \\ b & \text{si } a < b. \end{cases}$$

Similarmente se define $\min(a,b)$. Demuestre que

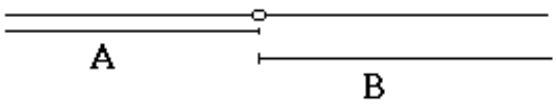
$$\max(a,b) = \frac{a+b+|a-b|}{2}, \quad \min(a,b) = \frac{a+b-|a-b|}{2}.$$

12. Demuestre que si $0 < a < b$, entonces $a < \sqrt{ab} < \frac{a+b}{2} < b$.

7.3 Completitud de $\mathbb{R}$

Hasta el momento no hemos dicho nada que diferencie los campos ordenados $\mathbb{Q}$ y $\mathbb{R}$. El axioma que hace la diferencia es el axioma de completitud, que explicaremos a continuación.

Para tratar de precisar el concepto de completitud en $\mathbb{R}$, tomemos un punto P en la recta, y consideremos el conjunto A formado por todos los números reales "ubicados" a la izquierda de ese punto. Consideremos también el conjunto B formado por todos los números reales "ubicados" a la derecha del mismo punto. Tenemos entonces que para $x \in A$ y $y \in B$ se cumple $x \leq y$. Una forma de expresar la completitud es diciendo que en este caso existe un número real α que corresponde al punto P, y por lo tanto $x \leq \alpha \leq y$, para todo $x \in A$ y todo $y \in B$.



Interpretación de la completitud.

Veamos esto desde un punto de vista más analítico. Consideremos un conjunto $A \subseteq \mathbb{R}$ no vacío, y definamos

$$B = \{y \in \mathbb{R} : y \geq x, \ \forall x \in A\}.$$

Este conjunto B podría ser vacío; tome por ejemplo $A = [1, \infty[$. Cuando $B \neq \emptyset$ decimos que A es acotado superiormente, y a cada elemento de B se le llama cota superior de A. Más precisamente:

Definición 7.3.1 *Decimos que un subconjunto A de los números reales es acotado superiormente si existe $b \in \mathbb{R}$ tal que $x \leq b$, $\forall x \in A$. En tal caso decimos que b es una cota superior de A.*

Considerando entonces el conjunto B de cotas superiores de A, debería existir un α tal que $x \leq \alpha \leq y$, para todo $x \in A$ y todo $y \in B$. Pero entonces, por definición tendríamos $\alpha \in B$, así que α sería la menor cota superior de A. A este número se le llama el *extremo superior de* A, o supremo de A, y se denota $\alpha = \sup A$. Definamos este concepto con más precisión:

Definición 7.3.2 *Sea $A \subset \mathbb{R}$ acotado superiormente, $A \neq \emptyset$. Un elemento $\beta \in \mathbb{R}$ se llama un extremo superior (o supremo) de A, si es la menor de las cotas superiores de A. Dicho de otra forma, β es un extremo superior de A si satisface:*

1. *β es cota superior de A.*
2. *Para todo $b \in \mathbb{R}$, cota superior de A, se tiene $\beta \leq b$.*

La pregunta que surge ahora es, ¿existirá siempre un extremo superior?, y si existe, ¿será único?
La segunda pregunta es fácil de contestar, y la respuesta es *sí.* Para ver esto, suponga que α_1 y α_2 son extremos superiores de A. Entonces, como α_2 es cota superior, la propiedad 2 aplicada a α_1 implica que $\alpha_1 \leq \alpha_2$. Cambiando los roles de α_1 y α_2 se obtiene $\alpha_2 \leq \alpha_1$, y consecuentemente $\alpha_1 = \alpha_2$. La primera pregunta la contesta el axioma del extremo superior.

Axioma 7.3.1 *(Axioma del extremo superior) Sea A un subconjunto no vacío de $\mathbb{R}$, acotado superiormente. Entonces existe el extremo superior de A.*

Ejemplo 7.3.1 *Para $A = [1, 3] \cup \{7\}$ tenemos que $\beta = 7$ es cota superior. Además, dada b otra cota superior de A, como $7 \in A$ debemos tener $7 \leq b$. Esto demuestra que* $\sup A = 7$.

Ejemplo 7.3.2 *Para $A = [0, 1[$, tenemos que $\alpha = 1$ es cota superior de A. Además, si b es cota superior de A, debemos tener $b \geq 1$. En efecto, primero observe que $b \geq 0$, pues $0 \in A$. Luego, si $b < 1$ entonces $x = (b + 1)/2$ sería un elemento de A, y además $x > b$, contradiciendo el hecho que b es cota superior. Esto demuestra que* $\sup A = 1$.

Nota: El ejemplo anterior demuestra que $\sup A$ no necesariamente es un elemento de A. Además, el argumento del ejemplo 7.3.1 demuestra que si una cota superior de A pertenece a dicho conjunto, entonces esa cota es el supremo. En tal caso suele usarse también la palabra *máximo,* y escribir $\max A$ en vez de $\sup A$.

Ejemplo 7.3.3 ***(Intervalos)*** *Para cada $\alpha \in \mathbb{R}$, el conjunto $A = \{x \in \mathbb{R} : x < \alpha\}$ es acotado superiormente, y además $\alpha = \sup A$. Dejamos la verificación como ejercicio.*

La siguiente caracterización del supremo suele ser útil:

Teorema 7.25 *Sea $A \subset \mathbb{R}$, acotado superiormente y no vacío, y sea $\alpha \in \mathbb{R}$. Entonces $\alpha = \sup A$ si y sólo si satisface:*

(a) $x \leq \alpha$, $\forall x \in A$.

(b) Para todo $\varepsilon > 0$, existe $x \in A$ tal que $\alpha - \varepsilon < x$.

Demostración
Supongamos primero que $\alpha = \sup A$, y sea $\varepsilon > 0$. Entonces, como $\alpha - \varepsilon < \alpha$, se tiene que $\alpha - \varepsilon$ no es cota superior de A, y consecuentemente debe existir $x \in A$ tal que $x > \alpha - \varepsilon$. Esto demuestra (b).

Supongamos ahora que (a) y (b) se cumplen y probemos que $\alpha = \sup A$. Primero α es cota superior por la propiedad (a). Ahora sea b una cota superior de A. Si $b < \alpha$, entonces tomando $\varepsilon = \alpha - b > 0$ tenemos, por hipótesis, que existe $x \in A$ tal que $x > \alpha - \varepsilon = b$, lo cual contradice el hecho que b es cota superior. Consecuentemente, $b \geq \alpha$. □

Los conceptos arriba introducidos sobre acotación superior, tienen su versión en el caso de acotación inferior. Veamos:

Definición 7.3.3 *Decimos que A es acotado inferiormente si existe $a \in \mathbb{R}$ tal que $a \leq x$, $\forall x \in A$. En tal caso decimos que a es una cota inferior de A.*

Definición 7.3.4 *Se llama extremo inferior, o ínfimo de un conjunto $A \subset \mathbb{R}$, a la mayor de sus cotas inferiores. Se denota por* $\inf A$.

Teorema 7.26 *Si $A \subset \mathbb{R}$, es acotado inferiormente y no vacío, entonces tiene un extremo inferior.*

Demostración
Consideremos el conjunto

$$B = \{b \in \mathbb{R} : b \text{ es cota inferior de } A\}.$$

Note que $B \neq \emptyset$, pues el hecho que A es acotado inferiormente, asegura la existencia de al menos una cota inferior. Además, como $A \neq \emptyset$, existe al menos un elemento $a \in A$. Si $b \in B$, por definición se tiene $b \leq a$, y esto significa que a es cota superior de B. Por el axioma del extremo superior, existe el extremo superior de B. Sea $\alpha = \sup B$. Ahora, como cada $a \in A$ es cota superior de B, se sigue que $\alpha \leq a$, y esto demuestra que α es cota inferior de A. Es decir, $\alpha \in B$, así que $\alpha = \max B$. Esto demuestra que α es la mayor cota inferior de A. □

Teorema 7.27 *Sea A un subconjunto no vacío de $\mathbb{R}$, acotado inferiormente, y sea $\beta \in \mathbb{R}$. Entonces: $\beta = \inf A$ si y solo si satisface:*
(1) $\forall x \in A$, $\beta \leq x$,
(2) Para todo $\varepsilon > 0$, existe $x \in A$ tal que $x < \beta + \varepsilon$.

Note que la condición (2), asegura que para cualquier $\varepsilon > 0$, $\beta + \varepsilon$ no es cota inferior de A.

Demostración
Totalmente análoga al Teorema 7.25, y se deja como ejercicio. □

7.3.1 Consecuencias de la completitud de $\mathbb{R}$

El axioma del extremo superior puede usarse para demostrar muchas de las propiedades básicas de los números reales, entre ellas:

Teorema 7.28 ***(Principio de Arquímedes)*** *Para todo $x \in \mathbb{R}$, existe $n \in \mathbb{N}$ tal que $n > x$.*

Demostración
Suponga que el resultado es falso. Entonces existe $x \in \mathbb{R}$ tal que $x \geq n$, $\forall n \in \mathbb{N}$. Esto dice que $\mathbb{N}$ es acotado superiormente, implicando la existencia de $\alpha = \sup \mathbb{N}$. Por el teorema 7.25 (con $\varepsilon = 1$), existe $n \in \mathbb{N}$ tal que $n > \alpha - 1$, de donde se sigue que $n+1 > \alpha$. Como $n+1 \in \mathbb{N}$, esto es una contradicción. □

Nota: el principio de Arquímedes o propiedad arquimediana garantiza que el conjunto de los números naturales no está acotado superiormente.
Se deja al lector la tarea de demostrar las siguientes consecuencias del teorema anterior:

Teorema 7.29 *Sea $y \in \mathbb{R}$ tal que $y > 0$. Entonces*

1. *Para cada $x \in \mathbb{R}$, existe $n \in \mathbb{N}$ tal que $x < ny$.*
2. *Existe $n \in \mathbb{N}$ tal que $\frac{1}{n} < y$.*

A continuación demostramos la densidad de $\mathbb{Q}$ como subconjunto de $\mathbb{R}$.

Teorema 7.30 *Dados $x, y \in \mathbb{R}$, con $x < y$, existe un racional $r \in \mathbb{Q}$ tal que $x < r < y$.*

Demostración
Primero tomemos el caso $0 \leq x < y$. Por el teorema anterior, existe $n \in \mathbb{N}$ tal que

$$\frac{1}{n} < y - x.$$

Ahora considere el conjunto

$$A = \{j \in \mathbb{N} : j > nx\}.$$

Por arquimedianidad, A no es vacío, y por el principio del buen orden existe el primer elemento k de A. En particular $k \in A$, $k - 1 \notin A$, esto es

$$\frac{k-1}{n} \leq x < \frac{k}{n}.$$

De la primera desigualdad se sigue que $\frac{k}{n} \leq x + \frac{1}{n} < x + (y - x) = y$, y consecuantemente

$$x < \frac{k}{n} < y.$$

El número racional buscado es entonces $r = \frac{k}{n}$.

En el caso $x < 0 < y$ no hay nada que demostrar (¿ por qué?)
En el caso $x < y \leq 0$, tenemos $0 \leq -y < -x$, y entonces existe $r \in \mathbb{Q}$ tal que $-y < r < -x$. Luego $x < -r < y$, y $-r \in \mathbb{Q}$. □
El teorema enterior es de vital importancia en análisis. Por ejemplo, para definir funciones como la exponencial, resulta sencillo hacerlo primero para los racionales y luego extender la definición a todos los reales utilizando la densidad.

Ejemplo 7.3.4 *Considere el conjunto*

$$A = \{x \in \mathbb{Q} : x < 1\}.$$

La densidad de $\mathbb{Q}$ *nos permite dar una demostración que* $\sup A = 1$. *Veamos:*
Es obvio que 1 *es una cota superior. Ahora, dado* $\varepsilon > 0$, *la densidad de* $\mathbb{Q}$ *permite concluir que existe* $x \in \mathbb{Q}$ *tal que* $1 - \varepsilon < x < 1$, *de donde* $x \in A$ *y* $x > 1 - \varepsilon$. *Esto demuestra que* $\sup A = 1$, *por la caracterización que se dio en el teorema* 25 □

7.3.2 Existencia de raíz cuadrada

El lector probablememente sabe muy bien que dado $a > 0$, $\sqrt{a}$ es un número real positivo tal que $\left(\sqrt{a}\right)^2 = a$, y su existencia se da por un hecho. En esta sección demostramos, usando el axioma del extremos superior, que realmente $\sqrt{a}$ existe, siempre que $a > 0$. Primero, y para enfatizar la diferencia entre $\mathbb{Q}$ y $\mathbb{R}$, recordemos que esto no es posible hacerlo en $\mathbb{Q}$. Específicamente, de acuerdo con el lema 7.1.1, si $n \in \mathbb{N}$ no es cuadrado perfecto, entonces no existe raíz cuadradsa en $\mathbb{Q}$.

Teorema 7.31 *Dado* $a > 0$, *existe un único número real positivo* α *tal que* $\alpha^2 = a$. *Se denota* $\alpha = \sqrt{a}$.

Demostración
Defina el conjunto

$$A = \left\{x \geq 0 : x^2 \leq a\right\}.$$

Note que $A \neq \emptyset$, dado que $0 \in A$. Ahora, note que

$$x > a + 1 \Rightarrow x^2 > (a+1)^2 > a + 1 > a \Rightarrow x \notin A.$$

Equivalentemente,

$$x \in A \Rightarrow x \leq a + 1.$$

Esto demuestra que $a + 1$ es una cota superior de A. Por el axioma del extremo superior, existe $\alpha = \sup A$. Para demostrar que $\alpha^2 = a$, debemos descartar las posibilidades $\alpha^2 > a$ y $\alpha^2 < a$. Veamos:

1. Si $\alpha^2 < a$, tome $0 < \varepsilon < 1$, y note que

$$(\alpha + \varepsilon)^2 = \alpha^2 + 2\alpha\varepsilon + \varepsilon^2 < \alpha^2 + (2\alpha + 1)\varepsilon.$$

Si además $\varepsilon < \left(a - \alpha^2\right) / (2\alpha + 1)$, se sigue que $(\alpha + \varepsilon)^2 < a$. Esto es, $\alpha + \varepsilon \in A$, para todo ε tal que $0 < \varepsilon < \min\left(1, \dfrac{a - \alpha^2}{2\alpha + 1}\right)$. Esto contradice el hecho que α es cota superior de A.

2. Si $\alpha^2 > a$, note que

$$(\alpha - \varepsilon)^2 = \alpha^2 - 2\alpha\varepsilon + \varepsilon^2 > \alpha^2 - 2\alpha\varepsilon.$$

Si $0 < \varepsilon < \left(\alpha^2 - a\right)/2\alpha$, obtenemos $(\alpha - \varepsilon)^2 > a$. Pero por ser $\alpha = \sup A$, existe $x \in A$ tal que $x > \alpha - \varepsilon$, de donde $x^2 > (\alpha - \varepsilon)^2 > a$, lo cual es contradictorio.

Hemos demostrado que efectivamente se tiene $a^2 = a$. La unicidad se deja como ejercicio. □

Un argumento similar al anterior se usa para demostrar que dados $a > 0$, $n \in \mathbb{N}$, existe un único α positivo tal que $\alpha^n = a$. Esto se hará en la sección 7.4

7.3.3 Los números irracionales

Tomando $a \in \mathbb{N}$ que no sea cuadrado perfecto, lo anterior demuestra que existe un número real positivo α tal que $\alpha^2 = a$, y este se denota por $\sqrt{a}$. Además, demostramos antes que no existe racional alguno r tal que $r^2 = a$. Se concluye entonces que $\sqrt{a} \in \mathbb{I}$, donde

$$\mathbb{I} = \mathbb{R} - \mathbb{Q}.$$

Los elementos de I se llaman números irracionales. Las propiedades de campo del conjunto de números racionales, permiten probar una serie de resultados interesantes sobre estos y los irracionales. Por ejemplo, si $a \in \mathbb{Q}$ y $b \in \mathbb{I}$, se sigue que $a + b \in \mathbb{I}$. En efecto, si no fuera así se tendría $a + b \in \mathbb{Q}$, de donde $b = (a + b) - a \in \mathbb{Q}$, imposible! Este hecho permite concluir por ejemplo que $\mathbb{I}$ también es denso en $\mathbb{R}$, usando la densidad de $\mathbb{Q}$ (ver los ejercicios).

Note sin embargo que $\mathbb{I}$ no es un campo, como lo muestra el hecho que la suma y la multiplicación no son cerradas en $\mathbb{I}$. Por ejemplo $\sqrt{2} \in \mathbb{I}$, pero $\sqrt{2} - \sqrt{2} = 0 \notin \mathbb{I}$ y $\sqrt{2} \cdot \sqrt{2} = 2 \notin \mathbb{I}$.

7.3.4 Ejercicios

1. Para los siguientes conjuntos, demuestre que son acotados superiormente, y halle el supremo:

   $A = \{x \in \mathbb{Q} : 1 \leq x < 3\}$

   $A = \left\{1 - \frac{1}{n} : n \in \mathbb{N}\right\}$

   $A =]-\infty, 17] - \mathbb{Z}.$

   $A = \left\{x : x = y^2 + 3y - 1, |y| < 1\right\}$

   $A = \left\{x : x^2 + 3x - 1 < 0\right\}$

2. Para $x, y \in \mathbb{R}$, con $y > 0$, demuestre que existe $n \in \mathbb{N}$ tal que $x < ny$.

3. Si $a < b$, $n \in \mathbb{N}$, demuestre que existen al menos n racionales entre a y b (use inducción). Concluya que existe un número infinito de racionales entre a y b.

4. Complete los detalles en el teorema 7.26.

5. Demuestre la arquimedianidad de $\mathbb{R}$, usando la densidad y arquimedianidad de $\mathbb{Q}$.

6. Demuestre usando el principio de inducción que para $r \neq 1$ y $n \in \mathbb{N}$ se tiene:

$$1 + r + \cdots + r^n = \frac{1 - r^{n+1}}{1 - r}.$$

7. Para $x > -1$, demuestre la desigualdad de Bernoulli: $(1 + x)^n \geq 1 + nx$, $\forall n \in \mathbb{N}$.

8. Sea $x \in \mathbb{R}$. Use el principio del buen orden para demostrar que existe un único $k \in \mathbb{Z}$ tal que $k \leq x < k + 1$. El número k se llama la parte entera de x, y se denota $k = [\![x]\!]$.

9. Demuestre con todo detalle que

$$\sum_{k=1}^{n} a_k = \sum_{k=0}^{n-1} a_{k+1} = \sum_{k=2}^{n+1} a_{k-1}, \quad \sum_{k=0}^{n} a_k = \sum_{k=0}^{n} a_{n-k}.$$

10. Si a es racional y b irracional, demuestre que $a + b$ es irracional. En particular, $-b$ es irracional. ¿Qué pasa con la suma si ambos a y b son irracionales?

11. Use el ejercicio anterior, y la densidad de $\mathbb{Q}$, para demostrar que el conjunto de los números irracionales es denso en $\mathbb{R}$.

12. Si $a \neq 0$ es racional y b irracional, demuestre que ab, ab^{-1} son irracionales. En particular, b^{-1} es irracional. ¿ Qué pasa con el producto si ambos a y b son irracionales?

13. Dé un ejemplo de dos números irracionales, tales que su suma y su producto sean ambos racionales.

14. Demuestre que $\sqrt{n}$ es irracional, si $n \in \mathbb{N}$ no es cuadrado perfecto.

15. Demuestre que $\sqrt{2}+\sqrt{3}$ y $\sqrt{2}-\sqrt{3}$ son irracionales. En general, demuestre que $\sqrt{p}+\sqrt{q}$ y $\sqrt{p} - \sqrt{q}$ son irracionales, si p y q son primos.

16. Más generalmente, demuestre que $\sqrt{n} + \sqrt{m}$ y $\sqrt{n} - \sqrt{m}$ son irracionales, si $n, m \in \mathbb{N}$ son primos relativos, y no son cuadrados perfectos. Dé varios ejemplos no triviales.

7.4 Sumatorias, conteo y existencia de raíces

Regresamos en esta sección, a un tema mencionado en el capítulo de números naturales, el cual sin embargo es importante retomar a la luz de los conceptos nuevos estudiados en el presente capítulo. Además, es importante su utilidad en la demostración de algunos resultados como la existencia de raíces, y el análisis combinatorio.

7.4.1 Repaso de sumatorias

Dada una función $f : \mathbb{N} \to \mathbb{R}$, con la notación $a_n = f(n)$ se define recursivamente:

$$\sum_{k=0}^{0} a_k = a_0, \qquad \sum_{k=0}^{n+1} a_k = \sum_{k=0}^{n} a_k + a_{n+1}.$$

Esto define recursivamente lo que entendemos intuitivamente por

$$\sum_{k=0}^{n} a_k = a_0 + \ldots + a_n.$$

Ejemplo 7.4.1 *Si $a_k = f(k) = k$, demostramos antes que*

$$\sum_{k=0}^{n} a_k = \sum_{k=0}^{n} k = \frac{n(n+1)}{2}.$$

Ejemplo 7.4.2 *Si $a_k = (-1)^k$, tenemos*

$$\sum_{k=0}^{99} a_k = 1 - 1 + 1 - 1 + \cdots + 1 - 1 = 0.$$

Ejemplo 7.4.3 *Si $a_k = \frac{1}{k+1}$ tenemos*

$$\sum_{k=0}^{4} a_k = \frac{1}{0+1} + \frac{1}{1+1} + \frac{1}{2+1} + \frac{1}{3+1} + \frac{1}{4+1} = \frac{137}{60}.$$

Ejemplo 7.4.4 *Demostrar que para todo $n \in \mathbb{N}$ se tiene*

$$\sum_{k=0}^{n} k^2 = \frac{n}{6}(n+1)(2n+1).$$

Para $n = 0$ la sumatoria es 0, mientras que $\frac{0}{6}(0+1)(2\cdot 0+1) = 0$. Ahora si la igualdad es válida para $n \in \mathbb{N}$, la demostramos para $n+1$, veamos:

$$\begin{aligned}\sum_{k=0}^{n+1} k^2 &= \sum_{k=0}^{n} k^2 + (n+1)^2 \\ &= \tfrac{n}{6}(n+1)(2n+1) + (n+1)^2 \\ &= (n+1)\left[\tfrac{n}{6}(2n+1) + n + 1\right] \\ &= \tfrac{n+1}{6}\left(2n^2+7n+6\right) \\ &= \tfrac{n+1}{6}(n+2)(2n+3).\end{aligned}$$

Como $2n+3 = 2(n+1)+1$, la igualdad es válida para $n+1$, y luego para todo n por el principio de inducción.

Si $0 < m \leq n$, se define la sumatoria desde m hasta n así:

$$\sum_{k=m}^{n} a_k = \sum_{k=0}^{n} a_k - \sum_{k=0}^{m-1} a_k = a_m + \cdots + a_n.$$

Ejemplo 7.4.5 *Para $a_k = \frac{1}{k}$ tenemos*

$$\sum_{k=4}^{6} a_k = \frac{1}{4} + \frac{1}{5} + \frac{1}{6} = \frac{37}{60}.$$

Ejemplo 7.4.6 *Para $a_k = k^2$ tenemos*

$$\sum_{k=2}^{n} a_k = \sum_{k=0}^{n} k^2 - \sum_{k=0}^{1} k^2 = \frac{n}{6}(n+1)(2n+1) - 1.$$

Ejemplo 7.4.7 *Para $a_k = \frac{1}{k-1}$ tenemos*

$$\sum_{k=2}^{3} a_k = \frac{1}{2-1} + \frac{1}{3-1} = \frac{3}{2}.$$

Note que aunque f no está definida en $n = 1$, esto no afecta la sumatoria.

Ejemplo 7.4.8 *(Suma geométrica) Para $r \neq 1$ y $n \in \mathbb{N}$ se tiene*

$$\sum_{k=0}^{n} r^k = \frac{1 - r^{n+1}}{1 - r}.$$

Para $r = \frac{1}{2}$ se obtiene en particular

$$\sum_{k=0}^{n} \frac{1}{2^k} = 2 - \frac{1}{2^k}.$$

Este resultado se puede deducir directamente, tomando el producto

$$\begin{aligned}(1-r)\sum_{k=0}^{n} r^k &= (1-r)(1+r+\cdots+r^n)\\ &= 1-r+r-r^2+\cdots+r^{n-1}-r^n+r^n-r^{n+1}\\ &= 1-r^{n+1},\end{aligned}$$

dado que todos los términos intermedios se cancelan. El lector puede dar una demostración por inducción.

7.4.2 Propiedades de las sumatorias

1. Si $c \in \mathbb{R}$ y $a_k = f(k)$, se tiene
$$\sum_{k=0}^{n} ca_k = c\sum_{k=0}^{n} a_k.$$
Para $n = 0$ tenemos $\sum\limits_{k=0}^{0} ca_k = ca_0 = c\sum\limits_{k=0}^{0} a_k$. Ahora si es válido para n se sigue que
$$\sum_{k=0}^{n+1} ca_k = \sum_{k=0}^{n} ca_k + ca_{n+1} = c\sum_{k=0}^{n} a_k + ca_{n+1} = c\left(\sum_{k=0}^{n} a_k + a_{n+1}\right) = c\sum_{k=0}^{n+1} a_k.$$

2. (Ejercicio) Si $a_k = f(k)$, $b_k = g(k)$, se tiene
$$\sum_{k=0}^{n} (a_k + b_k) = \sum_{k=0}^{n} a_k + \sum_{k=0}^{n} b_k.$$

3. (Ejercicio) Si para cada k se tiene $a_k \geq b_k$, entonces
$$\sum_{k=0}^{n} a_k \geq \sum_{k=0}^{n} b_k.$$
En particular, si cada a_k es positivo, se sigue que $\sum\limits_{k=0}^{n} a_k > 0$.

4. Dados $a_0, \ldots, a_{n+1} \in \mathbb{R}$ tenemos
$$\sum_{k=0}^{n} a_{k+1} = \sum_{k=1}^{n+1} a_k.$$
Este resultado es bastante evidente, y se deja como ejercicio.

5. Equivalentemente se tiene
$$\sum_{k=0}^{n} a_k = \sum_{k=1}^{n+1} a_{k-1}.$$

Ahora podemos demostrar más fácilmente la fórmula para la suma geométrica. Si $r \neq 1$ tenemos

$$\begin{aligned}(1-r)\sum_{k=0}^{n} r^k &= \sum_{k=0}^{n} r^k - \sum_{k=0}^{n} r^{k+1} \\ &= 1 + \sum_{k=1}^{n} r^k - \left(\sum_{k=1}^{n} r^k + r^{n+1}\right) \\ &= 1 - r^{n+1},\end{aligned}$$

y dividiendo por $1-r$ obtenemos

$$\sum_{k=0}^{n} r^k = \frac{1-r^{n+1}}{1-r}.$$

Ejemplo 7.4.9 *(**Suma telescópica**) Si $a_k = b_k - b_{k+1}$ para todo $k = 0, 1, \ldots$ tenemos*

$$\sum_{k=0}^{n} a_k = \sum_{k=0}^{n} (b_k - b_{k+1}) = b_0 - b_{n+1}.$$

La idea es que

$$\sum_{k=0}^{n} (b_k - b_{k+1}) = b_0 - b_1 + b_1 - b_2 + \cdots + b_n - b_{n+1} = b_0 - b_{n+1},$$

dado que los términos intermedios se cancelan. Usando las propiedades de las sumatorias tenemos

$$\sum_{k=0}^{n} (b_k - b_{k+1}) = \sum_{k=0}^{n} b_k - \sum_{k=0}^{n} b_{k+1} = b_0 + \sum_{k=1}^{n} b_k - \left(\sum_{k=1}^{n} b_k + b_{n+1}\right) = b_0 - b_{n+1}.$$

El lector puede hacer una demostración usando inducción. Casos particulares de este tipo de sumatorias son:

$$\begin{aligned}\sum_{k=1}^{99} \left(\frac{1}{k^2} - \frac{1}{(k+1)^2}\right) &= 1 - \frac{1}{100^2} = \frac{9\,999}{10\,000}. \\ \sum_{k=1}^{n} \frac{1}{k(k+1)} &= \sum_{k=1}^{n} \left(\frac{1}{k} - \frac{1}{k+1}\right) = 1 - \frac{1}{n+1} = \frac{n}{n+1}.\end{aligned}$$

7.4.3 Combinatoria y fórmula del binomio

Sean $k, n \in \mathbb{N}$, tales que $k \leq n$. Se define

$$\left(\begin{array}{c} n \\ k \end{array} \right) = \frac{n!}{(n-k)!\, k!}.$$

Por ejemplo tenemos

$$\left(\begin{array}{c} n \\ 0 \end{array} \right) = \left(\begin{array}{c} n \\ n \end{array} \right) = \frac{n!}{n!\, 0!} = 1, \qquad \left(\begin{array}{c} n \\ 1 \end{array} \right) = \left(\begin{array}{c} n \\ n-1 \end{array} \right) = \frac{n!}{(n-1)!\, 1!} = n.$$

En general se tiene

$$\left(\begin{array}{c} n \\ n-k \end{array} \right) = \left(\begin{array}{c} n \\ k \end{array} \right), \quad 0 \leq k \leq n.$$

El siguiente resultado es de vital importancia.

Lema 7.4.1 *Para $1 \leq k \leq n$ tenemos*

$$\left(\begin{array}{c} n \\ k-1 \end{array} \right) + \left(\begin{array}{c} n \\ k \end{array} \right) = \left(\begin{array}{c} n+1 \\ k \end{array} \right).$$

En particular $\left(\begin{array}{c} n \\ k \end{array} \right) \in \mathbb{N}$ *, para todo n y todo $k \leq n$.*

Prueba
La igualdad se demuestra en forma directa:

$$\begin{aligned} \left(\begin{array}{c} n \\ k-1 \end{array} \right) + \left(\begin{array}{c} n \\ k \end{array} \right) &= \frac{n!}{(n-k+1)!\,(k-1)!} + \frac{n!}{(n-k)!\, k!} \\ &= \frac{n!\,(k + (n-k+1))}{(n-k+1)!\, k!} \\ &= \frac{(n+1)!}{(n+1-k)!\, k!} \\ &= \left(\begin{array}{c} n+1 \\ k \end{array} \right). \end{aligned}$$

Ahora demostremos que $\left(\begin{array}{c} n \\ k \end{array} \right) \in \mathbb{N}$. Vamos a usar inducción en $\mathbb{N}$, para lo cual definimos el conjunto

$$A = \left\{ n \in \mathbb{N} : \left(\begin{array}{c} n \\ k \end{array} \right) \in \mathbb{N},\ \forall k \leq n \right\}.$$

Note que $0 \in A$, pues $\left(\begin{array}{c} 0 \\ 0 \end{array} \right) = 1 \in \mathbb{N}$. Ahora, si $n \in A$ debemos probar que $n+1 \in A$. Para esto tomamos $k \leq n+1$. Si $k = 0$ ó $k = n+1$, tenemos $\left(\begin{array}{c} n+1 \\ k \end{array} \right) = 1 \in \mathbb{N}$. Si $1 \leq k \leq n$ tenemos

$$\left(\begin{array}{c} n+1 \\ k \end{array} \right) = \left(\begin{array}{c} n \\ k-1 \end{array} \right) + \left(\begin{array}{c} n \\ k \end{array} \right) \in \mathbb{N},$$

por hipótesis de inducción. Luego $n+1 \in A$. Entonces A resulta ser inductivo, y por lo tanto $A = \mathbb{N}$. $\square$
Ahora podemos demostrar la fórmula del binomio.

Teorema 7.32 *Para $a, b \in \mathbb{R}$, y $n \in \mathbb{N}$ se tiene*[1]

$$\begin{aligned} (a+b)^n &= \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) a^{n-k} b^k \\ &= a^n + n a^{n-1} b + \frac{n(n-1)}{2} a^{n-2} b^2 + \ldots + \frac{n(n-1)}{2} a^2 b^{n-2} + n a b^{n-1} + b^n \end{aligned}$$

Prueba
Para $n = 0$ la igualdad es obvia. Supongamos que la igualdad se cumple para n. Entonces

$$\begin{aligned} (a+b)^{n+1} &= (a+b) \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) a^{n-k} b^k \\ &= \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) a^{n-k+1} b^k + \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) a^{n-k} b^{k+1}. \end{aligned}$$

Ahora, la primera sumatoria se escribe como

$$\sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) a^{n-k+1} b^k = a^{n+1} + \sum_{k=1}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) a^{n+1-k} b^k,$$

mientras que la segunda

$$\sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) a^{n-k} b^{k+1} = \sum_{k=1}^{n+1} \left(\begin{array}{c} n \\ k-1 \end{array} \right) a^{n-(k-1)} b^k = \sum_{k=1}^{n} \left(\begin{array}{c} n \\ k-1 \end{array} \right) a^{n+1-k} b^k + b^{n+1}.$$

[1] Nótese que en la sumatoria debe interpretarse $a^0 = 1$ aunque $a = 0$.

Luego, por el lema anterior

$$\begin{aligned}(a+b)^{n+1} &= a^{n+1} + \sum_{k=1}^{n} \left[\begin{pmatrix} n \\ k \end{pmatrix} + \begin{pmatrix} n \\ k-1 \end{pmatrix} \right] a^{n+1-k}b^k + b^{n+1} \\ &= a^{n+1} + \sum_{k=1}^{n} \begin{pmatrix} n+1 \\ k \end{pmatrix} a^{n+1-k}b^k + b^{n+1} \\ &= \sum_{k=0}^{n+1} \begin{pmatrix} n+1 \\ k \end{pmatrix} a^{n+1-k}b^k,\end{aligned}$$

así que la igualdad es válida también para $n+1$. Por el principio de inducción, se cumple para todo n. □

Note el caso particular en que $a = b = 1$, obtenemos:

$$\sum_{k=0}^{n} \begin{pmatrix} n \\ k \end{pmatrix} = 2^n.$$

Este resultado tiene una interpretación interesante. Un conjunto A con n elementos, tiene exactamente $\begin{pmatrix} n \\ k \end{pmatrix}$ subconjuntos con k elementos (ver la siguiente sección). Entonces la suma en el lado izquierdo representa la cantidad total de subconjuntos de A. Esto demuestra que si A tiene n elementos, entonces el conjunto potencia $\mathcal{P}(A)$ tiene 2^n elementos.

7.4.4 Un poco de conteo

Comencemos demostrando el siguiente lema:

Lema 7.4.2 *Dado un conjunto A con n elementos, y dado $k \leq n$, existen exactamente $\begin{pmatrix} n \\ k \end{pmatrix}$ subconjuntos de A con k elementos.*

Prueba
La prueba es por inducción en n, usando el lema de la sección anterior. Para $n = 0$ tenemos $A = \emptyset$, y la única posibilidad es $k = 0$. Como A tiene exactamente un subconjunto con 0 elementos (el conjunto vacío), y como $\begin{pmatrix} 0 \\ 0 \end{pmatrix} = 1$, el resultado es válido para $n = 0$.
Ahora supongamos que es válido para n, y sea A un conjunto con $n+1$ elementos. Sea $a \in A$ cualquiera. Si $k = 0$ ó $k = n+1$, hay exactamente un subconjunto de A con k elementos (el conjunto vacío ó A mismo), y la igualdad se cumple.
En el caso $1 \leq k \leq n$, los subconjuntos de A que tienen k elementos se dividen en dos clases:

- Los que son subconjuntos de $A - \{a\}$: Como $A - \{a\}$ tiene n elementos, por hipótesis de inducción hay $\begin{pmatrix} n \\ k \end{pmatrix}$ de estos subconjuntos.

- Los que contienen al elemento a : Si B es uno de estos, se tiene $B-\{a\} \subseteq A-\{a\}$, y como $B-\{a\}$ tiene $k-1$ elementos, por hipótesis de inducción hay $\left(\begin{array}{c} n \\ k-1 \end{array} \right)$ de estos subconjuntos.

Luego, en total hay

$$\left(\begin{array}{c} n \\ k \end{array} \right) + \left(\begin{array}{c} n \\ k-1 \end{array} \right) = \left(\begin{array}{c} n+1 \\ k \end{array} \right)$$

subconjuntos de A con k elementos, así que el resultado es cierto para $n+1$. □

La observación hecha al final de la sección anterior demuestra que:

Corolario 7.4.1 *Si A tiene n elementos, el conjunto potencia $\mathcal{P}(A)$ tiene 2^n elementos.*

Ejemplo 7.4.10 *¿Cuántos números naturales menores que 10^6 se pueden formar usando sólo los dígitos 0 y 1 ?*
Como los números son menores que 10^6, hay seis espacios a ser llenados con ceros y unos. Los números de menos de seis dígitos se pueden considerar de seis dígitos agregando ceros a la izquierda. Así por ejemplo el 110 se escribe 000110. Para determinar uno de estos números basta con determinar los espacios en que deben colocarse los ceros. El problema es entonces equivalente al de hallar cuántos subconjuntos tiene un conjunto de 6 elementos, y por el corolario tenemos que esta cantidad es $2^6 = 64$.

Ejemplo 7.4.11 *¿Cuántas palabras se pueden formar con las letras A y B, de manera que la A aparezca tres veces y la B cuatro veces?*
Note que las palabras son de siete letras. Para formar una de ellas, se deben escoger los tres espacios en que se va a colocar la letra A, así que el problema es el de hallar la cantidad de subconjuntos de tres elementos que hay en un conjunto de siete elementos. La respuesta es entonces

$$\left(\begin{array}{c} 7 \\ 3 \end{array} \right) = \frac{7!}{4! \cdot 3!} = \frac{7 \cdot 6 \cdot 5}{3 \cdot 2} = 35.$$

Note que la misma respuesta se obtiene escogiendo los cuatro espacios para la letra B.

Ejemplo 7.4.12 *¿Cuántas palabras se pueden formar con las letras A, B y C, de manera que la A aparezca tres veces, y la B cuatro veces y la C cinco veces?*
Ahora las palabras tienen 12 letras. Primero escogemos los espacios para la A, luego para la B, y los de la C quedan automáticamente determinados. Los espacios para la letra A se pueden escoger de $\left(\begin{array}{c} 12 \\ 3 \end{array} \right) = 220$ maneras distintas. Para cada una de esas escogencias, se procede luego a escoger cuatro espacios de los nueve restantes, y esto se puede hacer de $\left(\begin{array}{c} 9 \\ 4 \end{array} \right) = 126$ maneras distintas. En total hay entonces

$$\left(\begin{array}{c} 12 \\ 3 \end{array} \right) \cdot \left(\begin{array}{c} 9 \\ 4 \end{array} \right) = 220 \cdot 126 = 27720$$

palabras.

Ejemplo 7.4.13 *Ahora supongamos que tenemos siete letras distintas, y debemos usarlas todas para formar una palabra de siete letras. El número de palabras que se pueden formar es* 7!, *como se deduce del siguiente lema.*

Lema 7.4.3 *Si A tiene k elementos y B tiene n elementos, con $1 \leq k \leq n$, entonces existen $\dfrac{n!}{(n-k)!}$ funciones inyectivas de A en B.*

Prueba
Vamos a proceder por inducción en n, dejando k libre. Esto es, probamos que el conjunto de naturales n que cumplen el resultado para todo $k \leq n$, es todo $\mathbb{N}$.
Para $n = 1$ debemos tener $k = 1$, y sólo hay una función. Como $\dfrac{1!}{(1-1)!} = 1$, el resultado es válido.
Suponga que el resultado es válido para n. Sea B con $n+1$ elementos, y sea A con k elementos ($k \leq n+1$). Escojamos $a \in A$, $b \in B$, y contemos las funciones inyectivas de A en B tales que $f(a) = b$. Es evidente que el número de estas funciones es igual al número de funciones inyectivas de $A - \{a\}$ en $B - \{b\}$, y por hipótesis de inducción este número es $\frac{n!}{(n-(k-1))!}$. Ahora, como esto puede hacerse para cada $b \in B$, y hay exactamente $n+1$ elementos en B, el total de funciones inyectivas de A en B es

$$(n+1) \cdot \frac{n!}{(n-(k-1))!} = \frac{(n+1)!}{(n+1-k)!},$$

y el resultado es válido para $n+1$. □

Note el caso particular $k = n$. Obtenemos que el número de permutaciones de un conjunto de n elementos es $n!$.

Ejemplo 7.4.14 *¿Cuántas palabras de siete letras se pueden formar de un alfabeto de 28 letras, usando siete letras distintas?*
Tomamos como A al conjunto de espacios donde se colocan las letras de la palabra, y como B al alfabeto. Debemos hallar el número de funciones inyectivas de a en B. La respuesta es

$$\frac{28!}{21!} = 59675\,61600.$$

Ejemplo 7.4.15 *Cinco personas se quieren sentar en una sala en la que hay* 8 *asientos. ¿De cuántas maneras lo pueden hacer?*
La respuesta es $\frac{8!}{3!} = 6720$.

Ejemplo 7.4.16 *Cuatro hombres y tres mujeres se quieren sentar en fila de modo que los hombres queden separados. ¿Cuántas maneras hay de hacerlo?*

Los espacios para los hombres se pueden escoger de 10 *maneras (¿por qué?). Una vez escogidos los espacios, hay* $3! = 6$ *maneras de ubicar los hombres en esos espacios, y* $4! = 24$ *maneras de ubicar las mujeres en los restantes. En total hay entonces* $10 \cdot 6 \cdot 24 = 1440$ *maneras de sentar las siete personas, con las condiciones dadas.*

Ejemplo 7.4.17 *En el ejemplo anterior, si queremos los tres hombres queden juntos, entonces hay* 5 *maneras de escoger los espacios para los hombres. Entonces en total hay* $5 \cdot 6 \cdot 24 = 720$ *maneras de sentar las siete personas.*

Ejemplo 7.4.18 *Ahora supongamos que queremos exactamente dos hombres juntos. Ahora hay* 20 *maneras de escoger los espacios para los hombres. Entonces la respuesta es* $2 \cdot 1440 = 2880$ *maneras. Otra manera de resolver este caso es restando al total de posibilidades* $7! = 5040$, *los casos de los dos ejemplos anteriores, así:*

$$5040 - 1440 - 720 = 2880.$$

7.4.5 Existencia de raíces en $\mathbb{R}$

El argumento utilizado para demostrar la existencia de la raíz cuadrada, puede ser utilizado en general, con pequeñas modificaciones. Comenzaremos con un par de lemas que nos serán de utilidad.

Lema 7.4.4 *Para* $0 < \varepsilon < \alpha$, *y* $n \geq 2$ *se tiene*

$$(\alpha - \varepsilon)^n > \alpha^n - n\alpha^{n-1}\varepsilon.$$

Demostración
En efecto, como $\frac{-\varepsilon}{\alpha} > -1$ la desigualdad de Bernoulli implica

$$(\alpha - \varepsilon)^n = \alpha^n \left(1 + \frac{-\varepsilon}{\alpha}\right)^n > \alpha^n \left(1 + \frac{-\varepsilon}{\alpha} n\right) = \alpha^n - n\alpha^{n-1}\varepsilon. \ \square$$

Lema 7.4.5 *Para* $\alpha > 0$ *y* $0 < \varepsilon < 1$ *se tiene* $(\alpha + \varepsilon)^n < \alpha^n + (\alpha + 1)^n \varepsilon$.

Demostración
Por el teorema del binomio se tiene

$$(\alpha + \varepsilon)^n = \alpha^n + \sum_{k=1}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) \varepsilon^k \alpha^{n-k}.$$

Además, como $0 < \varepsilon < 1$ se sigue que $\varepsilon^k \leq \varepsilon$ para cada $k \geq 1$. Consecuentemente se tiene

$$\begin{aligned} (\alpha + \varepsilon)^n &< \alpha^n + \varepsilon \sum_{k=1}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) \alpha^{n-k} \\ &< \alpha^n + \varepsilon \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) \alpha^{n-k} \\ &= \alpha^n + \varepsilon \left(\alpha + 1\right)^n . \ \square \end{aligned}$$

Teorema 7.33 *Dado $n \in \mathbb{N}$, $n \geq 2$, y $a > 0$, existe un único $\alpha > 0$ tal que $\alpha^n = a$.*

Demostración
Consideramos el conjunto

$$A = \{x \geq 0 : x^n \leq a\}.$$

Note que $A \neq \emptyset$, dado que $0 \in A$. Por otro lado se tiene

$$x > a + 1 \Rightarrow x^n > (a+1)^n > a + 1 > a \Rightarrow x \notin A.$$

Esto demuestra que $a + 1$ es cota superior de A. Por el axioma del extremo superior, existe $\alpha = \sup A$. Para demostrar que $\alpha^n = a$, debemos descartar las posibilidades $\alpha^n > a$ y $\alpha^n < a$. Veamos:

1. Si $\alpha^n < a$, tomemos $0 < \varepsilon < 1$. Por el lema 7.4.5 se tiene

$$(\alpha + \varepsilon)^n < \alpha^n + (\alpha + 1)^n \varepsilon.$$

Si además $\varepsilon < (a - \alpha^n) / (\alpha + 1)^n$ se sigue que $(\alpha + \varepsilon)^n < a$, lo que implica $\alpha + \varepsilon \in A$. Esto contradice el hecho que α es cota superior de A.

2. Si $\alpha^n > a$, tomamos $0 < \varepsilon < a$. Por el lema 7.4.4 se tiene

$$(\alpha - \varepsilon)^n > \alpha^n - n\alpha^{n-1}\varepsilon.$$

Si además $\varepsilon < (\alpha^n - a) / \left(n\alpha^{n-1}\right)$, obtenemos $(\alpha - \varepsilon)^n > a$. Pero por ser $\alpha = \sup A$, existe $x \in A$ tal que $x > \alpha - \varepsilon$, de donde $x^n > (\alpha - \varepsilon)^n > a$, lo cual es contradictorio.

Hemos demostrado que efectivamente se tiene $a^n = a$. La unicidad se deja como ejercicio. □

7.4.6 Ejercicios

1. Demuestre que $\sqrt[4]{3}$, $\sqrt[3]{5}$, $\sqrt[5]{6}$ son irracionales.
2. Sean $k, n \in \mathbb{N}$. Demuestre que si $\sqrt[k]{n} \notin \mathbb{N}$, entonces es irracional. Es decir, $\sqrt[k]{n} \in \mathbb{N} \cup \mathbb{I}$.
3. Demuestre que
$$\sum_{k=0}^{n} (a_k + b_k) = \sum_{k=0}^{n} a_k + \sum_{k=0}^{n} b_k.$$
4. Si para cada k se tiene $a_k \geq b_k$, entonces
$$\sum_{k=0}^{n} a_k \geq \sum_{k=0}^{n} b_k.$$

Si además $a_k > b_k$ para al menos un k, se sigue que

$$\sum_{k=0}^{n} a_k > \sum_{k=0}^{n} b_k.$$

En particular, si $a_k \geq 0$ para cada k, y al menos uno es positivo, se sigue que $\sum_{k=0}^{n} a_k > 0$.

5. Demuestre la fórmula de las sumas telescópicas, usando el principio de inducción.

6. Usando la fórmula del binomio, demuestre que

$$\sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) = 2^n, \quad \sum_{k=0}^{n} (-1)^k \left(\begin{array}{c} n \\ k \end{array} \right) = 0.$$

7. Para α, ε reales positivos, y $n \geq 2$ demuestre que

$$(\alpha + \varepsilon)^n > \alpha^n + n\alpha^{n-1}\varepsilon.$$

8. Demuestre que si A tiene n elementos, entonces A tiene 2^{n-1} subconjuntos de cardinalidad par, y 2^{n-1} subconjuntos de cardinalidad impar. Sug. Aplique el teorema del binomio con $a = -1$ y $b = 1$.

9. Dé un argumento combinatorio para demostrar el teorema del binomio.

Apéndice A

Axiomatización de $\mathbb{N}$

A.1 Los axiomas de Peano

La descripción que haremos se debe a G. Peano (1889). Se parte de la existencia de un sistema $(\mathbb{N}, *)$, compuesto por un conjunto $\mathbb{N}$ y una función $* : \mathbb{N} \to \mathbb{N}$ (llamada la función sucesor) que satisfacen los siguientes axiomas:

P1 Todo $n \in \mathbb{N}$ tiene un único sucesor $n^* \in \mathbb{N}$ (es decir que $*$ es una función).

P2 $n \neq m$ implica $n^* \neq m^*$ (esto es, $*$ es inyectiva).

P3 Existe un elemento en $\mathbb{N}$, denotado por 0, tal que $0 \neq n^*$, para todo $n \in \mathbb{N}$ (i.e. $*$ no es sobreyectiva).

P4 Principio de inducción: Si $S \subseteq \mathbb{N}$ satisface: $0 \in S$ y $(n \in S \Rightarrow n^* \in S)$, entonces $S = \mathbb{N}$.

Con estos cuatro axiomas se puede construir toda la aritmética de los números naturales.

El sucesor de 0 se denota por 1. De la misma forma se denota $2 = 1^*$, $3 = 2^*$, etc. Si $m = n^*$, diremos que n es el antecesor de m. Nótese que por el axioma P2, el antecesor de m es único.

Los axiomas no dicen explícitamente que todo natural diferente de cero tenga antecesor (i.e. pertenezca al ámbito de $*$). Comenzaremos demostrando este hecho. Para ello consideremos el conjunto

$$S = \{m^* : m \in \mathbb{N}\} \cup \{0\} \subseteq \mathbb{N}.$$

Nótese que por definición $0 \in S$. Además, la implicación

$$n \in S \Rightarrow n^* \in S$$

se cumple trivialmente, dado que $n^* \in S$ para todo $n \in \mathbb{N}$. Por el axioma P4 se concluye que $S = \mathbb{N}$. Esto demuestra que todo $n \in \mathbb{N}$, excepto el cero, tiene antecesor. $\square$

Definición A.1.1 *Diremos que un conjunto $D \subseteq \mathbb{N}$ es un segmento inicial de $\mathbb{N}$ si cumple*

1. $0 \in D$
2. Si $n \in \mathbb{N}$ es tal que $n^* \in D$, entonces $n \in D$
3. Existe $m \in D$ único, tal que $m^* \notin D$ (m se llama elemento maximal de D)

Intuitivamente, los segmentos iniciales son los conjuntos de la forma $\{0, 1, \ldots, m\}$.

Nota: Es importante observar que si D es un segmento inicial con elemento maximal m, entonces $D \cup \{m^*\}$ es un segmento inicial con elemento maximal m^*. Recíprocamente, si D es un segmento inicial con elemento maximal m^*, entonces $D - \{m^*\}$ es un segmento inicial con elemento maximal m. La demostración de estas afirmaciones es bastante directa, y se deja como ejercicio.

Lema A.1.1 *Para cada $m \in \mathbb{N}$, existe un único segmento inicial D_m con elemento maximal m.*

Demostración
Sea

$$S = \{m \in \mathbb{N} : m \text{ es maximal para un único segmento inicial}\}.$$

Como $D = \{0\}$ es el único segmento inicial para el que $m = 0$ es maximal, se tiene $0 \in S$. Ahora si $m \in S$, sea D_m el único segmento inicial cuyo elemento maximal es m. Dado un segmento inicial D, si m^* es maximal para D, se sigue que $D - \{m^*\}$ es un segmento inicial con elemento maximal m, y por unicidad $D - \{m^*\} = D_m$. Consecuentemente $D = D_m \cup \{m^*\}$. Esto demuestra que $D_m \cup \{m^*\}$ es el único segmento inicial con elemento maximal m^*. Se concluye que S es inductivo, y por el principio de inducción $S = \mathbb{N}$. □

Definición A.1.2 *El segmento inicial D_m del lema anterior, se llamará segmento inicial determinado por m.*

Lema A.1.2 *(principio de recurrencia) Dado un conjunto A, un elemento $a \in A$, y una función $g : \mathbb{N} \times A \to A$, existe una única función $f : \mathbb{N} \to A$ que satisface la fórmula recurrente:*

$$f(0) = a, \quad f(n^*) = g(n, f(n)). \tag{A.1}$$

Demostración
Diremos que una función φ es aceptable, si su dominio es un segmento inicial de $\mathbb{N}$, y si satisface (A.1) siempre que n^* pertenezca a dicho dominio.
Considere el conjunto

$$S = \{m \in \mathbb{N} : \text{existe una única función aceptable definida en } D_m\}.$$

Note que $0 \in S$, pues $\varphi = (\{0\}, A, \{(0,a)\})$ es la única función aceptable en $D_0 = \{0\}$. Ahora sea $m \in S$ y φ_m la función aceptable única correspondiente. Se define φ_{m^*} en $D_{m^*} = D_m \cup \{m^*\}$ mediante

$$\varphi_{m^*}(n) = \begin{cases} \varphi_m(n) & \text{si } n \in D_m \\ g(m, \varphi(m)) & \text{si } n = m^* \end{cases}$$

Entonces claramente φ_{m^*} es la única función aceptable en D_{m^*}, y por lo tanto $m^* \in S$. Esto demuestra que S es inductivo, y consecuentemente $S = \mathbb{N}$.
Finalmente, definimos $f : \mathbb{N} \to A$ por

$$f(n) = \varphi_n(n), \ \forall n \in \mathbb{N}.$$

Claramente, esta cumple con la fórmula recurrente. Por otro lado, si h fuera otra función que cumple con (A.1), la restricción de h a D_m sería aceptable, y por la unicidad en los segmentos iniciales se tendría $h(m) = \varphi_m(m) = f(m)$ para cada m. Consecuentemente f es única. □

A.2 Operaciones en $\mathbb{N}$

Note que los axiomas no dan tampoco las operaciones de $\mathbb{N}$, de una manera explícita. Debemos entonces dar una definición de ellas.

A.2.1 La suma en $\mathbb{N}$

Para definir la suma, podemos fijar un elemento $m \in \mathbb{N}$, y definir $m + n$ para cada $n \in \mathbb{N}$ en forma recursiva en n. Es decir, se define

$$m + 0 = m, \quad m + n^* = (m + n)^*. \tag{A.2}$$

Más precisamente, considerando $A = \mathbb{N}$, $a = m$ y $g(n, x) = x^*$, el principio de recurrencia nos dice que existe una única función $f : \mathbb{N} \to \mathbb{N}$ que cumple $f(0) = m$, $f(n^*) = (f(n))^*$, luego se denota $m + n = f(n)$.
Note que en particular

$$m + 1 = m + 0^* = (m + 0)^* = m^*.$$

Demostremos algunas de las propiedades básicas de la suma.

Propiedad A.2.1 *(Asociatividad) Para $m, n, k \in \mathbb{N}$ se tiene*

$$(m + n) + k = m + (n + k).$$

Para demostrarlo usaremos inducción en k. Más precisamente, demostraremos que el conjunto

$$S = \{k \in \mathbb{N} : (m + n) + k = m + (n + k), \forall m, n \in \mathbb{N}\}$$

es inductivo, concluyendo que $S = \mathbb{N}$.
Primero, como $(m+n)+0 = m+n = m+(n+0)$, *tenemos que* $0 \in S$. *Luego, partiendo de* $k \in S$, *tenemos por definición que*

$$(m+n)+k^* = ((m+n)+k)^* = (m+(n+k))^* = m+(n+k)^* = m+(n+k^*),$$

lo que demuestra que $k^* \in S$. *Por el principio de inducción (axioma P4) se tiene* $S = \mathbb{N}$, *y por lo tanto la suma es asociativa.*

Propiedad A.2.2 *Para todo* $m \in \mathbb{N}$ *se tiene* $0+m = m$.
Para demostrar esto, consideramos el conjunto

$$A = \{m \in \mathbb{N} : 0+m = m\}.$$

Tenemos $0 \in A$ *pues* $0+0 = 0$. *Dado* $m \in A$ *se tiene* $0+m = m$, *de donde* $0+m^* = (0+m)^* = m^*$, *y entonces* $m^* \in A$. *Por el axioma P4 tenemos* $A = \mathbb{N}$.

Propiedad A.2.3 *Para todo* $m \in \mathbb{N}$ *se tiene* $1+m = m^*$. *Es decir* $1+m = m+1$.
La demostración es similar a la anterior, y se deja como ejercicio.

Propiedad A.2.4 *(Conmutatividad) Para* $m, n \in \mathbb{N}$ *se tiene* $m+n = n+m$.
Considere

$$S = \{n \in \mathbb{N} : m+n = n+m, \forall m \in \mathbb{N}\}.$$

Tenemos $0 \in S$ *pues* $m+0 = m = 0+m$, *para todo* $m \in \mathbb{N}$, *por la definición y lo que acabamos de demostrar.*
Procedamos con el paso inductivo: Dado $n \in S$ *tenemos* $m+n = n+m$, *para todo* $m \in \mathbb{N}$. *Usando esto y las propiedades anteriores tenemos*

$$\begin{aligned} m+n^* &= (m+n)^* = (n+m)^* = n+m^* \\ &= n+(m+1) = n+(1+m) \\ &= (n+1)+m = n^*+m, \end{aligned}$$

así que $n^* \in S$. *Por el axioma P4 tenemos* $S = \mathbb{N}$, *y la suma es conmutativa.*

Propiedad A.2.5 *(No hay inversos en* $\mathbb{N}$*) Si* $m+n = 0$ *entonces* $m = n = 0$.
En efecto, supongamos que $m, n \in \mathbb{N}$ *son tales que* $m+n = 0$. *Si* $n \neq 0$ *entonces* $n = k^*$, *para algún* $k \in \mathbb{N}$. *Luego*

$$0 = m+n = m+k^* = (m+k)^*,$$

lo que contradice el axioma P3. Luego debe tenerse $n = 0$, *y consecuentemente* $m = 0$.

Propiedad A.2.6 *(Ley de cancelación) Supongamos que $m, n, p \in \mathbb{N}$ son tales que $n + p = m + p$. Entonces $n = m$.*
En efecto, si $p = 0$ la implicación es inmediata. Luego, asumiendo que es válida para $p \in \mathbb{N}$, se sigue que:

$$n + p^* = m + p^* \Rightarrow (n + p)^* = (m + p)^* \Rightarrow n + p = m + p \Rightarrow n = m,$$

donde hemos usado el axioma P2 y la hipótesis de inducción. Por el principio de inducción, la implicación es válida para todo $p \in \mathbb{N}$.

Propiedad A.2.7 *Como un caso particular de la ley de cancelación, tomando $m = 0$ tenemos:*

$$n + p = p \Rightarrow n = 0.$$

A.2.2 La multiplicación en $\mathbb{N}$

Similarmente al caso de la suma, se define la multiplicación por recurrencia así:

$$m \cdot 0 = 0, \quad m \cdot (n + 1) = m \cdot n + m.$$

Note que en particular $m \cdot 1 = m \cdot (0 + 1) = m \cdot 0 + m = m$, es decir el 1 es el neutro de la multiplicación por la derecha. A continuacion se demuestra que también lo es por la izquierda.

Propiedad A.2.8 *Para todo $n \in \mathbb{N}$ se tiene $1 \cdot n = n$.*
En efecto, para $n = 0$ la igualdad se obtiene por definición. Luego, si $1 \cdot n = n$ tenemos

$$1 \cdot n^* = 1 \cdot n + 1 = n + 1 = n^*.$$

Por el axioma P4 se obtiene el resultado.
Tenemos entonces

$$n \cdot 1 = 1 \cdot n = n, \ \forall n \in \mathbb{N},$$

así que 1 es el neutro de la multiplicación en $\mathbb{N}$.

Propiedad A.2.9 *(Distributividad por la izquierda) Para $m, n, k \in \mathbb{N}$ se tiene*

$$m \cdot (n + k) = m \cdot n + m \cdot k.$$

Hagamos inducción en k. Para $k = 0$ se tiene

$$m \cdot (n + 0) = m \cdot n = m \cdot n + 0 = m \cdot n + m \cdot 0.$$

Paso inductivo: Si $m \cdot (n + k) = m \cdot n + m \cdot k$*, se sigue que*

$$\begin{aligned} m \cdot (n + k^*) &= m \cdot (n + k)^* \\ &= m \cdot (n + k) + m \\ &= (m \cdot n + m \cdot k) + m \\ &= m \cdot n + (m \cdot k + m) \\ &= m \cdot n + m \cdot k^*, \end{aligned}$$

lo que demuestra que la igualdad es válida para k^**. Luego, por el principio de inducción es válida para todo* $k \in \mathbb{N}$*.*

Propiedad A.2.10 *(Distributividad por la derecha) Para* $m, n, k \in \mathbb{N}$ *se tiene*

$$(n + k) \cdot m = n \cdot m + k \cdot m.$$

La demostración es similar a la anterior, y se deja como ejercicio. En este caso, es recomendable hacer inducción en m*.*

Usando las propiedades anteriores, se demuestra la conmutatividad y asociatividad de la multiplicación.

Propiedad A.2.11 *Para* $m, n, k \in \mathbb{N}$ *se tiene*

$$m \cdot (n \cdot k) = (m \cdot n) \cdot k, \quad m \cdot n = n \cdot m.$$

La demostración se deja como ejercicio.

Propiedad A.2.12 *(En* $\mathbb{N}$ *no hay divisores de cero) Si* $m \cdot n = 0$*, entonces* $m = 0$ *ó* $n = 0$*. En efecto, supongamos que* $m, n \in \mathbb{N}$ *son tales que* $m \cdot n = 0$*. Si* $n \neq 0$ *entonces* $n = k^*$*, para algún* $k \in \mathbb{N}$*. Luego*

$$0 = m \cdot n = m \cdot k^* = m \cdot k + m.$$

Como no hay inversos en $\mathbb{N}$ *(propiedad A.2.5) se tiene* $m = 0$*.*

A.3 Orden en $\mathbb{N}$

Diremos que m es "*menor que o igual a*" n si existe $k \in \mathbb{N}$ tal que $m + k = n$. En tal caso se escribe $m \leq n$. Note que en particular $n \leq n^*$, para todo $n \in \mathbb{N}$, pues $n + 1 = n^*$. Además, para todo n tenemos $0 \leq n$, pues tomando $k = n$ se tiene $0 + k = n$. Veamos que esta relación es de orden:

- Dado que $n + 0 = n$ tenemos $n \leq n$, para todo $n \in \mathbb{N}$. Entonces la relación $\leq$ es reflexiva.

- Si $m \leq n$ y $n \leq m$,se sigue que existen k_1, $k_2 \in \mathbb{N}$ tales que $m + k_1 = n$ y $n + k_2 = m$. Luego
$$m + (k_1 + k_2) = (m + k_1) + k_2 = n + k_2 = m,$$
y por la ley de cancelación se sigue que $k_1 + k_2 = 0$. Luego $k_1 = k_2 = 0$ (por la propiedad A.2.5) y consecuentemente $m = n$. Esto demuestra que la relación $\leq$ es antisimétrica.

- Por último, si $m \leq n$ y $n \leq p$, existen k_1, $k_2 \in \mathbb{N}$ tales que $m + k_1 = n$ y $n + k_2 = p$. Luego
$$p = n + k_2 = (m + k_1) + k_2 = m + (k_1 + k_2),$$
lo que demuestra que $m \leq p$. Hemos demostrado la trasitividad.

La relación $\leq$ es entonces de orden. Si $m \leq n$ y $m \neq n$, decimos que m es menor que n, y escribimos $m < n$. Note que $0 < n$, para todo $n \neq 0$.

A.3.1 La ley de tricotomía

Sea $n \in \mathbb{N}$, y defina el conjunto

$$\begin{aligned} A &= \{m \in \mathbb{N} : m < n\} \cup \{m \in \mathbb{N} : n \leq m\} \\ &= \{m \in \mathbb{N} : m < n\} \cup \{n\} \cup \{m \in \mathbb{N} : n < m\}. \end{aligned}$$

Vamos a probar que A es inductivo. Primero note que como $0 \leq n$ entonces $0 \in A$. Supongamos que $m \in A$ y probemos que $m^* \in A$. Tenemos dos posibilidades:

- Si $m < n$ entonces existe $k \in \mathbb{N}$ tal que $n = m + k$, y además $k \neq 0$. Luego $k = p^*$, para algún $p \in \mathbb{N}$, con lo que $n = m + (p + 1) = (m + 1) + p$. Esto muestra que $m + 1 \leq n$, y por lo tanto $m + 1 \in A$.

- Si $n \leq m$, dado que $m \leq m + 1$ se sigue por transitividad que $n \leq m + 1$, y por lo tanto $m + 1 \in A$.

Por el principio de inducción concluimos que $A = \mathbb{N}$.
Esto demuestra la llamada *ley de tricotomía* que conocemos desde la secundaria. Dicho de otra forma, el orden que hemos definido en $\mathbb{N}$ es un orden total.

Lema A.3.1 *(ley de tricotomía) Dados $m, n \in \mathbb{N}$, se cumple una y solo una de las siguientes:*

$$m < n,\ m = n,\ n < m.$$

A.4 La resta y la división

La resta y la división en $\mathbb{N}$ son operaciones "incompletas", en el sentido que no siempre se pueden realizar. Por ejemplo, en $\mathbb{N}$ no tiene sentido hablar de $3-7$, $0-1$, ó $5 \div 9$. Para poder hablar de $n-m$, necesitamos tener $n \geq m$. En tal caso, la misma definición de orden nos da la definición de $n-m$.
En efecto, para $m \leq n$ tenemos por definición que existe $k \in \mathbb{N}$ tal que $m+k=n$. Por la ley de cancelación de la suma, dicho k es único ($m+k=m+k'=n \Rightarrow k=k'$). Definimos entonces $n-m=k$. Esto es, $n-m$ se caracteriza por:

$$k = n-m \Leftrightarrow m+k=n.$$

En particular, si $n=m^*=m+1$, entonces $m=n-1$. Note además que algunas propiedades de la suma se heredan a la resta. Por ejemplo:

Propiedad A.4.1 *La multiplicación es distributiva con respecto a la resta:*

$$p \cdot (n-m) = p \cdot n - p \cdot m,$$

para $p \in \mathbb{N}$, $m \leq n$. En efecto, si $k=n-m$ tenemos $m+k=n$, de donde

$$p \cdot m + p \cdot k = p \cdot (m+k) = p \cdot n,$$

lo que significa $p \cdot k = p \cdot n - p \cdot m$. Finalmente, reemplazando k por $n-m$ obtenemos el resultado.

Sin embargo, hay que tener cuidado con ciertas propiedades de la suma que no son válidas para la resta. Por ejemplo, la resta no es asociativa, como lo muestran los siguientes cálculos:

$$9-(4-3) = 9-1 = 8 \neq (9-4)-3 = 5-3 = 2.$$

Por otro lado, acerca de la conmutatividad de la resta en $\mathbb{N}$, no tiene siquiera sentido hablar, puesto que cuando $m<n$, $m-n$ no está definido.

Similarmente se puede definir la división: Dados $m, n \in \mathbb{N}$, con $m>0$, decimos que m es divisor de n si existe $k \in \mathbb{N}$ tal que $m \cdot k = n$. En los ejercicios se pide demostrar la ley de cancelación de la multiplicación, la cual implica, al igual que en el caso de la suma, que k es único. Definimos entonces $n \div m = k$. Con frecuencia se usa la notación $\frac{n}{m}$ en vez de $n \div m$. Tenemos

$$k = \frac{n}{m} \Leftrightarrow m \cdot k = n.$$

A.5 Ejercicios

1. Demuestre que la relación de orden en $\mathbb{N}$ es compatible con las operaciones:

$$\begin{aligned} m &\leq n \Rightarrow (m+k \leq n+k) \text{ y } (m \cdot k \leq n \cdot k), \\ m &< n \Rightarrow m+k < n+k. \end{aligned}$$

   Si además $k > 0$ entonces:

$$m < n \Rightarrow m \cdot k < n \cdot k.$$

2. Use la segunda parte del ejercicio anterior, y la ley de tricotomía, para demostrar la ley de cancelación de la multiplicación: Si $k \neq 0$ entonces

$$m \cdot k = n \cdot k \Rightarrow m = n.$$

3. Si $k \leq m$ y $m \leq n$, demuestre que $m - k \leq n - k$.

4. Demuestre que no existe $n \in \mathbb{N}$ tal que $0 < n < 1$. Concluya que en general, dado $m \in \mathbb{N}$, no existe $n \in \mathbb{N}$ tal que $m < n < m + 1$.

5. Demuestre que la división distribuye por la derecha con respecto a la suma y la resta. Es decir si p es divisor de m y n se tiene:

$$(m+n) \div p = m \div p + n \div p, \quad (m-n) \div p = m \div p - n \div p,$$

   donde $m > n$ en el segundo caso.

6. Demuestre que la división no distribuye por la izquierda con respecto a la suma y la resta. Esto es, en general se tiene

$$p \div (m+n) \neq p \div m + p \div n, \quad p \div (m-n) \neq p \div m - p \div n.$$

   Es más, dé ejemplos en los que $p \div m$ y $p \div n$ estén definidos, pero $p \div (m+n)$ no lo esté (o viceversa).

Apéndice B

Construcción de $\mathbb{R}$

B.1 Un poco de intuición

Pensemos en un punto P sobre una recta numérica en la cual se han ubicado los racionales en la forma usual. Geométricamente, este punto determina dos conjuntos de números racionales, uno de los cuales está el formado por los que corresponden a puntos a la izquierda de P. Denotemos este conjunto con A, y observemos lo siguiente:

1. $A \neq \phi$ y $A \neq \mathbb{Q}$, pues existen racionales tanto a la izquierda como a la derecha del punto P.

2. Si $r \in A$ entonces todos los racionales menores que r también pertenecen a A.

3. El conjunto A no tiene máximo. Esto es consecuencia del hecho que en cualquier segmento de la recta numérica siempre existen "puntos racionales".

Si bien estas observaciones son bastante heurísticas, pues nos hemos basado únicamente en nuestra intuición geométrica, ellas nos indican una forma de proceder para dar una construcción rigurosa de $\mathbb{R}$. A un conjunto con estas propiedades lo llamaremos cortadura de Dedekind, o simplemente cortadura.

Definición B.1.1 *Sea α un subconjunto de $\mathbb{Q}$. Decimos que α es una cortadura de Dedekind si satisface:*

(i) $\alpha \neq \phi$ *y* $\alpha \neq \mathbb{Q}$

(ii) Si $r \in \alpha$ *entonces* $\{q \in \mathbb{Q} : q < r\} \subseteq \alpha$ *(α contiene todos los racionales menores que r)*

(iii) Dado $r \in \alpha$, *existe* $q \in \alpha$ *tal que* $q > r$ *(α no tiene máximo)*

Ejemplo B.1.1 *Por ejemplo, el conjunto*

$$\mathbb{Q}^- = \{x \in \mathbb{Q} : x < 0\}$$

es una cortadura. Denotaremos esta cortadura por $\widehat{0}$.

Ejemplo B.1.2 *En general, dado cualquier racional* p*, el conjunto*

$$\widehat{p} = \{q \in \mathbb{Q} : q < p\}$$

es una cortadura (demuéstrelo como ***ejercicio****). Usaremos también* α_p *para denotar esta cortadura.*

Ejemplo B.1.3 *Los conjuntos*

$$A = \{x \in \mathbb{Q} : x \leq 3\} \ y \ \ B = \{x \in \mathbb{Q} : x > 3\}$$

no son cortaduras. El primero no satisface la propiedad (iii), mientras que el segundo no satisface la propiedad (ii).

Las siguientes propiedades son consecuencia de la definición de cortadura.

Lema B.1.1 *Sea* α *una cortadura. Entonces:*

(a) Si $p \in \alpha$ *y* $q \notin \alpha$*, se tiene* $p < q$*. En otras palabras, si* $q \notin \alpha$ *entonces* q *es cota superior de* α*.*

(b) Si $r \notin \alpha$ *y* $r < s$*, entonces* $s \notin \alpha$*.*

Demostración

(a) En efecto, si se diera $q \leq p$ se tendría $q \in \alpha$, lo cual contradice la hipótesis.

(b) Si tuviésemos $s \in \alpha$ entonces, como $r < s$ se tendría $r \in \alpha$, lo cual es falso. □

Ya vimos en forma intuitiva que cada punto sobre la recta determina una cortadura, y también es intuitivamente claro que cada cortadura corresponde a un punto de la recta. Con esa misma intuición, podemos convencernos de que dos puntos distintos corresponden con a cortaduras distintas. Es decir, hay exactamente una cortadura para cada punto sobre la recta.

B.2 Definición de $\mathbb{R}$

Ahora, queremos definir el conjunto de los números reales de manera que haya un real para cada punto sobre la recta. Dado que ya nos convencimos de que hay una cortadura para cada punto sobre la recta, es natural definir:

$$\mathbb{R} = \{\alpha \in \mathcal{P}(\mathbb{Q}) : \alpha \text{ es una cortadura}\}.$$

Los elementos de $\mathbb{R}$ son entonces cortaduras, y los llamaremos también *números reales*. El ejemplo B.1.2 demuestra que cada racional p determina una cortadura (i.e. número real) $\widehat{p} \in \mathbb{R}$. Más adelante utilizaremos esto para identificar a $\mathbb{Q}$ con el conjunto

$$\widehat{\mathbb{Q}} = \{\widehat{p} : p \in \mathbb{Q}\} \subseteq \mathbb{R}.$$

Ejemplo B.2.1 *Consideremos el conjunto*

$$A = \mathbb{Q}^- \cup \{x \in \mathbb{Q} : x^2 < 2\}. \tag{B.1}$$

(i) Nótese que $A \neq \phi$, pues $\mathbb{Q}^- \subseteq A$. Además $A \neq \mathbb{Q}$, pues por ejemplo $3 \notin A$.

(ii) Sean $r \in A$ y $q \in \mathbb{Q}$ tales que $q < r$. Consideremos dos casos:

- *Si $q \leq 0$, entonces $q \in \mathbb{Q}^-$, así que $q \in A$.*
- *Si $q > 0$, entonces $r > 0$, así que $r^2 < 2$. Luego tenemos $r^2 - q^2 = (r-q)(r+q) > 0$, y por lo tanto $q^2 < r^2 < 2$.*

Esto demuestra que en todo caso se tiene $q \in A$. Hemos demostrado que para $r \in A$ se tiene

$$q < r \Rightarrow q \in A.$$

(iii) Sea $r \in A$. Entonces existe $q \in A$ tal que $r < q$. En efecto, si $r \leq 0$ se puede tomar $q = 1$. Si $r > 0$, tenemos $r^2 < 2$. Tomando $q = r + \frac{1}{n}$, con $n \in \mathbb{N}$ tenemos

$$q^2 = r^2 + \frac{2r}{n} + \frac{1}{n^2} \leq r^2 + \frac{2r}{n} + \frac{1}{n} = r^2 + \frac{2r+1}{n}.$$

Para que q^2 sea menor que 2, basta que $r^2 + \dfrac{2r+1}{n} < 2$, y como $r^2 < 2$, eso es equivalente a

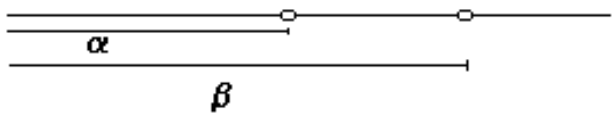
$$\frac{2r+1}{2-r^2} < n.$$

Tal n existe por arquimedianidad de $\mathbb{Q}$. Esto demuestra que el conjunto A es una cortadura (es decir, un número real), el cual más adelante llamaremos $\sqrt{2}$.

En el conjunto $\mathbb{R}$ se pueden definir las operaciones "suma" y "multiplicación", así como la relación de orden, y demostrar todas las propiedades que en teoría axiomática se conocen como "axiomas de campo y orden". Hacer ese trabajo con detalle no es nuestra intención. Nos conformaremos con indicar las definiciones y algunas de las demostraciones más simples, y remitimos al lector interesado en los detalles, a la literatura correspondiente.

B.2.1 Definición del orden

Cuando pensamos en un número real (cortadura), pensamos realmente en el punto geométrico que lo define. Ahora, si un punto está a la derecha de otro, es geométricamente claro que la cortadura que define el primero contiene a la que define el segundo. Es natural entonces definir la relación de orden en $\mathbb{R}$, como la relación de inclusión entre cortaduras.



Representación geométrica del orden en cortaduras.

Definimos entonces la relación de orden "$\leq$" así:

$$\alpha \leq \beta \Leftrightarrow \alpha \subseteq \beta.$$

Se le recomienda al lector demostrar que efectivamente esta relación es de orden. Es decir, es reflexiva, antisimétrica y transitiva. Cuando $\alpha \leq \beta$ y $\alpha \neq \beta$, escribimos $\alpha < \beta$, y decimos que α es menor que β.

Ejemplo B.2.2 *Sea α la cortadura dada por (B.1), y sea $\beta = \{p \in \mathbb{Q} : p < 3\} = \widehat{3}$. Entonces $\alpha < \beta$, pues $\alpha \subseteq \beta$ y $\alpha \neq \beta$ (verifíquelo).*

Ejemplo B.2.3 *Si $p_1, p_2 \in \mathbb{Q}$ se tiene*

$$\widehat{p}_1 < \widehat{p}_2 \Leftrightarrow p_1 < p_2.$$

La demostración se deja como ejercicio.

Nótese que la relación de inclusión definida en una familia arbitraria de conjuntos, no necesariamnte es de orden total, pero por las propiedades de cortaduras, en el conjunto $\mathbb{R}$ sí lo es.

Teorema B.1 *(Ley de tricotomía) Dados α y β en $\mathbb{R}$, se cumple una y sólo una de las siguientes alternativas:*

$$\alpha < \beta, \quad \alpha = \beta, \quad \beta < \alpha.$$

Demostración
En efecto, suponga que no se cumplen las dos primeras. En otras palabras, α no es subconjunto de β. Entonces existe $q \in \alpha$ tal que $q \notin \beta$. Dado $p \in \beta$, el lema B.1.1 (aplicado a β) demuestra que $p < q$, y por la definición de cortadura se sigue que $p \in \alpha$. Consecuentemente $\beta \subseteq \alpha$, y como $\beta \neq \alpha$ se sigue que $\beta < \alpha$. Por otro lado, es evidente que no pueden darse dos de estas posibilidades a la vez. □

Nota: El ejemplo anterior demuestra que el conjunto

$$\widehat{\mathbb{Q}} = \{\widehat{p} : p \in \mathbb{Q}\}$$

se comporta igual que $\mathbb{Q}$, al menos en cuanto al orden. Más adelante veremos que las operaciones que definiremos en $\mathbb{R}$ también se comportan, al verlas en $\widehat{\mathbb{Q}}$, como las operaciones usuales de $\mathbb{Q}$. Es natural entonces identificar cada racional p con su respectivo $\widehat{p}$, obteniendo así una identificación de $\mathbb{Q}$ con $\widehat{\mathbb{Q}}$. Sin embargo, para efectos de claridad, seguiremos usando $\widehat{p}$ por el resto de la construcción.

Ejemplo B.2.4 *Dado $\alpha \in \mathbb{R}$, es un buen ejercicio demostrar que*

$$\alpha = \{p \in \mathbb{Q} : \widehat{p} < \alpha\}\,.$$

En efecto, si $p \in \alpha$ se sigue por definición de cortaduras que $\widehat{p} \subseteq \alpha$ y $\widehat{p} \neq \alpha$, de donde $\widehat{p} < a$. Recíprocamente, si $\widehat{p} < \alpha$ tenemos $\widehat{p} \subseteq \alpha$ y $\widehat{p} \neq \alpha$. Tomando $q \in \alpha$ tal que $q \notin \widehat{p}$, se concluye que $q \geq p$, y por lo tanto $p \in \alpha$.
Con la identificación de p con $\widehat{p}$, este ejemplo demuestra que efectivamente, un número real es el conjunto formado por los racionales menores que este.

B.2.2 Operaciones en $\mathbb{R}$

Para completar la construcción de los números reales, debemos decir algo sobre la forma en que se definen las operaciones. Nos restringiremos a indicar las definiciones y esbozar algunas demostraciones, dejando el resto como ejercicio para el lector interesado en completarlos.

La suma

Queremos definir la operación suma de manera que sea compatible con la relación de orden. Esto es, debe cumplirse:

$$(a < \alpha \wedge b < \beta) \Rightarrow a + b < \alpha + \beta.$$

Tomando $a = \widehat{p}$ y $b = \widehat{q}$, esto es lo mismo que

$$(p \in \alpha \wedge q \in \beta) \Rightarrow p + q \in \alpha + \beta.$$

Esto sugiere que definamos:

$$\alpha + \beta = \{p + q : p \in \alpha \text{ y } q \in \beta\}.$$

Antes que todo debemos verificar que $\alpha + \beta$ es efectivamente una cortadura. Esto es, demostraremos que:

S1. (La suma es una operación cerrada) Para $\alpha, \beta \in \mathbb{R}$ se tiene $\alpha + \beta \in \mathbb{R}$.

Demostración

Verifiquemos las propiedades de cortaduras:

(i) Lógicamente tenemos $\alpha+\beta \subseteq \mathbb{Q}$. Además, como $\alpha \neq \emptyset$, existe $p \in \alpha$, y similarmente existe $q \in \beta$. Luego $p+q \in \alpha+\beta$ y por lo tanto $a+\beta \neq \emptyset$.
Para demostrar que $\alpha+\beta \neq \mathbb{Q}$, escojamos $r, s \in \mathbb{Q}$ tales que $r \notin \alpha$ y $s \notin \beta$. Dados todo $p \in \alpha$ y $q \in \beta$ se tiene $p < r$ y $q < s$, y por la compatibilidad de la suma con la relación de orden en $\mathbb{Q}$ se sigue que

$$p+q < r+s.$$

Esto demuestra que $r+s \notin \alpha+\beta$ y por lo tanto $\alpha+\beta \neq \mathbb{Q}$.

(ii) Sea $t \in \alpha+\beta$ y sea $r < t$. Tenemos $t = p+q$, con $p \in \alpha$ y $q \in \beta$. Luego

$$r = p + (r-p)\,,$$

donde $p \in \alpha$ y $r-p \in \beta$ (debido a que $r-p < q \in \beta$). Por lo tanto $r \in \alpha+\beta$.

(iii) Sea $t = p+q \in \alpha+\beta$. Como α y β son cortaduras, existen $p' \in \alpha$ y $q' \in \beta$ tales que $p < p'$ y $q < q'$. Luego $t' = p'+q' \in \alpha+\beta$ y $t = p+q < p'+q' = t'$. □

Las demostraciones de las siguiente propiedades se dejan de ejercicio al lector.

S2. (Conmutatividad de la suma) Para $\alpha, \beta \in \mathbb{R}$ se tiene $\alpha+\beta = \beta+\alpha$.

S3. (Asociatividad de la suma) Para $\alpha, \beta, \gamma \in \mathbb{R}$ se tiene $\alpha+(\beta+\gamma) = (\alpha+\beta)+\gamma$

S4. (Existencia del neutro) Existe $\widehat{0}$ en $\mathbb{R}$ tal que $\alpha+\widehat{0} = \alpha$, $\forall \alpha \in \mathbb{R}$.

Para la existencia del inverso, definimos

$$-\alpha = \{p \in \mathbb{Q} : -p \notin \alpha\}\,,$$

excepto cuando $\alpha \in \widehat{\mathbb{Q}}$. En este último caso se tiene $\alpha = \alpha_p$ para algún $p \in \mathbb{Q}$, y entonces $-\alpha$ se define como α_{-p}.

S5. (Existencia de inversos aditivos) Para cada $\alpha \in \mathbb{R}$, existe $-\alpha \in \mathbb{R}$ tal que $-\alpha+\alpha = \widehat{0}$. El elemento $-\alpha$ se llama el inverso aditivo de α.

En efecto, el caso $\alpha \in \widehat{\mathbb{Q}}$ es bastante directo y se deja como ejercicio. En el caso $\alpha \notin \widehat{\mathbb{Q}}$, debemos verificar primero que $-\alpha$ es una cortadura.

(i) Note que $-\alpha \neq \emptyset$ pues existe $q \notin \alpha$, lo que implica $-q \in -\alpha$. Además $-\alpha \neq \mathbb{Q}$ pues existe $q \in \alpha$, lo que implica $-q \notin -\alpha$.

(ii) Si $p \in -a$ y $q < p$, tenemos $-p \notin \alpha$ y $-p < -q$. Luego $-q \notin \alpha$, es decir $q \in -\alpha$.

(iii) Dado $p \in -\alpha$, por definición se tiene $-p \notin \alpha$. Luego, por el ejercicio 3 existe $r < -p$ tal que $r \notin \alpha$, y esto significa que $-r > p$ y $-r \in -\alpha$.

Ahora demostremos que $-\alpha + \alpha = \widehat{0}$.

Dado $t = p + q \in -\alpha + \alpha$, con $p \in -\alpha$ y $q \in \alpha$, tenemos $-p \notin \alpha$ y $q \in \alpha$, lo que implica $q < -p$. Luego $p + q < 0$, así que $t \in \widehat{0}$. Esto demuestra que $-\alpha + \alpha \subseteq \widehat{0}$.

Por otro lado, dado $r \in \widehat{0}$ tenemos $r < 0$. Escojamos $p \in \alpha$ y $q \notin \alpha$ cualesquiera. Por Arquimedianidad de $\mathbb{Q}$ existe $n \in \mathbb{N}$ tal que $p - rn > q$, y en particular $p - nr \notin \alpha$. Por el principio del buen orden, existe el menor natural n tal que $p - nr \notin \alpha$. Se sigue que $p_1 = -(p - nr) \in -\alpha$, mientras que $p_2 = p - (n-1)\, r \in \alpha$, y además $p_1 + p_2 = r$. Se concluye que $r \in -\alpha + \alpha$, y esto demuestra la otra inclusión. □

La multiplicación

La multiplicación se debe definir con más cuidado, pues el conjunto

$$\{pq : p \in \alpha \text{ y } q \in \beta\}$$

no es una cortadura (¿por qué?). Debe considerarse primero el caso $\alpha > \widehat{0}$ y $\beta > \widehat{0}$. En tal caso se define

$$\alpha \cdot \beta = \mathbb{Q}^- \cup \{pq : 0 \leq p \in \alpha,\ 0 \leq q \in \beta\}\,.$$

Nótese que $\alpha \cdot \beta > \widehat{0}$. En efecto, como $\alpha > \widehat{0}$ existe $p \in \alpha$ tal que $p > 0$, y como $\beta > \widehat{0}$ existe $q \in \beta$ tal que $q > 0$. Luego $pq > 0$ y $pq \in \alpha\beta$.

Al igual que en la suma, lo primero a demostrar es que $\alpha \cdot \beta$ es una cortadura, es decir que la multiplicación es cerrada en $\mathbb{R}$. Después se demuestran las demás propiedades (para el caso que α y β sean positivos), de manera similar a como se hizo con la suma. Finalmente se extiende la definición al caso en que alguno de los factores sea negativo, utilizando para ello la ley de signos. Por ejemplo, si $\alpha > 0$ y $\beta < 0$, se define

$$\alpha \cdot \beta = -\alpha \cdot (-\beta)\,,$$

y similarmente con los demás casos. La ley de signos se utiliza entonces como definición, lo mismo que la absorvencia del cero. Esto es, se define

$$\alpha \cdot \widehat{0} = \widehat{0},\ \forall \alpha \in \mathbb{R}.$$

Los detalles de este proceso los dejamos de lado, para no hacer la presentación muy tediosa. Invitamos al lector interesado, a intentar una demostración de estas propiedades, o consultar la bibliografía.

M1. Para $\alpha, \beta \in \mathbb{R}$ se tiene $\alpha \cdot \beta \in \mathbb{R}$.

M2. Para $\alpha, \beta \in \mathbb{R}$ se tiene $\alpha \cdot \beta = \beta \cdot \alpha$.

M3. Para $\alpha, \beta, \gamma \in \mathbb{R}$ se tiene $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$

M4. Existe $\widehat{1}$ en $\mathbb{R}$ tal que $\alpha \cdot \widehat{1} = \alpha$, $\forall \alpha \in \mathbb{R}$.

M5. Para cada $\alpha \in \mathbb{R}$, $\alpha \neq \widehat{0}$, existe $\alpha^{-1} \in \mathbb{R}$ tal que $\alpha \cdot \alpha^{-1} = \widehat{1}$. En efecto, para $\alpha > 0$ se define la cortadura α^{-1} como

$$\alpha^{-1} = \begin{cases} \mathbb{Q}^- \cup \left\{p \in \mathbb{Q}^+ : p^{-1} \notin \alpha\right\} & \text{si } \alpha \notin \widehat{\mathbb{Q}} \\ \alpha_{p^{-1}} & \text{si } \alpha \in \widehat{\mathbb{Q}} \end{cases}$$

Finalmente se demuestra la distributividad:

D. Para $\alpha, \beta, \gamma \in \mathbb{R}$ se tiene

$$\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma.$$

Las propiedades S1, ..., S5, M1, ..., M5, D definen los "axiomas" de campo. Los axiomas de orden se obtienen también de manera inmediata en este caso. Para esto definamos el conjunto de los números reales positivos:

$$P = \{\alpha \in \mathbb{R} : \alpha > 0\}.$$

Tenemos:

O1. Si $\alpha, \beta \in P$ entonces $\alpha + \beta \in P$.

En efecto, como $\alpha > 0$ y $\beta > 0$, existen racionales positivos $p \in \alpha$ y $q \in \beta$, y luego $0 < p + q \in \alpha + \beta$, lo que demuestra que $\alpha + \beta > 0$.

O2. Si $\alpha \in P$ y $\beta \in P$, entonces $\alpha \cdot \beta \in P$.

Esto es directo de la definición, como observamos arriba.

O3. Dado $\alpha \in \mathbb{R}$, se tiene que $\alpha \in P$ ó $-\alpha \in P$ (pero no ambos).

Esta propiedad es también bastante directa, y se deja como ejercicio.

B.3 Completitud de $\mathbb{R}$

Recordemos las definiciones relacionadas con este concepto.

Definición B.3.1 *Decimos $b \in \mathbb{R}$ es cota superior de un conjunto $A \subseteq \mathbb{R}$, si para cada $x \in A$ se tiene $x \leq b$. Si tal es el caso, se dice que A es acotado superiormente.*

Considerando entonces el conjunto B de cotas superiores de A, nos preguntamos si B tiene mínimo. Si tal es el caso, adicho mínimo le llamamos *extremo superior de A*, o supremo de A, y le denotamos $\sup A$. Definamos este concepto con más precisión:

Definición B.3.2 *Sea $A \subset \mathbb{R}$ acotado superiormente, $A \neq \emptyset$. Un elemento $\beta \in \mathbb{R}$ se llama el extremo superior (o supremo) de A, si es la menor de las cotas superiores. Dicho de otra forma, β es el extremo superior de A si satisface:*

1. *β es cota superior de A.*

2. *Para toda b cota superior de A, entonces $\beta \leq b$.*

En nuestra construcción, el llamado axioma del extremo superior es un teorema.

Teorema B.2 *(Axioma del extremo superior) Sea A un subconjunto no vacío de $\mathbb{R}$, acotado superiormente. Entonces existe el extremo superior de A.*

Demostración
Se define

$$\beta = \bigcup_{\alpha \in A} \alpha = \{p \in \mathbb{Q} : p \in \alpha \text{ para algún } \alpha \in A\},$$

y tomamos b cota superior de A. Entonces claramente se tiene $\beta \subseteq b$, y como $b \neq \mathbb{Q}$, se sigue que $\beta \neq \mathbb{Q}$. Además $\beta \neq \emptyset$, pues contiene a todos los $\alpha \in A$. Por lo tanto β satisface (i) en la definición de cortadura. Por otro lado, si $p \in \beta$ tenemos $p \in \alpha$ para algún $\alpha \in A$. Si q es un racional tal que $q < p$, se sigue que $q \in \alpha$, y por lo tanto $q \in \beta$. Esto demuestra que β también satisface (ii), en la definición de cortadura. Similarmente se demuestra que β satisface (iii), y por lo tanto es una cortadura, o sea que $\beta \in \mathbb{R}$.
Ahora, es obvio que $\alpha \leq \beta$ para cada $\alpha \in A$. Además, como $\beta \leq b$ y b es una cota superior arbitraria, se concluye que β es la menor cota superior de A. $\square$

Ejemplo B.3.1 ***(Intervalos)*** *Para cada $\alpha \in \mathbb{R}$, el conjunto $A = \{x \in \mathbb{R} : x < \alpha\}$ es acotado superiormente, y además $\alpha = \sup A$. En efecto, es evidente que α es cota superior. Además, si $\beta < \alpha$ entonces existe $p \in \alpha$ tal que $p \notin \beta$. Pero entonces, por las propiedades de cortaduras, $\beta < \widehat{p} < \alpha$, demostrando que β no es cota superior de A. Esto demuestra que α es la menor cota superior, y por lo tanto el supremo de A. El conjunto A se denota por $]-\infty, \alpha[$.*

Ejemplo B.3.2 *Para $\gamma \in \mathbb{R}$ considere el conjunto*

$$A = \{\widehat{p} : p \in \gamma\}.$$

De la demostración del teorema anterior se tiene que

$$\sup A = \bigcup_{\alpha \in A} a = \bigcup_{p \in \gamma} \widehat{p} = \gamma.$$

Si identificamos a p con $\widehat{p}$, esto pone de manifiesto el hecho que las cortaduras son precisamente los supremos de los conjuntos de racionales que las definen.

B.4 Ejercicios

1. Demuestre que para $p, q \in \mathbb{Q}$ se tiene
$$p < q \Leftrightarrow \widehat{p} < \widehat{q}.$$

2. Para $p \in \mathbb{Q}$ y $\alpha \in \mathbb{R}$, demuestre que
$$\widehat{p} < \alpha \Leftrightarrow p \in \alpha.$$

3. Demuestre que si A es una cortadura, entonces $\mathbb{Q} - A$ tiene mínimo si y solo si $A \in \widehat{\mathbb{Q}}$.

4. Demuestre que para cada $\alpha \in \mathbb{R}$ se tiene
$$-\alpha = \{p \in \mathbb{Q} : \text{existe } r < -p \text{ tal que } r \notin \alpha\}.$$

5. Demuestre que para $p \in \mathbb{Q}$ se tiene $\alpha_p^{-1} = \alpha_{p^{-1}}$.

6. Si $\alpha > 0$ demuestre que
$$\alpha^{-1} = \mathbb{Q}^- \cup \left\{p \in \mathbb{Q}^+ : \text{existe } q < p^{-1} \text{ tal que } q \notin \alpha\right\}.$$

7. (**Compatibilidad de la suma con la relación de orden**) Sean $\alpha, \beta, \gamma \in \mathbb{R}$. Entonces
$$\alpha \leq \beta \Leftrightarrow \alpha + \gamma \leq \beta + \gamma.$$

8. Para $\alpha, \beta \in \mathbb{R}$ se define $\alpha - \beta = \alpha + (-\beta)$. Demuestre que $\alpha > \beta \Leftrightarrow \alpha - \beta > 0$.

9. (**Compatibilidad de la multiplicación con la relación de orden**) Sean $\alpha, \beta, \gamma \in \mathbb{R}$, con $\gamma > 0$. Entonces
$$\alpha \leq \beta \Leftrightarrow \alpha\gamma \leq \beta\gamma.$$

10. Demuestre las propiedades S2, S3, S4.

11. Demuestre las propiedades M1...M5 y D para números reales positivos.

12. Defina explícitamente $\alpha \cdot \beta$ para α y β reales, considerando todos los casos.

13. Para $p, q \in \mathbb{Q}$ demuestre que $\widehat{p+q} = \widehat{p} + \widehat{q}$, y que $\widehat{pq} = \widehat{p} \cdot \widehat{q}$. Concluya que $\widehat{\mathbb{Q}}$ es una copia de $\mathbb{Q}$, en el sentido que la función
$$f : \mathbb{Q} \to \mathbb{R}$$
definida por $f(p) = \widehat{p}$, es un isomorfimos de campos.

Bibliografía

[1] Bartle, R.G. & D.R. Sherbert. *Introducción al Análisis Matemático de una Variable.* Limusa, 1996.

[2] Boyer, C. *Historia de la matemáticas*. Madrid, Alianza Universidad, 1986.

[3] Courant, R. & F. John. *Introduction to Calculus and Analysis.* Vol. I. Springer-Verlag, N.Y. 1989.

[4] Courant, R. & H. Robbins. *What is Mathematics?* New York, 1941.

[5] Dahan-Dalmedico, A. & J. Peiffer: *Une histoire des mathématiques*, Editions du Seuil, 1986.

[6] Dieudonnè, J. *Pour l'honneur de l'esprit Humain*. Hachette, 1987

[7] D'hombre, J.: *Nombre, mesure et continu. Èpistemologie et histoire*. Nathan, 1978

[8] Eves, H. *An Introduction to the History of Mathematics.* 3rd ed. NY 1961.

[9] Halmos, P.R. *Naive Set Theory.* Springer–Verlag, NY 1974.

[10] Hutton, R,L. *Number Systems. An Intuitive Approach.* Entex Educ. Publishers, 1971.

[11] Pedrick, G. *A first Course in Analysis.* Springer-Varlag, N.Y. 1994.

[12] Pownall, M.W. *Real Analysis. A first course with foundations.* WCB Publishers, 1994.

[13] Ruiz, Luisa. *La Noción de Función: Análisis Epistemológico y Didáctico.* Universidad de Jaén, España, 1998.

[14] Spivak, M. *calculus.* Editorial Reverté, Barcelona 1977.

[15] Sprecher, D.A. *Elements of Real Analysis.* Dover Pub. Inc. New York, 1970.

[16] Yakutia, M. *El Inf.* CAEM 1974.