Taller de Cálculo Avanzado

Notas de clase

Mariano Suárez-Álvarez

[°]Versión del 24 de agosto de 2023

CAPÍTULO 1

El cuerpo de los números reales

Nuestro objetivo en este curso es establecer las bases del análisis de las funciones reales y para ello, por supuesto, necesitaremos trabajar con números reales. El primer paso que daremos, entonces, será dar una descripción precisa de qué entendemos exactamente por *números reales*.

Esta no es una tarea fácil. A lo largo de casi 3000 años el problema de precisar qué es exactamente un número ha sido encarado de diversas maneras por filósofos, por matemáticos, por psicólogos, por lingüistas, por biólogos, por neurocientíficos… y no se puede decir que en todo ese tiempo y después de tanto esfuerzo toda esta gente haya llegado a ningún acuerdo — al menos, un acuerdo que sirva a nuestros fines! La forma en que saldremos de este laberinto milenario será hacia arriba. Siguiendo a David Hilbert, cambiaremos el problema: en lugar de tratar de describir *qué* son los números reales nos propondremos el objetivo un poco más modesto de describir *cómo* son. Dicho de otra forma: en lugar de tratar de describir qué son los números reales intentaremos encontrar criterios que nos permitan decidir, cuando los tengamos enfrente, que se trata de ellos — es decir, reconocerlos. Por supuesto, hacer esto no es lo mismo que lo que nos propusimos hacer originalmente: explicaremos más tarde por qué es de todas formas suficiente para nuestros fines.

Ahora bien: ¿qué significa describir *cómo* son los números reales? Siguiendo a Hilbert, entenderemos por esto describir, en primer lugar, *qué podemos hacer con ellos* y, en segundo lugar, *qué podemos esperar del resultado de hacerlo*. Así, esperamos poder realizar operaciones aritméticas con los números reales y compararlos — por ejemplo, poder decidir cuál es el más grande entre dos de ellos — entre muchas otras cosas. Por otro lado, necesitamos que esas operaciones y comparaciones tengan ciertas propiedades específicas, como que la suma sea una operación conmutativa.

En este primer capítulo nos dedicaremos a establecer un lenguaje preciso en el que podamos describir lo que queremos poder hacer con los números y las propiedades que esperamos tengan.

1.1. Cuerpos

Empezaremos por dar la definición de qué es un ***cuerpo***. Como la intención de esta definición es capturar la idea intuitiva de las operaciones aritméticas y sus propiedades — tal como las aprendimos de niños — todo debería resultar muy familiar al lector. De todas formas, y en vista de que nuestro objetivo es sentar bases formales para lo que queremos hacer, iremos presentando la definición por partes y en detalle.

1.1.1. Operaciones asociativas

Supongamos que tenemos un conjunto K y una operación binaria $\star$ definida en K o, lo que es lo mismo, una función $\star : K \times K \to K$.

Definición 1.1. Decimos que la operación $\star : K \times K \to K$ es ***asociativa*** si siempre que x, y y z son elementos de K se tiene que $x \star (y \star z) = (x \star y) \star z$.

Es fácil dar ejemplos de operaciones asociativas, porque las operaciones aritméticas elementales tienen esa propiedad.

Ejemplo 1.2. La operación $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ sobre el conjunto $\mathbb{N}$ de los enteros positivos dada por la suma ordinaria es asociativa, como aprendimos todos en la escuela primaria. Otra operación asociativa es la dada por la función

$$(x, y) \in \mathbb{Q} \times \mathbb{Q} \mapsto 17 \in \mathbb{Q}$$

que toma el valor 17 independientemente de cuáles sean sus argumentos, y otras — un poco más interesantes — son las funciones

$$(x, y) \in \mathbb{R} \times \mathbb{R} \mapsto x \in \mathbb{R}, \qquad (x, y) \in \mathbb{R} \times \mathbb{R} \mapsto \max\{x, y\} \in \mathbb{R}.$$

Por otro lado, no toda operación es asociativa — si ese fuera el caso la Definición 1.1 no tendría mucho interés!

Ejemplo 1.3. La función

$$\star : (x, y) \in \mathbb{N} \times \mathbb{N} \mapsto x^y \in \mathbb{N}$$

no es una operación asociativa sobre el conjunto $\mathbb{N}$: para verlo es suficiente observar que

$$3 \star (3 \star 3) = 3 \star 3^3 = 3 \star 27 = 3^{27} = 7\,625\,597\,484\,987$$

mientras que

$$(3 \star 3) \star 3 = 3^3 \star 3 = 27 \star 3 = 27^3 = 19\,683,$$

y que estos dos números son manifiestamente diferentes. Notemos que en este ejemplo no es cierto que $a \star (b \star c)$ sea diferente de $(a \star b) \star c$ para *toda* elección de a, b y c en $\mathbb{N}$, ya que, por ejemplo, $1 \star (1 \star 1) = (1 \star 1) \star 1$ y $2 \star (2 \star 2) = (2 \star 2) \star 2$.

Otro ejemplo familiar de una operación que no es asociativa es la resta: la función

$$\star : (x, y) \in \mathbb{Z} \mapsto x - y \in \mathbb{Z}$$

no es asociativa, ya que, por caso,

$$1 - (1 - 1) = 1 - 0 = 1 \neq -1 = 0 - 1 = (1 - 1) - 1.$$

Supongamos que $\star : K \times K \times K$ es una operación sobre un conjunto K, y sean x, y y z tres elementos de K. La expresión

$$x \star y \star z \tag{1.1}$$

no tiene sentido, ya que $\star$ es una operación binaria. Las que sí tienen sentido son las dos expresiones

$$x \star (y \star z), \qquad (x \star y) \star z, \tag{1.2}$$

que son las dos formas de poner paréntesis en (1.1) de manera que quede determinado el orden de las operaciones a realizar. Si la operación $\star$ es asociativa, entonces sabemos que estas dos expresiones denotan al mismo elemento de K: cuando ese es el caso, *hacemos la convención* de escribir $x \star y \star z$ al valor común de las dos expresiones.

Es importante no olvidar esto: cuando escribimos un producto con tres factores como $x \star y \star z$ con respecto a una operación asociativa, lo que estamos escribiendo es el resultado de evaluar la expresión que se obtiene poniendo paréntesis de manera de que el orden de las operaciones quede bien determinado — esto puede hacerse de dos maneras distintas, pero la condición de asociatividad implica que el resultado final que obtengamos evaluando cualquiera de las dos es independiente de cuál de las dos hayamos elegido. Al momento de evaluar la expresión $x \star y \star z$, claro, nos vemos forzados a elegir una de las expresiones de (1.2), ya que la operación $\star$ es binaria.

¿Qué ocurre si tenemos *cuatro* elementos de K? Si x, y, z y u son elementos de K, entonces, como antes, la expresión

$$x \star y \star z \star u$$

no tiene, en principio, ningún sentido, y si queremos darle alguno tenemos que insertar paréntesis para dejar en claro un orden específico en el que realizar las operaciones. A diferencia de lo que ocurre cuando tenemos tres factores, ahora tenemos *cinco* formas de hacerlo:

$$\begin{aligned} &((x \star y) \star z) \star u, \qquad (x \star (y \star z)) \star u, \qquad (x \star y) \star (z \star u), \\ &x \star ((y \star z) \star u), \qquad x \star (y \star (z \star u)). \end{aligned} \tag{1.3}$$

Si $\star$ es una operación cualquiera, no hay ninguna razón para pensar que estas cinco expresiones denotan algo siquiera parecido.

Ejemplo 1.4. Si en el conjunto $\mathbb{N}$ consideramos la operación

$$\star : (x, y) \mapsto 2^x 3^y \in \mathbb{N},$$

entonces las cinco expresiones

$$((1 \star 1) \star 1) \star 1, \quad (1 \star (1 \star 1)) \star 1, \quad (1 \star 1) \star (1 \star 1), \quad 1 \star ((1 \star 1) \star 1), \quad 1 \star (1 \star (1 \star 1))$$

denotan enteros distintos. Verificarlo directamente es un poco laborioso, de todas maneras: por ejemplo, el valor de la expresión $((1 \star 1) \star 1) \star 1$ es el entero

$$18\,831\,305\,206\,160\,042\,291\,507\,368\,269\,622\,999\,248\,307\,066\,333\,392\,103\,538\,688,$$

y el entero $1 \star (1 \star (1 \star 1))$ tiene 696 dígitos… Dejamos al lector la tarea de encontrar una prueba de esto que no requiera calcular explícitamente los valores de las cinco expresiones de arriba.

De todas formas, si suponemos que la operación $\star$ es asociativa, entonces podemos mostrar que las cinco expresiones listadas en (1.3) denotan el mismo valor. En efecto, es consecuencia de la condición de asociatividad que tenemos las siguientes igualdades:

$$\begin{aligned} &(\underline{x} \star (\underline{y} \star \underline{z})) \star u = ((\underline{x} \star \underline{y}) \star \underline{z}) \star u, && \underline{x} \star (\underline{(y \star z)} \star \underline{u}) = (\underline{x} \star \underline{(y \star z)}) \star \underline{u}, \\ &x \star (\underline{y} \star (\underline{z} \star \underline{u})) = x \star ((\underline{y} \star \underline{z}) \star \underline{u}), && \underline{(x \star y)} \star (\underline{z} \star \underline{u}) = (\underline{(x \star y)} \star \underline{z}) \star \underline{u}\,. \end{aligned}$$

Cada una de estas cuatro igualdades resulta de usar la igualdad $a \star (b \star c) = (a \star b) \star c$ garantizada por la condición de asociatividad reemplazando a, b y c por las expresiones que aparecen subrayadas en el lado izquierdo. Así, en la última tomamos $a = x \star y$, $b = z$ y $c = u$.

Esta observación — de que si la operación $\star$ es asociativa, entonces las cinco expresiones de (1.3) denotan el mismo valor — nos permite hacer, como antes, la convención de que cuando escribamos

$$x \star y \star z \star u$$

nos estaremos refiriendo a su valor común. En otras palabras, siempre que estemos operando con una operación asociativa, un producto de cuatro factores como este último denotará el resultado de evaluar la expresión que se obtiene insertando en la expresión paréntesis de alguna forma hasta determinar completamente el orden de las operaciones — podemos hacer esto porque, como dijimos, el resultado final no depende de la forma específica en que insertemos los paréntesis.

Por supuesto, la pregunta natural ahora es: ¿qué ocurre si tenemos *cinco* factores? Bueno, si x, y, z, u y v son elementos de K hay 14 formas de insertar paréntesis en la expresión

$$x \star y \star z \star u \star v \tag{1.4}$$

de manera que el orden de las operaciones quede completamente determinado:

$$
\begin{aligned}
&x \star (y \star (z \star (u \star v))), && x \star (y \star ((z \star u) \star v)),\\
&(x \star y) \star ((z \star u) \star v), && x \star ((y \star z) \star (u \star v)),\\
&x \star (((y \star z) \star u) \star v), && x \star ((((y \star z) \star u) \star v),\\
&(x \star y) \star ((z \star u) \star v), && (x \star (y \star z)) \star (u \star v),\\
&(x \star (y \star (z \star u))) \star v, && (x \star ((y \star z) \star u)) \star v,\\
&((x \star y) \star (z \star u)) \star v, && ((x \star y) \star z) \star (u \star v),\\
&((x \star (y \star z)) \star u) \star v, && (((x \star y) \star z) \star u) \star v.
\end{aligned}
$$

En general, si $\star$ es una operación cualquiera, estas expresiones pueden denotar elementos distintos de K — eso ocurre, de hecho, con la operación descripta en el Ejemplo 1.4 — pero si suponemos que la operación es asociativa entonces es posible mostrar que todas tienen el mismo valor. Como en los casos anteriores, hacemos la convención de denotar ese valor común por el producto (1.4).

Claro, ahora deberíamos preguntarnos qué ocurre cuando tenemos seis factores, y siete, y ocho… La respuesta es que siempre ocurre lo mismo: ese es el contenido del siguiente resultado, que podríamos llamar la *ley de asociatividad generalizada*.

Proposición 1.5. *Sea K un conjunto y sea $\star$ una operación binaria en K que es asociativa. Si n es un entero positivo y $x_1, x_2, \ldots, x_n$ son elementos de K, entonces todas las expresiones que se obtienen insertando paréntesis en el producto*

$$x_1 \star x_2 \star \cdots \star x_n \tag{1.5}$$

hasta determinar completamente el orden de las operaciones denotan el mismo elemento de K. □

En vista de esto, desde ahora haremos la convención de que siempre que escribamos un producto como el de (1.5) refiriéndonos a una operación asociativa $\star$ nos estaremos refiriendo al valor común de todas las expresiones que se obtienen de él insertando paréntesis hasta determinar completamente el orden de las operaciones. Que esto no produce ninguna ambigüedad es precisamente lo que afirma la proposición.

No probaremos aquí esta proposición, aunque su demostración no es especialmente difícil. Tampoco es trivial, de todas formas! No es posible verificar igualdad por igualdad como hicimos arriba en los casos en que el número n de factores es pequeño, ya que el número de expresiones a considerar crece muy rápidamente con n: cuando n es 20 hay 1 767 263 190 expresiones a considerar. La demostración de la proposición, entonces, requiere de una nueva idea.

1.1.2. Elementos neutros

Supongamos otra vez que K es un conjunto y que $\star : K \times K \to K$ es una operación binaria en K.

Definición 1.6. Un elemento e de K es ***neutro*** para la operación $\star$ si se tiene que

$$x \star e = x, \qquad e \star x = x$$

cualquiera sea x en K.

Así, el entero 0 es neutro para la operación + dada por la suma usual en el conjunto $\mathbb{Z}$ de los enteros, y el número 1 es neutro para la operación $\cdot$ dada por la multiplicación usual en el conjunto $\mathbb{Q}$ de los números racionales. Es importante observar que no toda operación admite algún elemento neutro: la suma usual + en el conjunto $\mathbb{N}$ de los enteros positivos no posee ninguno, por ejemplo. Por otro lado, una operación no puede nunca admitir más que *un* elemento neutro — ese es el contenido del siguiente resultado.

Proposición 1.7. *Sea K un conjunto y sea $\star$ una operación binaria en K. Si hay en K un elemento neutro para $\star$, entonces hay exactamente uno.*

Demostración. Si e y e' son dos elementos de K que son neutros para $\star$, entonces tenemos que

$$e = e \star e' = e'.$$

La primera de estas dos igualdades es consecuencia de que e' es un elemento neutro para $\star$, mientras que la segunda es consecuencia de que e lo es. □

Gracias a esta proposición, cada vez que tengamos una operación en un conjunto que admite un elemento neutro podremos hablar de «*el* elemento neutro» de esa operación, sin ninguna ambigüedad. La notación que usaremos para denotarlo, de todas formas, dependerá del contexto.

1.1.3. Elementos inversos

Como siempre, supongamos que tenemos un conjunto K y una operación binaria $\star : K \times K \to K$ sobre K. Haremos ahora además la hipótesis de que hay en K un elemento neutro para $\star$, al que escribiremos e.

Definición 1.8. Un elemento x de K es ***inversible*** con respecto a la operación $\star$ si existe otro elemento y en K tal que $x \star y = e$ e $y \star x = e$, y en ese caso decimos que este elemento y es un ***elemento inverso*** de x.

En el conjunto $\mathbb{Z}$ dotado de la operación + de la suma usual hay un elemento neutro, el cero 0,

y todo elemento de $\mathbb{Z}$ es inversible con respecto a $+$: en efecto, si x es un entero, entonces el entero opuesto $-x$ tiene la propiedad de que $x + (-x) = 0$ y $(-x) + x = 0$, así que, de acuerdo a la definición que acabamos de dar, este opuesto $-x$ es un elemento inverso de x con respecto a $+$. De manera similar, en el conjunto $(0, +\infty)$ de todos los números reales positivos la operación $\cdot$ de la multiplicación usual admite un elemento neutro, el número 1, y todo elemento de $(0, +\infty)$ es inversible con respecto a esa operación: si x es un elemento de $(0, +\infty)$, entonces el número $1/x$ es un elemento inverso de x con respecto a $\cdot$ ya que, por supuesto, $x \cdot 1/x = 1$ y $1/x \cdot x = 1$.

Por otro lado, podemos considerar al conjunto $\mathbb{Z}$ de todos los enteros dotado de la operación $\cdot$ de la multiplicación usual. El número 1 es claramente un elemento neutro para $\cdot$. El número 2, por su parte, no es inversible con respecto a esta operación: no hay ningún número entero $y \in \mathbb{Z}$ tal que $2 \cdot y = 1$. De hecho, los únicos elementos de $\mathbb{Z}$ que son inversibles con respecto a esta operación $\cdot$ son 1 y -1: hay en este ejemplo exactamente dos elementos inversibles.

Es fácil dar un ejemplo en el que hay uno solo: con respecto a la operación

$$\vee : (x, y) \in [0, +\infty) \times [0, +\infty) \mapsto \text{máx}\{x, y\} \in [0, +\infty),$$

sobre el conjunto $[0, +\infty)$ el número 0 es un elemento neutro y es el único elemento del conjunto que es inversible. Notemos que no puede no haber *ningún* elemento inversible en K, ya que el elemento neutro de K siempre es inversible.

De acuerdo a la definición de arriba, un elemento de K es inversible si posee algún inverso. En general puede ser que posea varios — daremos un ejemplo de esto más abajo en el Ejercicio 1.12 — pero el siguiente resultado nos dice que esto no ocurre si la operación es asociativa, lo que es afortunado porque este es el caso que más nos interesa.

Proposición 1.9. *Sea K un conjunto, y sea $\star : K \times K \to K$ una operación en K que admite un elemento neutro e. Si esta operación $\star$ es asociativa, entonces todo elemento de K que es inversible admite exactamente un elemento inverso.*

Demostración. Supongamos que la operación $\star$ es asociativa y que x es un elemento de K que es inversible. Si y e y' son dos elementos inversos de x con respecto a $\star$, entonces

$$\begin{aligned}
y &= y \star e && \text{porque } e \text{ es un elemento neutro para } \star \\
&= y \star (x \star y') && \text{porque } y' \text{ es un elemento inverso de } x \\
&= (y \star x) \star y' && \text{porque la operación } \star \text{ es asociativa} \\
&= e \star y' && \text{porque } y \text{ es un elemento inverso de } x \\
&= y' && \text{porque } e \text{ es un elemento neutro para } \star.
\end{aligned}$$

Esto prueba lo que afirma la proposición. □

Gracias a esta proposición, siempre que tengamos una operación asociativa sobre un conjunto que admite un elemento neutro y un elemento x del conjunto que es inversible podremos hablar sin ambigüedades de «*el* elemento inverso» de x y denotarlo de alguna manera específica. La notación que usamos para denotarlo, sin embargo, normalmente depende del contexto. Así, cuando trabajamos con el conjunto de los enteros $\mathbb{Z}$ dotado de la operación $+$ de suma usual, escribimos $-x$ al elemento inverso de un entero x, mientras que cuando trabajamos con el conjunto $\mathbb{Q}$ de los números racionales dotado de la operación $\cdot$ de multiplicación usual escribimos x^{-1} al elemento inverso de un elemento x de $\mathbb{Q}$ que es inversible.

El siguiente resultado nos da algunas propiedades básicas de los elementos inversibles con respecto a una operación asociativa que admite un elemento neutro.

Proposición 1.10. *Sea K un conjunto, y sea $\star : K \times K \to K$ una operación en K que admite un elemento neutro e.*

(*i*) *Si x es un elemento de K que es inversible y x' es un inverso de x, entonces x' es también inversible y x es un elemento inverso de x'.*

(*ii*) *Si x e y son dos elementos de K que son inversibles y x' e y' son sus elementos inversos, entonces el producto $x \star y$ también es inversible y su elemento inverso es $y' \star x'$.*

Demostración. (*i*) Sea x un elemento de K que es inversible y sea x' su elemento inverso. Esto significa que $x \star x' = e$ y $x' \star x = e$, y estas igualdades nos dicen que x' es inversible y que x un su elemento inverso.

(*ii*) Sean ahora x e y dos elementos de K que son inversibles y sean x' e y' sus correspondientes elementos inversos. Tenemos entonces que

$$\begin{aligned}
(x \star y) \star (y' \star x') &= x \star (y \star (y' \star x')) && \text{porque la operación } \star \text{ es asociativa} \\
&= x \star ((y \star y') \star x') && \text{por la misma razón} \\
&= x \star (e \star x') && \text{porque } y' \text{ es un elemento inverso de } x \\
&= x \star x' && \text{porque } e \text{ es un elemento neutro para } \star \\
&= e && \text{porque } x' \text{ es un elemento inverso de } x.
\end{aligned}$$

Por razones similares tenemos también que

$$\begin{aligned}
(y' \star x') \star (x \star y) &= y' \star (x' \star (x \star y)) \\
&= y' \star ((x' \star x) \star y) \\
&= y' \star (e \star y) \\
&= y' \star y \\
&= e,
\end{aligned}$$

y estas dos igualdades nos permiten concluir que el elemento $x \star y$ es inversible y que $y' \star x'$ es su elemento inverso, como afirma la proposición. □

Ejercicio 1.11. Pruebe que en la misma situación que en la proposición vale que

> *si x, y y z son tres elementos inversibles de K y x', y' y z' son sus elementos inversos, entonces el producto $x \star y \star z$ es inversible y $z' \star y' \star x'$ es su inverso.*

Generalice este resultado a productos de un número cualquiera de elementos inversibles y pruebe la afirmación correspondiente.

Ejercicio 1.12. Considere el conjunto $K \coloneqq \{1, 2, 3\}$ y la operación $\star : K \times K \to K$ cuya *tabla de multiplicar* es

$\star$	1	2	3
1	1	2	3
2	2	1	1
3	3	1	1

Muestre que hay un elemento neutro para $\star$ y que todo elemento de K es inversible, pero que hay elementos que tienen más de un elemento inverso. ¿Por qué esto no contradice la Proposición 1.9?

1.1.4. Operaciones conmutativas

Otra vez, supongamos que tenemos un conjunto K dotado de una operación binaria $\star : K \times K \to K$.

Definición 1.13. Decimos que la operación $\star$ es ***conmutativa*** si siempre que x e y son dos elementos de K se tiene que $x \star y = y \star x$.

Las operaciones dadas por la suma usual y el producto usual sobre el conjunto $\mathbb{Z}$ de los enteros son conmutativas, como lo es la operación

$$(x, y) \in \mathbb{R} \times \mathbb{R} \mapsto \max\{x, y\} \in \mathbb{R}.$$

En cambio, la operación

$$(x, y) \in [0,1] \times [0,1] \mapsto y \in [0,1]$$

sobre el conjunto $[0,1]$ no es conmutativa.

La condición de conmutatividad sobre la operación $\star$ pide que el valor de un producto de dos factores $x \star y$ no dependa del orden en que esos dos factores aparecen. ¿Qué ocurre si tenemos un producto de tres factores? Discutiremos esto bajo la hipótesis de que la operación $\star$ es asociativa, de manera que una expresión como $x \star y \star z$ tenga sentido.

Supongamos que x, y y z son tres elementos de K. De acuerdo a nuestras convenciones, el valor de la expresión $x \star y \star z$ es el de $(x \star y) \star z$. Si la operación $\star$ es conmutativa, entonces

$x \star y = y \star x$ y, por lo tanto, $(x \star y) \star z = (y \star x) \star z$. Esta última expresión tiene el mismo valor que $y \star x \star z$, y esto muestra que si $\star$ es asociativa y conmutativa, entonces

$$x \star y \star z = y \star y \star z \tag{1.6}$$

cualesquiera sean x, y y z en K. De manera similar, el valor de $x \star y \star z$ es el de $x \star (y \star z)$ y si la operación $\star$ es conmutativa tenemos que $y \star z = z \star y$, así que $x \star (y \star z) = x \star (z \star y)$ y, por lo tanto, vale que

$$x \star y \star z = x \star z \star y \tag{1.7}$$

cualesquiera sean x, y y z en K.

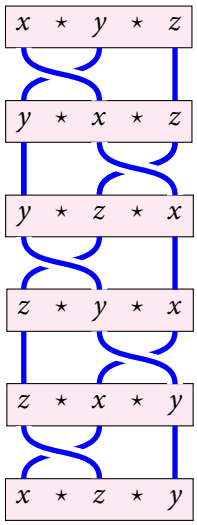
Ahora bien, usando las dos igualdades (1.6) y (1.7) podemos probar que las seis expresiones

$$x \star y \star z, \quad y \star x \star z, \quad y \star z \star x, \quad z \star y \star x, \quad z \star x \star y, \quad x \star z \star y$$

que pueden obtenerse permutando los factores en la primera de ellas tienen todas el mismo valor. En efecto, tenemos que

$$\begin{aligned} x \star y \star z &= y \star x \star z && \text{por (1.6)} \\ &= y \star z \star x && \text{por (1.7)} \\ &= z \star y \star x && \text{por (1.6)} \\ &= z \star x \star y && \text{por (1.7)} \\ &= x \star z \star y && \text{por (1.6).} \end{aligned}$$

Notemos que en cada paso de esta cadena de igualdades intercambiamos dos de los factores. Una forma de visualizar lo que hicimos es con el siguiente diagrama:



Un argumento similar sirve para probar que si x, y, z y u son cuatro elementos de K y la operación $\star$ es asociativa y conmutativa entonces las 24 expresiones

$$\begin{array}{llll} x\star y\star z\star u, & x\star y\star u\star z, & x\star u\star y\star z, & u\star x\star y\star z,\\ u\star x\star z\star y, & x\star u\star z\star y, & x\star z\star u\star y, & x\star z\star y\star u,\\ z\star x\star y\star u, & z\star x\star u\star y, & z\star u\star x\star y, & u\star z\star x\star y,\\ u\star z\star y\star x, & z\star u\star y\star x, & z\star y\star u\star x, & z\star y\star x\star u,\\ y\star z\star x\star u, & y\star z\star u\star x, & y\star u\star z\star x, & u\star y\star z\star x,\\ u\star y\star x\star z, & y\star u\star x\star z, & y\star x\star u\star z, & y\star x\star z\star u \end{array} \tag{1.8}$$

que se obtienen al permutar los factores de la primera de ellas denotan todas al mismo elemento de K. En efecto, gracias a la asociatividad y la conmutatividad de $\star$ tenemos que

$$x\star y\star z\star u=(x\star y)\star(z\star u)=(y\star x)\star(z\star u)=y\star x\star z\star u,$$
$$x\star y\star z\star u=x\star((y\star z)\star u)=x\star((z\star y)\star u)=x\star z\star y\star u,$$

y

$$x\star y\star z\star u=(x\star y)\star(z\star u)=(x\star y)\star(u\star z)=x\star y\star u\star z.$$

Estas tres cadenas de igualdades nos dicen que en un producto con cuatro factores podemos intercambiar dos factores *consecutivos* sin cambiar el valor de la expresión completa. Con esta observación a mano, basta ahora notar que podemos pasar de cualquiera de las 24 expresiones listadas en (1.8) a cualquier otra haciendo ese tipo de intercambios. Una forma de hacer esto está indicada en la Figura 1.1 de la página 14.

Por supuesto, razonando de la misma manera podemos probar la siguiente *ley de conmutatividad generalizada*:

Proposición 1.14. *Sea K un conjunto y sea $\star$ una operación binaria en K que es asociativa y conmutativa. Si n es un entero positivo y $x_1, x_2, \ldots, x_n$ son elementos de K, entonces el valor de la expresión*

$$x_1\star x_2\star\cdots\star x_n \tag{1.9}$$

no depende del orden de los n factores. □

No daremos aquí una demostración de este resultado. La idea que usamos para ver que es cierta cuando n es 3 o 4 ciertamente funciona para establecer la afirmación general[1].

[1] Observemos que no es necesario mostrar explícitamente cómo es posible ir de cada expresión obtenida permutando los factores del producto (1.9) a cualquier otra haciendo intercambios de factores consecutivos, sino que es suficiente con probar que es posible hacerlo. De todas formas, cualquiera sea el entero positivo n es posible construir de manera explícita un diagrama exactamente igual que el de la Figura 1.1. ¡Esto no es para nada evidente! Para construir esa figura usamos el algoritmo de Johnson [Joh63], Steinhaus [Ste64] y Trotter [Tro62], que da lo que se llama un *código de Gray* para las permutaciones, aunque hay muchos otros.

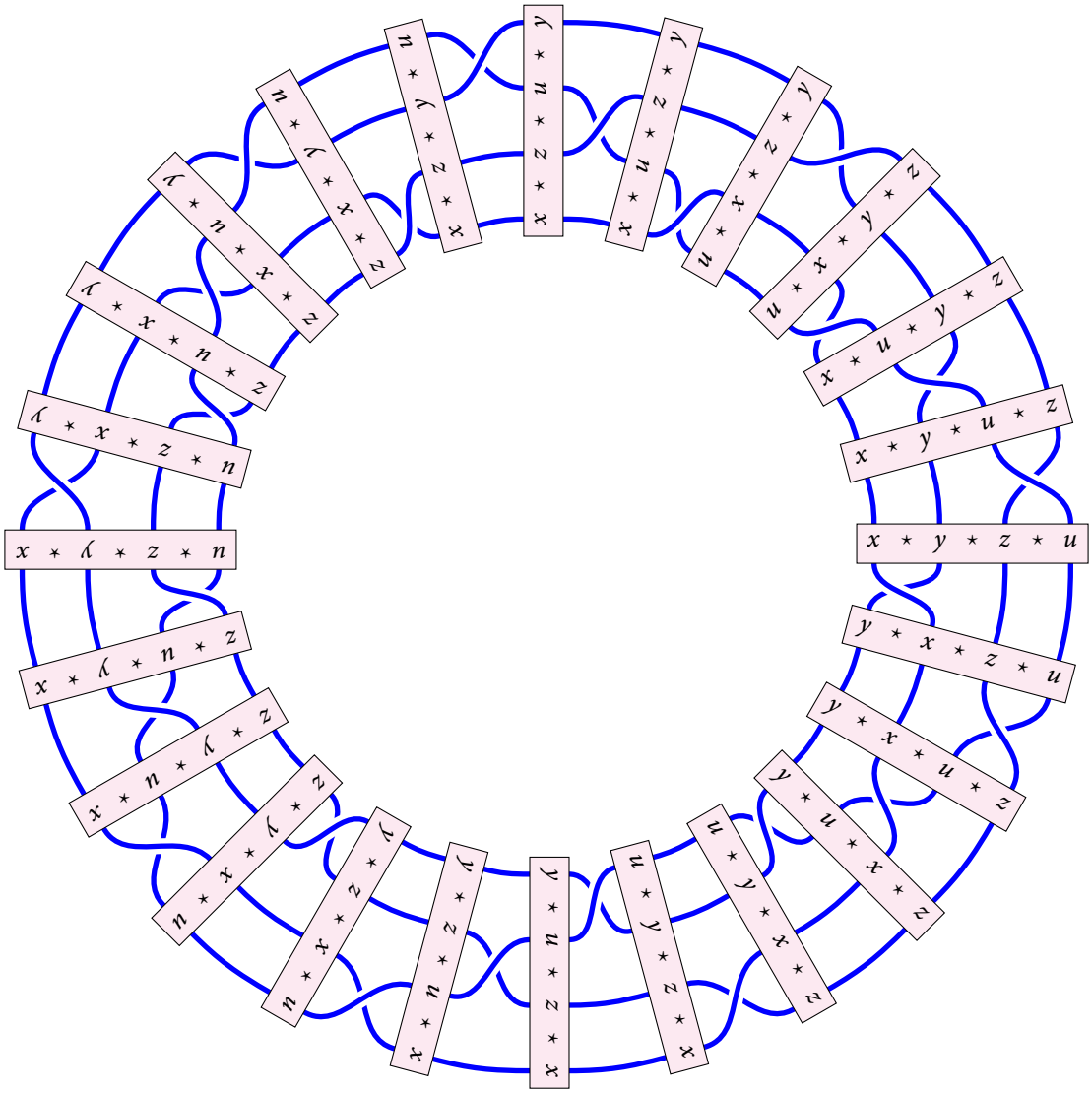


Figura 1.1. Los 24 posibles productos de cuatro factores.

1.1.5. Cuerpos

Podemos por fin dar la definición de qué es un cuerpo, ya que ya tenemos todas las partes necesarias a nuestra disposición.

Definición 1.15. Un ***cuerpo*** es un conjunto K dotado de dos operaciones binarias $+, \cdot : K \times K \to K$, la ***suma*** y el ***producto*** de K, que satisfacen las siguientes condiciones:

(*i*) La suma $+$ es asociativa y conmutativa, y admite un elemento neutro, al que escribimos 0 y llamamos el ***cero*** de K. Todo todo elemento x de K posee un elemento inverso, al que llamamos el ***elemento opuesto*** de x y escribimos $-x$.

(*ii*) El producto $\cdot$ es asociativo y conmutativo, y admite un elemento neutro, al que escribimos 1 y llamamos el ***uno*** de K. Todo elemento x de $K \setminus \{0\}$ posee un elemento inverso con respecto a $\cdot$, al que llamamos el ***elemento inverso*** de x y escribimos x^{-1}.

(*iii*) Siempre que x, y y z son elementos de K vale que

$$x \cdot (y + z) = x \cdot y + x \cdot z.$$

(*iv*) Es $0 \neq 1$.

La primera de estas condiciones se refiere solamente a la suma de K, mientras que la segunda lo hace solamente a su producto. La tercera de estas condiciones impone una cierta forma de compatibilidad entre esas dos operaciones: nos dice que el producto de K se «distribuye» sobre la suma de K, y nos referimos a ella como la ***ley de distributividad***. Finalmente, la cuarta condición sirve para eliminar ciertos casos triviales que no tienen interés, como veremos abajo.

Para simplificar el trabajo con cuerpos hacemos las siguientes convenciones de lenguaje y notación:

- Salvo en situaciones excepcionales, siempre escribiremos a las operaciones de suma y producto de un cuerpo usando los signos $+$ y $\cdot$. Esto nos permite decir simplemente cosas como «sea K un cuerpo» sin hacer mención alguna a las operaciones. De la misma forma, siempre escribiremos 0 y 1 a los elementos cero y uno de un cuerpo.
- Por otro lado, como dijimos en la definición, al elemento inverso de un elemento x de K con respecto a la suma $+$ lo escribiremos siempre $-x$ y, si x es distinto de 0, al elemento inverso de x con respecto al producto $\cdot$ lo escribiremos siempre x^{-1}. Usando estas notaciones, el resultado de la Proposición 1.10 nos dice que siempre que x e y son elementos de K se tiene que

$$-(-x) = x, \qquad -(x + y) = (-y) + (-x), \tag{1.10}$$

y que si x e y son distintos de 0, entonces $x \cdot y$ es inversible con respecto al producto y

$$(x^{-1})^{-1} = x, \qquad (x \cdot y)^{-1} = y^{-1} \cdot x^{-1}.$$

En mucho de lo que sigue usaremos estas igualdades sin mencionarlas explícitamente.

- Finalmente, cuando trabajamos con un cuerpo escribiremos generalmente $x - y$ y x/y en lugar de $x + (-y)$ y de $x \cdot y^{-1}$. Por supuesto, nos referimos a las operaciones $- : K \times K \to K$ y $/ : K \times (K \setminus \{0\}) \to K$ que obtenemos de esta forma como la ***substracción*** y la ***división*** de K.

El conjunto $\mathbb{Q}$ de los números racionales dotado de sus operaciones usuales + y · de suma y producto es un cuerpo. Para probarlo hay que verificar una a una las condiciones de la definición se satisface, y que esto es así es algo que aprendimos de niños. De la misma forma, el conjunto $\mathbb{R}$ de todos los números reales dotado de sus operaciones usuales de suma y producto es un cuerpo, y lo mismo es cierto del conjunto $\mathbb{C}$ de los números complejos dotado de sus operaciones usuales.

Estos ejemplos «familiares» de cuerpos no agotan ni de lejos la clase de los cuerpos que existen. Demos algunos ejemplos menos familiares para entrever las posibilidades.

Ejemplo 1.16. Consideremos el subconjunto

$$K = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$$

de $\mathbb{R}$ de todos los números reales que pueden escribirse en la forma $a + b\sqrt{2}$ con a y b en $\mathbb{Q}$. Si x e y son dos elementos de K, de manera que hay números racionales $a, b, c, d \in \mathbb{Q}$ tales que $x = a + b\sqrt{2}$ e $y = c + d\sqrt{2}$, entonces operando en $\mathbb{R}$ tenemos que

$$x + y = (a + c) + (b + d)\sqrt{2}, \qquad x \cdot y = (ac + 2bd) + (ad + bc)\sqrt{2},$$

y, como los números $a + c$, $b + d$, $ac + 2bd$ y $ad + bc$ son todos racionales, esto nos dice que $x + y$ y $x \cdot y$ son elementos de K. Podemos entonces definir dos funciones

$$\oplus : (x, y) \in K \times K \mapsto x + y \in K, \qquad \odot : (x, y) \in K \times K \mapsto x \cdot y \in K$$

usando las operaciones de $\mathbb{R}$. Mostraremos que el conjunto K dotado de estas dos operaciones $\oplus$ y $\odot$ como suma y producto es un cuerpo.

Que se satisfacen todas las condiciones de la parte *(i)* de la Definición 1.15 es consecuencia inmediata de que la operación + del cuerpo $\mathbb{R}$ las satisface. Así, si x, y y z son elementos cualesquiera de K tenemos que

$$\begin{aligned} x \oplus (y \oplus z) &= x + (y + z) && \text{por la definición de la operación } \oplus \\ &= (x + y) + z && \text{porque la operación + de } \mathbb{R} \text{ es asociativa} \\ &= (x \oplus y) \oplus z && \text{otra vez por la definición de la operación } \oplus \end{aligned}$$

y

$$\begin{aligned} x \oplus y &= x + y && \text{por la definición de la operación } \oplus \\ &= y + x && \text{porque la operación } + \text{ en } \mathbb{R} \text{ es conmutativa} \\ &= y \oplus x && \text{por la definición de la operación } \oplus, \end{aligned}$$

y esto nos dice que la operación $\oplus$ en K es asociativa y conmutativa. El número real 0 claramente pertenece a K, y si x es un elemento cualquiera de K tenemos que

$$\begin{aligned} 0 \oplus x &= 0 + x && \text{por la definición de la operación } \oplus \\ &= x && \text{porque 0 es un elemento neutro para } + \text{ en } \mathbb{R} \end{aligned}$$

y

$$\begin{aligned} x \oplus 0 &= x + 0 && \text{por la definición de la operación } \oplus \\ &= x && \text{porque 0 es un elemento neutro para } + \text{ en } \mathbb{R}, \end{aligned}$$

así que 0 es un elemento neutro para la operación $\oplus$ en K. Finalmente, si x es un elemento de K, de manera que hay dos números racionales a y b tales que $x = a + b\sqrt{2}$, entonces ciertamente $-a$ y $-b$ son números racionales, así que $y \coloneqq (-a) + (-b)\sqrt{2}$ es un elemento de K, y es

$$x \oplus y = \left(a + b\sqrt{2}\right) + \left((-a) + (-b)\sqrt{2}\right) = (a + (-a)) + (b + (-b))\sqrt{2} = 0$$

y

$$y \oplus x = \left((-a) + (-b)\sqrt{2}\right) + \left(a + b\sqrt{2}\right) = ((-a) + a) + ((-b) + b)\sqrt{2} = 0,$$

así que y es un elemento opuesto de x con respecto a $\oplus$. Con esto hemos verificado que K dotado de la operación $\oplus$ satisface la condición *(i)* de la Definición 1.15.

Exactamente de la misma forma podemos verificar que la operación $\odot$ satisface casi todas las partes de la condición *(ii)* de esa definición: que es asociativa, que es conmutativa, y que el número 1, que ciertamente pertenece al conjunto K, es un elemento neutro para $\odot$ — otra vez, todo esto es consecuencia de que la operación $\cdot$ de $\mathbb{R}$ satisface esas condiciones. Para terminar de verificar que K y $\odot$ satisfacen la condición *(ii)* tenemos que mostrar que todo elemento de $K \setminus \{0\}$ posee un inverso con respecto a $\odot$. Hagamos eso.

Sea x un elemento del conjunto $K \setminus \{0\}$. Como x pertenece a K, sabemos que hay dos números racionales a y b tales que $x = a + b\sqrt{2}$ y, como x no es nulo, alguno al menos de a o b es no nulo. El número $c \coloneqq a^2 - 2b^2$ es claramente racional. Supongamos por un momento que $c = 0$, de manera que $a^2 = 2b^2$. Si fuera $b = 0$, esta igualdad nos diría que también es $a = 0$, y esto es absurdo. Debe ser entonces $b \neq 0$ y, por lo tanto, $2 = a^2/b^2 = (a/b)^2$: como el número a/b es racional, esto es imposible, ya que sabemos que 2 no posee una raíz cuadrada racional. Esta contradicción nos permite concluir que el número c no es nulo y considerar el número real

$$y \coloneqq \frac{a}{c} + \left(-\frac{b}{c}\right)\sqrt{2}.$$

Como a/c y $-b/c$ son claramente números racionales, tenemos que y es un elemento de K. Por otro lado, usando la definición de la operación $\odot$ y calculando directamente vemos que

$$x \odot y = (a + b\sqrt{2}) \cdot \left(\frac{a}{c} + \left(-\frac{b}{c}\right)\sqrt{2}\right) = \frac{a^2 - 2b^2}{c} = 1$$

y, de manera similar, que $y \odot x = 1$. Podemos concluir entonces que y es un elemento inverso para x en K con respecto a la operación $\odot$, que, por lo tanto, el elemento x es inversible con respecto a esa operación y, con ello, que la operación $\odot$ satisface la condición *(ii)* de la Definición 1.15.

Que la condición *(iii)* se satisface en K es consecuencia de que se satisface en $\mathbb{R}$: usando dos veces las definiciones de $\oplus$ y $\odot$ y una el hecho de que $\mathbb{R}$ es un cuerpo podemos ver que si x, y y z son tres elementos de K, entonces

$$x \odot (y \oplus z) = x \cdot (y + z) = x \cdot y + x \cdot z = x \odot y \oplus x \odot z.$$

Finalmente, es claro que 0 y 1 son elementos distintos de K, simplemente porque se trata de elementos distintos de $\mathbb{R}$. Esto completa la verificación de que el conjunto K dotado de las operaciones de suma $\oplus$ y producto $\odot$ es un cuerpo. Casi siempre escribimos $\mathbb{Q}(\sqrt{2})$ al conjunto K, y + y · en lugar de $\oplus$ y $\odot$ cuando trabajamos con él.

La construcción que hicimos en este ejemplo puede modificarse para obtener muchos ejemplos de cuerpos — dejaremos dos instancias de esto como ejercicios para el lector.

Ejercicio 1.17. Sea d un número entero que no es el cuadrado de un número entero, y consideremos el subconjunto

$$K \coloneqq \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$$

de $\mathbb{C}$. Notemos que si d es positivo, este conjunto K está contenido en $\mathbb{R}$, pero que en general contiene números complejos que no son reales.

(a) Pruebe que si x e y son dos elementos de K, entonces su suma $x + y$ y su producto $x \cdot y$ calculados en $\mathbb{C}$ pertenecen a K, y que hay, por lo tanto, dos operaciones

$$\oplus : (x, y) \in K \times K \mapsto x + y \in K, \qquad \odot : (x, y) \in K \times K \mapsto x \cdot y \in K$$

en el conjunto K.

(b) Pruebe que el conjunto K dotado de estas dos operaciones como suma y como producto, respectivamente, es un cuerpo.

Normalmente escribimos $\mathbb{Q}(\sqrt{d})$ al cuerpo que construimos en este ejercicio.

Ejercicio 1.18. Escribamos α al número $\sqrt[3]{2}$ y consideremos el subconjunto

$$K \coloneqq \{a + b\alpha + c\alpha^2 : a, b, c \in \mathbb{Q}\}$$

de $\mathbb{R}$. Muestre, usando las mismas ideas que en el Ejemplo 1.16 y en el Ejercicio 1.17, que es posible hacer de K un cuerpo usando las operaciones de suma y producto que hereda de $\mathbb{R}$. La notación usual para este cuerpo es $\mathbb{Q}(\sqrt[3]{2})$.

Para construir los próximos dos ejemplos de cuerpos que queremos dar usaremos el siguiente resultado.

Proposición 1.19. *Sea K un conjunto, y sean $+, \cdot : K \times K \to K$ dos operaciones binarias sobre K que hacen de él un cuerpo.*

(*i*) *Para todo elemento x de K se tiene que $x \cdot 0 = 0$.*

(*ii*) *Si x, x' e y son elementos de K tales que $x + y = x' + y$, entonces $x = x'$.*

Demostración. (*i*) Si x es un elemento cualquiera de K, entonces

$$\begin{aligned}
x \cdot 0 &= x \cdot 0 + 0 && \text{porque 0 es neutro para la suma } + \\
&= x \cdot 0 + (x \cdot 0 + (-(x \cdot 0)) && \text{porque } -(x \cdot 0) \text{ es opuesto de } x \cdot 0 \\
&= (x \cdot 0 + x \cdot 0) + (-(x \cdot 0)) && \text{porque la suma } + \text{ es asociativa} \\
&= x \cdot (0 + 0) + (-(x \cdot 0)) && \text{por la ley distributiva} \\
&= x \cdot 0 + (-(x \cdot 0)) && \text{porque 0 es neutro para la suma } + \\
&= 0 && \text{porque } -(x \cdot 0) \text{ es opuesto de } x \cdot 0.
\end{aligned}$$

Esto prueba la primera afirmación de la proposición. Para ver la segunda, supongamos que x, x' e y son elementos de K tales que $x + y = x' + y'$, y calculemos que

$$\begin{aligned}
x &= x + 0 && \text{porque 0 es neutro para la suma } + \\
&= x + (y + (-y)) && \text{porque } -y \text{ es opuesto a } y \text{ con respecto a } + \\
&= (x + y) + (-y) && \text{porque la suma } + \text{ es asociativa} \\
&= (x' + y) + (-y) && \text{por la hipótesis de que } x + y = x' + y' \\
&= x' + (y + (-y)) && \text{porque la suma } + \text{ es asociativa} \\
&= x' + 0 && \text{porque } -y \text{ es opuesto a } y \text{ con respecto a } + \\
&= x' && \text{porque 0 es neutro para la suma } +.
\end{aligned}$$

□

Antes de dar nuestros ejemplos, notemos que usando esto podemos ver por qué incluimos en la Definición 1.15 la cuarta condición:

Proposición 1.20. *Sea K un conjunto, y sean $+, \cdot : K \times K \to K$ dos operaciones. Si estas dos operaciones satisfacen las tres primeras condiciones de la Definición 1.15 y es $0 = 1$, entonces K tiene exactamente un elemento.*

Demostración. En efecto, en esas condiciones, si x es un elemento cualquiera de K tenemos que

$$\begin{aligned} x &= 1 \cdot x && \text{porque 1 es neutro para el producto} \\ &= 0 \cdot x && \text{por la hipótesis hecha sobre } K \\ &= 0 && \text{por la primera parte de la Proposición 1.19,} \end{aligned}$$

y esto muestra que $K = \{0\}$. □

Esta proposición nos dice que la cuarta condición de la Definición 1.15 hace que no haya cuerpos de un solo elemento. La motivación para hacer eso es práctica: no hay nada muy interesante en considerar cuerpos con un sólo elemento. Por el contrario, los cuerpos con dos elementos son extremadamente útiles e interesantes — nuestro siguiente ejemplo los describe.

Ejemplo 1.21. Sea K un conjunto con *dos* elementos, y supongamos que tenemos dos operaciones binarias $+, \cdot : K \times K \to K$ que hacen de K un cuerpo. Tiene que haber en K un elemento cero y un elemento uno, y estos dos tienen que ser distintos: si los escribimos 0 y 1, respectivamente, entonces claramente es $K = \{0, 1\}$. Como el elemento 0 es neutro para la suma $+$, debe ser

$$0 + 0 = 0, \qquad 0 + 1 = 1, \qquad 1 + 0 = 1. \tag{1.11}$$

De manera similar, el elemento 1 es neutro para el producto $\cdot$, así que debe ser

$$1 \cdot 0 = 0, \qquad 0 \cdot 1 = 0, \qquad 1 \cdot 1 = 1.$$

El elemento 1 tiene que tener un opuesto: esto es, tiene que existir en K un elemento y tal que $1 + y = 0$ y $y + 1 = 0$, y de acuerdo a las dos últimas igualdades de (1.11) no puede ser que y sea igual a 0, así que no hay otra alternativa que que sea igual a 1. Esto nos dice que $1 + 1 = 0$. Por otro lado, sabemos de la primera parte de la Proposición 1.19 que $0 \cdot 0 = 0$. Toda esta información determina completamente las dos operaciones $+$ y $\cdot$, cuyas tablas tienen que ser necesariamente las siguientes:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Esto nos dice que *si es que hay un cuerpo con exactamente dos elementos*, entonces hay esencialmente uno solo, ya que sus elementos son necesariamente su cero y su uno y sus operaciones están completamente determinadas.

Es importante observar que esto no prueba, de todas formas, que exista algún cuerpo con exactamente dos elementos! De todas formas, sí existe. De hecho, si consideramos un conjunto K con dos elementos, a los que escribimos 0 y 1, y *definimos* sobre K dos operaciones $+, \cdot : K \times K \to K$ de manera que sus tablas sean precisamente las dos que encontramos arriba, entonces K es un cuerpo. Lamentablemente, la única forma de verificar esto en este punto — con la información que tenemos disponible — es verificar una a una las muchas condiciones implícitas en la Definición 1.15.

Hagamos primero una pequeña observación general que nos simplificará la verificación de que las dos operaciones son asociativas:

> *si L es un conjunto y $\star : L \times L \to L$ es una operación que admite un elemento neutro e, entonces siempre que x, y y z son tres elementos de K tales que $e \in \{x, y, z\}$ vale que $x \star (y \star z) = (x \star y) \star z$.*

Probarla es fácil: si x, y y z son elemento de L, entonces

- si $x = e$, es $x \star (y \star z) = e \star (y \star z) = y \star z = (e \star y) \star z = (x \star y) \star z$,
- si $y = e$, es $x \star (y \star z) = x \star (e \star z) = x \star z = (x \star e) \star z = (x \star y) \star z$,
- y si $z = e$, es $x \star (y \star z) = x \star (y \star e) = x \star y = (x \star y) \star e = (x \star y) \star z$.

Probemos ahora que el conjunto K dotado de las operaciones descriptas arriba es un cuerpo.

- Mirando la tabla se hace evidente que 0 es un elemento neutro para la operación $+$. Queremos ver que esta operación es asociativa, y para ello tenemos que mostrar que $x + (y + z) = (x + y) + z$ cualesquiera sean x, y y z en K. Nuestra observación implica que esta igualdad vale si alguno de los tres elementos es igual a 0, así que es suficiente considerar el caso en el que ninguno de los tres lo es, esto es, el caso en el que $x = y = z = 1$. Podemos calcular en ese caso que

  $$1 + (1 + 1) = 1 + 0 = 1 = 0 + 1 = (1 + 1) + 1.$$

  La operación $+$ es, por lo tanto, asociativa. Para ver que también es conmutativa es suficiente con observar que su tabla es simétrica con respecto a su diagonal principal. Finalmente, como $0 + 0 = 0$ y $1 + 1 = 0$, los elementos 0 y 1 tienen inversos con respecto a $+$, y estos son respectivamente, 0 y 1. Concluimos así que la primera condición de la Definición 1.15 se satisface.
- Otra vez, viendo la tabla de la operación $\cdot$ es claro que 1 es un elemento neutro para $\cdot$ y que $\cdot$ es una operación conmutativa y, gracias a la observación que hicimos arriba, para ver que se trata de una operación asociativa es suficiente con calcular que

  $$0 \cdot (0 \cdot 0) = 0 \cdot 0 = (0 \cdot 0) \cdot 0.$$

  El único elemento de K distinto de 0 es 1, que es el elemento neutro para la operación $\cdot$, así que ciertamente es inversible con respecto a esa operación. Esto prueba que la segunda condición de la definición se cumple.

- Tenemos que probar ahora que se satisface la ley distributiva en K, esto es, que siempre que x, y y z son elementos de K vale que $x \cdot (y + z) = x \cdot y + x \cdot z$. Ahora bien, si el elemento x es 0, entonces

$$x \cdot (y + z) = 0 \cdot (y + z) = 0 = 0 + 0 = 0 \cdot y + 0 \cdot z = x \cdot y + x \cdot z$$

  así que la igualdad vale en ese caso. Si, en cambio, es $x = 1$, entonces

$$x \cdot (y + z) = 1 \cdot (y + z) = y + z = 1 \cdot y + 1 \cdot z = x \cdot y + x \cdot z.$$

- Finalmente, es evidente que en K los elementos 0 y 1 son distintos.

Esto prueba que, como dijimos, K dotado de las dos operaciones descriptas arriba es un cuerpo con exactamente dos elementos.

Razonando de manera similar podemos describir los cuerpos de tres elementos.

Ejemplo 1.22. Supongamos ahora que K es, con respecto a dos operaciones $+, \cdot : K \times K \to K$ un cuerpo y que tiene exactamente *tres* elementos. De acuerdo a la Definición 1.15, hay en K un elemento cero 0 y un elemento uno 1, y estos dos elementos son distintos. Como K tiene tres elementos, hay entonces en K un tercer elemento distinto de 0 y de 1, al que escribiremos α, y es $K = \{0, 1, \alpha\}$. Nuestro objetivo es determinar, si es que esto es posible, las dos operaciones $+$ y $\cdot$.

Como el cero 0 es un elemento neutro para la suma $+$, la tabla de esta operación tiene que tener las siguientes entradas:

$+$	0	1	α
0	0	1	α
1	1		
α	α		

¿Qué valor tiene la expresión $1 + \alpha$? No puede ser igual a 1, porque en ese caso tendríamos que

$$1 + \alpha = 1 = 1 + 0,$$

y usando la segunda parte de la Proposición 1.19 podríamos concluir que $\alpha = 0$, lo que es absurdo. De manera similar, el valor de $1 + \alpha$ no puede ser α, ya que en ese caso tendríamos que

$$\alpha + 1 = 1 + \alpha = \alpha = \alpha + 0$$

y usando la misma proposición podríamos concluir que $1 = 0$, lo que otra vez es absurdo. Vemos así que necesariamente debe ser $1 + \alpha = 0$ y, como la suma $+$ es conmutativa, también $\alpha + 1 = 0$. La

tabla de la suma es entonces de la forma

$+$	0	1	α
0	0	1	α
1	1		0
α	α	0	

¿Qué valor tiene $1+1$? Si fuera 1, tendríamos que $1+1=1=1+0$ y, por lo tanto, gracias a la segunda parte de la Proposición 1.19, que $1=0$, lo que no es cierto, y si fuera 0 tendríamos que $1+1=0=1+\alpha$, de manera que $1=\alpha$, lo que tampoco es cierto: debe ser, entonces $1+1=\alpha$. De manera similar, el valor de $\alpha+\alpha$ no es α, ya que en ese caso tendríamos que $\alpha+\alpha=\alpha=\alpha+0$ y, por lo tanto, que $\alpha=0$, y tampoco es 0, porque en ese caso sería $\alpha+\alpha=0=\alpha+1$ y, por lo tanto, que $\alpha=1$. Juntando todo, vemos que la tabla de la suma $+$ está completamente determinada: es necesariamente

$+$	0	1	α
0	0	1	α
1	1	α	0
α	α	0	1

¿Qué podemos decir de la multiplicación? De acuerdo a la primera parte de la Proposición 1.19, es $x\cdot 0=0$ y $0\cdot x=0$ para todo $x\in K$, y el elemento 1 es neutro para el producto $\cdot$. Esto determina todas las entradas de la tabla de multiplicar de K salvo por una: debe ser

$\cdot$	0	1	α
0	0	0	0
1	0	1	α
α	0	α	

Si fuera $\alpha\cdot\alpha=0$, tendríamos que

$$
\begin{aligned}
\alpha &= \alpha\cdot 1 && \text{porque 1 es neutro para el producto}\\
&= \alpha\cdot 1+0 && \text{porque 0 es neutro para la suma}\\
&= \alpha\cdot 1+\alpha\cdot\alpha && \text{por la hipótesis de que } \alpha\cdot\alpha=0\\
&= \alpha\cdot(1+\alpha) && \text{por la ley distributiva}\\
&= \alpha\cdot 0 && \text{porque sabemos que } 1+\alpha=0\\
&= 0, && \text{por la primera parte de la Proposición 1.19,}
\end{aligned}
$$

lo que es absurdo. Por otro lado, si fuera $\alpha \cdot \alpha = \alpha$, tendríamos que

$$\begin{aligned}
\alpha &= \alpha \cdot 1 && \text{porque 1 es neutro para el producto} \\
&= \alpha \cdot (\alpha \cdot \alpha^{-1}) && \text{porque } \alpha^{-1} \text{ es inverso de } \alpha \\
&= (\alpha \cdot \alpha) \cdot \alpha^{-1} && \text{porque el producto es asociativo} \\
&= \alpha \cdot \alpha^{-1} && \text{por la hipótesis de que } \alpha \cdot \alpha = \alpha \\
&= 1 && \text{porque } \alpha^{-1} \text{ es inverso de } \alpha,
\end{aligned}$$

y esto es otra vez imposible. Debe ser entonces $\alpha \cdot \alpha = 1$. Vemos así que la tabla de la multiplicación $\cdot$ también está completamente determinada: debe ser necesariamente la siguiente.

$\cdot$	0	1	α
0	0	0	0
1	0	1	α
α	0	α	1

Exactamente de la misma forma que en el Ejemplo 1.21, este razonamiento nos dice que si es que existe algún cuerpo con tres elementos, entonces hay esencialmente uno solo, ya que sus operaciones quedan completamente determinadas por las condiciones de la Definición 1.15. De la misma forma que allí, también, todo esto que hemos hecho no prueba que existe algún cuerpo con tres elementos. Para hacer esto es suficiente, de todas maneras, verificar que si usamos las dos tablas que acabamos de encontrar para *definir* operaciones de suma y producto en un conjunto de tres elementos efectivamente obtenemos un cuerpo. Dejamos esta tarea al lector.

Ejercicio 1.23. Muestre que existen cuerpos con cuatro elementos y que esencialmente hay uno solo, en el mismo sentido que en los dos ejemplos anteriores.

Observación 1.24. Es posible probar que

> *el cardinal de un cuerpo finito es de la forma p^r con p un número primo y r un entero positivo*

y que, más aún,

> *si p es un número primo y r es un entero positivo, entonces existe un cuerpo finito de cardinal p^r y, de hecho, esencialmente uno solo.*

Escribimos a ese cuerpo $\mathbb{F}_{p^r}$ o $\mathsf{GF}(p^r)$ y lo llamamos el ***cuerpo de Galois*** de orden p^r, porque este tipo de cuerpos fue considerado por primera vez por Évariste Galois [BA62]. Los cuerpos descriptos en los Ejemplos 1.21 y 1.22 y en Ejercicio 1.23 son, por lo tanto, los cuerpos de Galois $\mathbb{F}_2$, $\mathbb{F}_3$ y $\mathbb{F}_4$.

Como dijimos, el conjunto $\mathbb{R}$ de los números reales dotado de sus operaciones usuales de suma y producto es un cuerpo. Esto, de todas maneras, no lo caracteriza ni mucho menos: esto es claro en vista de los ejemplos que acabamos de ver de cuerpos que son distintos de $\mathbb{R}$. Necesitamos entonces imponer condiciones más estrictas que la de ser simplemente un cuerpo si queremos encontrar una caracterización de $\mathbb{R}$. Daremos un paso más en esta dirección en la siguiente sección.

1.2. Cuerpos ordenados

Recordemos la siguiente definición.

Definición 1.25. Sea X un conjunto. Una relación $R \subseteq X \times X$ sobre el conjunto X es una ***relación de orden*** si satisface las siguientes tres condiciones.

- Es *reflexiva*: para cada $x \in X$ se tiene que xRx.
- Es *transitiva*: si x, y y z son elementos de X tales que xRy e yRz, entonces también xRz.
- Es *antisimétrica*: si x e y son elementos de X tales que xRy e yRx, entonces es $x = y$.

Si además se cumple la siguiente condición, entonces decimos que es una ***relación de orden total***:

- Cada vez que x e y son elementos de X se tiene que xRy o yRx.

Si dos elementos x e y de X son tales que xRy o yRx decimos que son ***comparables*** con respecto a R, y usando este lenguaje podemos decir que una relación de orden en X es total si todos los elementos de X son comparables con respecto a R.

Cuando tenemos un conjunto X dotado de una relación de orden que escribimos $\leq$, normalmente escribimos $<$ a la relación en X tal que

$$x < y \iff x \leq y \wedge x \neq y,$$

y la llamamos la relación de ***orden estricto*** asociada a $\leq$. Es fácil verificar que esta relación satisface las siguientes condiciones:

- Es ***irreflexiva***: para todo x de X no vale que $x < x$.
- Es ***asimétrica***: si x e y son elementos de X tales que $x < y$, entonces no vale que $y < x$.
- Es ***transitiva***: si x, y y z son elementos de X tales que $x < y$ e $y < z$, entonces también $x < z$.

Ejercicio 1.26. Pruebe en detalle que estas tres condiciones se satisfacen.

Las relaciones $\leq$ y $<$ son transitivas, y además tienen la siguiente propiedad útil:

Proposición 1.27. *Sea X un conjunto, sea $\leq$ una relación de orden total sobre X, y sea $<$ la correspondiente relación de orden estricto. Si x, y y z son elementos de K, entonces*

$$x < y \wedge y \leq z \implies x < z, \qquad x \leq y \wedge y < z \implies x < z,$$

Demostración. Supongamos que $x < y$ e $y \leq z$. Como es $x \leq y$, la transitividad de $\leq$ implica que $x \leq z$. Ahora bien, si fuera $x = z$ tendríamos que $x < y$ y que $y \leq z$, lo que es absurdo, así que debe ser, de hecho, $x < z$. Esto prueba la primera implicación del enunciado, y la segunda puede probarse de exactamente la misma forma. □

Es fácil dar ejemplos de relaciones de orden. La relación de orden usual $\leq$ en el conjunto $\mathbb{N}$ es una relación de orden total. Las relaciones de orden usuales en los conjuntos $\mathbb{Z}$, $\mathbb{Q}$, y $\mathbb{R}$ también lo son. La relación $|$ de divisibilidad en $\mathbb{N}$, que para cada x e y en $\mathbb{Z}$ satisface la condición

$$x \mid y \iff x \text{ divide a } y,$$

es una relación de orden sobre $\mathbb{N}$ que no es total: por ejemplo, tenemos que $2 \nmid 3$ y $3 \nmid 2$. De manera similar, la relación R sobre el conjunto $\mathbb{R}^2$ que para cada par de elementos (x, y) y (x', y') de $\mathbb{R}^2$ satisface la condición

$$(x, y)\ R\ (x', y') \iff x \leq x' \wedge y \leq y'$$

es una relación de orden sobre $\mathbb{R}^2$ que no es total: por ejemplo, los elementos $(1, 0)$ y $(0, 1)$ no son comparables con respecto a R.

La razón por la que nos interesan aquí las relaciones de orden es que nos permiten hacer la siguiente definición:

Definición 1.28. Sea K un cuerpo. Una relación de orden $\leq$ sobre K hace de K un ***cuerpo ordenado*** si es total y se satisfacen las siguientes condiciones:

(*i*) Si x, y y z son elementos de K tales que $x \leq y$, entonces $x + z \leq y + z$.

(*ii*) Si x e y son elementos de K tales que $0 < x$ y $0 < y$, entonces también $0 < x \cdot y$.

Las relaciones de orden usuales sobre los conjuntos $\mathbb{Q}$ y $\mathbb{R}$ hacen de esos cuerpos cuerpos ordenados. El cuerpo $\mathbb{Q}(\sqrt{2})$ del Ejemplo 1.16 está contenido en $\mathbb{R}$, así que podemos considerar en él la relación de orden $\leq$ evidente: con respecto a ella es también un cuerpo ordenado.

Ejercicio 1.29. Muestre que un elemento de $\mathbb{Q}(\sqrt{2})$ puede escribirse en la forma $a + b\sqrt{2}$ con a y b dos números racionales de exactamente una forma y, usando esto, que hay una relación de

orden $\leq$ sobre el conjunto $\mathbb{Q}(\sqrt{2})$ tal que

$$a + b\sqrt{2} \leq c + d\sqrt{2} \iff a - b\sqrt{2} \leq c - d\sqrt{2}$$

que hace del cuerpo $\mathbb{Q}(\sqrt{2})$ un cuerpo ordenado. Esta relación de orden es distinta de la que este conjunto hereda de $\mathbb{R}$, y esto muestra que un cuerpo puede admitir más de un orden con respecto al cual sea un cuerpo ordenado.

Este ejemplo muestra, como dijimos, que hay cuerpos que pueden ordenarse de muchas formas. Hay, por otro lado, cuerpos que no pueden ordenarse de ninguna. Un ejemplo de esto es el cuerpo de los números complejos:

Proposición 1.30. *No hay ninguna relación de orden sobre el cuerpo $\mathbb{C}$ de los números complejos que haga de él un cuerpo ordenado.*

Demostración. Supongamos que $\leq$ es una relación de orden sobre el conjunto $\mathbb{C}$ que hace de él un cuerpo ordenado. Como 0 e i son elementos distintos de $\mathbb{C}$, debe ser o bien $0 < i$ o bien $i < 0$.

Supongamos que es $0 < i$. Usando la segunda condición de la Definición 1.28 vemos que $0 < i \cdot i = -1$ y, usándola una vez más, que $0 < (-1) \cdot (-1) = 1$. Por otro lado, como $0 < -1$, de la primera condición de la definición tenemos que $1 = 0 + 1 \leq (-1) + 1 = 0$ y, por lo tanto, que simultáneamente es $0 < 1$ y $1 \leq 0$, lo que es absurdo.

Debe ser entonces $i < 0$, así que $0 = i + (-i) \leq 0 + (-i) = -i$ de acuerdo a la primera condición. Como $0 \neq -i$, es de hecho $0 < -i$ y la segunda condición implica entonces que $0 < (-i) \cdot (-i) = -1$. A partir de esta desigualdad la primera condición nos permite deducir que que $1 = 0 + 1 \leq (-1) + 1 = 0$, mientras que la segunda nos dice que $0 < (-1) \cdot (-1) = 1$. Otra vez tenemos que $1 \leq 0$ y $0 < 1$ al mismo tiempo, lo que es imposible.

En cualquier caso llegamos a una contradicción, y esto proviene de haber supuesto que hay en $\mathbb{C}$ una relación de orden que hace de él un cuerpo ordenado. Esto debe ser, por lo tanto, falso, y la proposición verdadera. □

Una familia importante de cuerpos que no pueden ordenarse es la de los cuerpos finitos. Esto es consecuencia del siguiente resultado:

Proposición 1.31. *Un cuerpo ordenado es infinito.*

Demostración. Supongamos que K es un cuerpo finito y que $\leq$ es una relación de orden sobre K que hace de él un cuerpo ordenado. Los elementos 0 y 1 de K son distintos, así que o bien $0 < 1$ o bien $1 < 0$, y en este segundo caso tenemos que $0 = 1 + (-1) \leq 0 + (-1) = -1$. Más aún, en este último caso es $0 \neq -1$, ya que de lo contrario tendríamos que $0 = 1 + (-1) = 1 + 0 = 1$, así que $0 < -1$.

Vemos así que hay un elemento x de K tal que $0 < x$.

Consideremos la sucesión $(a_n)_{n\geq 1}$ de elementos de K que tiene $a_1 = x$ y $a_n = x + a_{n-1}$ para cada $n \in \mathbb{N}$ tal que $n > 1$, de manera que

$$a_1 = x, \qquad a_2 = x + x, \qquad a_3 = x + x + x, \qquad a_4 = x + x + x + x, \qquad \dots$$

Como el conjunto K es finito, no puede ser que todos los elementos de la sucesión $(a_n)_{n\geq 1}$ sean distintos y existe, por lo tanto, dos enteros positivos r y s tales que $r < s$ y $a_r = a_s$.

Afirmamos que

$$\textit{para todo } i \in \mathbb{N} \textit{ vale que } a_r < a_{r+i}. \tag{1.12}$$

Que esto es cierto cuando $i = 1$ es claro: como $0 < x$, la primera condición de la Definición 1.28 implica que $a_r = a_r + 0 \leq a_r + x = a_{r+1}$, y debe ser $a_r < a_{r+1}$, ya que en caso contrario tendríamos que $a_r + 0 = a_r = a_{r+1} = a_r + x$ y, de acuerdo a la segunda parte de la Proposición 1.19, que $x = 0$. Por otro lado, si $i \in \mathbb{N}$ es tal que vale que $a_r < a_{r+i}$, entonces también tenemos que

$$a_r < a_{r+i} = a_{r+i} + 0 \leq a_{r+i} + x = a_{r+i+1},$$

gracias a la primera condición de la Definición 1.28, y, de acuerdo a la Proposición 1.27, esto implica que $a_r < a_{r+i+1}$. Nuestra afirmación sigue entonces por inducción.

Ahora bien, como $s - r \in \mathbb{N}$, esa afirmación (1.12) nos dice que $a_r < a_{r+(s-r)} = a_s$, y esto es absurdo en vista de la forma en que elegimos los enteros r y s. Esto prueba la proposición. □

El cuerpo $\mathbb{R}$ de los números reales es un cuerpo ordenado con respecto a su relación de orden usual, y acabamos de mostrar que no todo cuerpo puede ordenarse. Esto nos dice que la condición de ser un cuerpo ordenado nos permite distinguir a $\mathbb{R}$ de otros cuerpos. Por supuesto, no lo distingue de todos — por ejemplo, los cuerpos $\mathbb{Q}$ o $\mathbb{Q}(\sqrt{2})$ son también cuerpos ordenados con respecto a sus órdenes usuales. En la próxima sección mejoraremos esta situación.

1.3. Completitud

Supongamos que tenemos un conjunto X dotado de una relación de orden total $\leq$.

Definición 1.32. Sea A un subconjunto de X.

- Un elemento c de X es una ***cota superior*** para A en X si $a \leq c$ cualquiera sea $a \in A$.
- El conjunto A es ***acotado superiormente en X*** si hay una cota superior para A en X.
- Un elemento c de X es un ***máximo*** para A si es una cota superior para A en X y pertenece a A.

- Un elemento c de X es un ***supremo*** para A en X si
  - c es una cota superior para A en X, y
  - cada vez que $d \in X$ es una cota superior para A en X se tiene que $c \leq d$.

Un conjunto acotado superiormente posee en general muchas cotas superiores. Por ejemplo, en el conjunto $\mathbb{R}$ con su orden usual, los números 2 y 3 son cotas superiores para el subconjunto $[0, 1]$. Por el contrario, un subconjunto posee a lo sumo un supremo:

Proposición 1.33. *Sea X un conjunto y sea $\leq$ una relación de orden total en X. Si A es un subconjunto de X que posee un supremo en X, entonces posee exactamente uno.*

Siempre que A sea un subconjunto de un conjunto totalmente ordenado X que admite un supremo en X, escribiremos a este sup A y nos referiremos a él como *el* supremo de A. Notemos que el conjunto X queda implícito en esta notación.

Demostración. Supongamos que A es un subconjunto de X y que c y c' son dos supremos para A en X. Como c es una cota superior para A y c' es un supremo para A, tenemos que $c' \leq c$. De manera similar, como c' es una cota superior para A y c es un supremo para A, tenemos que $c \leq c'$. Juntando estas dos desigualdades vemos que $c = c'$, y esto prueba la proposición. □

El siguiente resultado, que es inmediato, da una caracterización útil del supremo de un conjunto que usaremos muy frecuentemente.

Proposición 1.34. *Sea X un conjunto, sea $\leq$ una relación de orden total en X, sea A un subconjunto de X. Un elemento c de X es el supremo de A en X si y solamente si*

- *c es una cota superior para A y*
- *si d es un elemento de X tal que $d < c$, entonces d no es una cota superior para A.* □

Las nociones de máximo y de supremo están íntimamente relacionadas: ese es el punto del siguiente resultado.

Proposición 1.35. *Sea X un conjunto, sea $\leq$ una relación de orden total en X, y sea A un subconjunto de A. Un elemento c de X es un máximo para A si y solamente sí es un supremo para A en X y pertenece a él.*

Una consecuencia inmediata de esto y de la Proposición 1.33, claro, es que un subconjunto de A posee a lo sumo un máximo — y cuando posee uno podemos escribirlo máx A sin ambigüedad.

Demostración. Sea c un elemento de X y supongamos primero que c es un máximo para A. De esto se sigue, claro, que c es una cota superior para A. Por otro lado, si d es un elemento de X tal que $d < c$, entonces d no es una cota superior para A, porque c pertenece a A. Esto muestra que c es un supremo para A en X que pertenece a A.

Por otro lado, si c es un supremo para A en X que pertenece a A, entonces es una cota superior para A que pertenece a A y, por lo tanto, es un máximo para A. □

Demos algunos ejemplos de las nociones presentadas en esta sección.

Ejemplo 1.36. Consideremos el conjunto $\mathbb{R}$ ordenado con su orden usual.

- El conjunto $[0,1]$ tiene a 1 como supremo. En efecto, es claro que $x \leq 1$ siempre que $x \in [0,1]$, así que 1 es una cota superior para $[0,1]$. Como además pertenece a $[0,1]$, se trata de un máximo de ese conjunto y, en particular, de un supremo de $[0,1]$ en $\mathbb{R}$.
- El conjunto $[0,1)$ también tiene a 1 como supremo en $\mathbb{R}$. Otra vez es claro que $x \leq 1$ para todo $x \in [0,1)$. Ahora, si d es un elemento de $\mathbb{R}$ tal que $d < 1$, entonces el número $a \coloneqq \max\{1/2, (1+d)/2\}$ pertenece a $[0,1)$ y es $d < a$, de manera que d no es una cota superior para $[0,1)$. Esto prueba que $\sup[0,1) = 1$, como dijimos. Notemos que como 1 no pertenece al conjunto $[0,1)$, no es un máximo suyo y, por lo tanto, que este conjunto no posee ningún máximo.
- El conjunto $S \coloneqq \{1 - \frac{1}{n} : n \in \mathbb{N}\}$ también tiene a 1 como supremo en $\mathbb{R}$. En efecto, 1 es una cota superior de S, ya que para todo $n \in \mathbb{N}$ es $1 - \frac{1}{n} < 1$. Sea, por otro lado, d un número real tal que $d < 1$. Como $1 - d > 0$, es $1/(1-d) > 0$ y sabemos que hay un número natural $n \in \mathbb{N}$ tal que $1/(1-d) < n$: en ese caso tenemos que $d < 1 - \frac{1}{n} \in S$ y, por lo tanto, el número d no es una cota superior para S. Usando la proposición podemos concluir de esto que $\sup S = 1$.

Es claro que un conjunto que posee supremo es acotado superiormente, ya que su supremo es una de sus cotas superiores. Sin embargo, esta condición no es en general suficiente.

Ejemplo 1.37. Consideremos el conjunto $\mathbb{Q}$ dotado de su orden usual, y su subconjunto

$$A \coloneqq \{x \in \mathbb{Q} : x^2 < 2\}.$$

Este conjunto esta acotado superiormente en $\mathbb{Q}$. En efecto, si x es un número real tal que $x > 2$, entonces $x^2 > 4 > 2$ y $x \notin A$: esto nos dice que $x \leq 2$ siempre que $x \in A$ y, por lo tanto, que 2 es una cota superior para A en $\mathbb{Q}$.

Supongamos ahora que el conjunto A posee un supremo $s \coloneqq \sup A$ en $\mathbb{Q}$. Como $1 \in A$, sabemos que $1 \leq s$. Por otro lado, como 2 no es el cuadrado de un número racional, sabemos que $s^2 - 2 \neq 0$, así que o bien es $s^2 < 2$ o bien $s^2 > 2$. Consideraremos estas dos posibilidades separadamente.

- Supongamos primero que $s^2 < 2$. Como $s > 1$, el número $s + 2$ es estrictamente positivo y

podemos considerar el número

$$t \coloneqq \frac{2s+2}{s+2}.$$

Como s es un número racional, t también lo es, y es

$$t^2 - 2 = \frac{(2s+2)^2}{(s+2)^2} - 2 = 2\frac{s^2-2}{(s+2)^2} < 0,$$

así que $t^2 < 2$ y, en definitiva, es $t \in A$. Como s es una cota superior para A, es entonces $t \leq s$ y, por lo tanto,

$$0 \geq t - s = \frac{2s+2}{s+2} - s = \frac{2s+2-s^2-2s}{s+2} = \frac{2-s^2}{s+2} > 0,$$

ya que $s > s^2$ y $s + 2 > 0$. Esto es, por supuesto, absurdo.

- Debe ser entonces $s^2 > 2$. Como $s > 0$, podemos considerar el número

  $$u \coloneqq \frac{s^2+2}{2s},$$

  que otra vez es racional y positivo. Este número es estrictamente menor que s, ya que $s^2 > 2$ y, por lo tanto,

  $$u - s = \frac{s^2+2}{2s} - s = \frac{2-s^2}{2s} < 0.$$

  Además, es

  $$u^2 - 2 = \frac{(s^2-2)^2}{4s^2} > 0,$$

  de manera que $2 < u^2$.

  Sea a es un elemento de A. Si $a \leq 0$, entonces claramente $a \leq u$. Supongamos que, por el contrario, es $a > 0$. Como $a^2 < 2 < u^2$, tenemos que $0 < u^2 - a^2 = (u-a)(u+a)$ y, dado que $u + a > 0$, esto implica que $0 < u - a$, es decir, que $a < u$. Vemos así que, en cualquier caso se tiene que $a \leq u$: esto muestra que u es una cota superior para el conjunto A. Esto es absurdo, ya que es menor que s y s es el supremo de A.

Como ninguna de estas dos posibilidades puede ocurrir, llegamos a una contradicción. La conclusión de esto es que el conjunto A no posee un supremo en $\mathbb{Q}$.

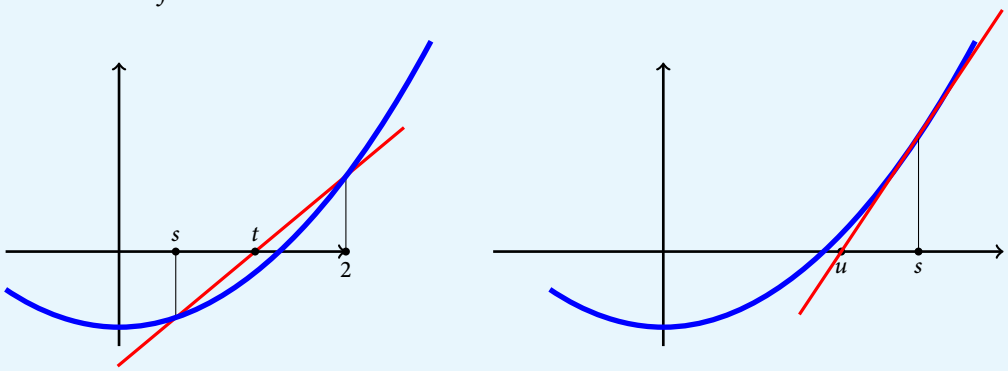
Observación 1.38. Esta demostración parece un poco mágica porque no explicamos de dónde sacamos los números t y u que usamos en ella. Revelemos el secreto. Consideremos la función

$$f : x \in \mathbb{R} \mapsto x^2 - 2 \in \mathbb{R}.$$

Para encontrar el número t hicimos un paso del *método de la secante* para aproximar los ceros de la función f: en general, si a y b son dos aproximaciones para un cero de esa función, el método nos propone usar a

$$c \coloneqq a - \frac{f(a)(b-a)}{f(b) - f(a)}$$

como una mejor aproximación. Si aquí tomamos $a = s$ y $b = 2$, entonces x resulta igual a t, y las propiedades de este número son consecuencia de propiedades generales del método de la secante y de que la función f es convexa.



De manera similar, para encontrar el número u hicimos un paso del *método de Newton–Raphson* para encontrar aproximar los ceros de f: si a es una aproximación de un cero de f, este método nos propone usar a

$$c \coloneqq a - \frac{f(a)}{f'(a)}$$

como una mejor aproximación. Si empezamos con $a = s$, entonces esta aproximación c es precisamente el numero u que usamos arriba, y otra vez las propiedades útiles de este número son consecuencia de propiedades generales del método de Newton–Raphson.

La situación en la que todo conjunto acotado superiormente posee un supremo es extremadamente importante, y le ponemos un nombre:

Definición 1.39. Sea X un conjunto dotado de una relación de orden total $\leq$. Decimos que X es ***completo*** con respecto a $\leq$ si todo subconjunto no vacío de X que es acotado superiormente posee un supremo en X.

El Ejemplo 1.37 muestra que el conjunto $\mathbb{Q}$ dotado de su orden usual no es completo. Por otro lado, el conjunto $\mathbb{R}$ dotado de su orden usual sí es completo — esta es la razón por que nos interesa esa noción de completitud, de hecho. Con las herramientas que tenemos a nuestra disposición en este momento no podemos describir exactamente qué subconjuntos de $\mathbb{R}$ son completos con respecto al orden que heredan de $\mathbb{R}$.

Ejercicio 1.40. Muestre que el subconjunto $\mathbb{Q}(\sqrt{2})$ de $\mathbb{R}$ descripto en el Ejemplo 1.16 no es completo con respecto al orden que hereda de $\mathbb{R}$. Una forma de hacer esto es probar que su subconjunto $\{x \in \mathbb{Q}(\sqrt{2}) : x^2 < 3\}$ es acotado en $\mathbb{Q}(\sqrt{2})$ y no posee supremo allí.

Hemos dado ejemplos de conjuntos ordenados que *no* son completos, pero ninguno de conjuntos ordenados que sí lo son. Demos algunos.

Proposición 1.41. *Un conjunto totalmente ordenado y finito es completo.*

Demostración. Sea X un conjunto finito, sea $\leq$ una relación de orden total en X, y sea A un subconjunto no vacío de X. Para probar la proposición tenemos que mostrar que A posee un supremo en X. Ahora bien, como X es finito y A es un subconjunto de X, es claro que A mismo es un conjunto finito. Escribamos n a su cardinal, que es un elemento de $\mathbb{N}$. Probaremos que A posee un supremo en X haciendo inducción con respecto a este entero n.

Supongamos primero que A tiene exactamente un elemento y escribamos a ese elemento a, de manera que $A = \{a\}$. Como $a \leq a$, es claro que a es una cota superior para A. Como además pertenece a A, se trata, de hecho, de un máximo para A y, en particular, de un supremo para A. Lo que queremos es, por lo tanto, cierto en este caso.

Supongamos ahora que el cardinal n de A es mayor que 1 y sea a un elemento cualquiera de A. El conjunto $B \coloneqq A \setminus \{a\}$ es entonces un subconjunto de A, así que se trata de un subconjunto finito de X, y su cardinal es $n - 1$, así que no es vacío. Inductivamente, entonces, podemos suponer que B admite un supremo en X, al que escribiremos b. Tenemos ahora que considerar dos casos, dependiendo de la relación de orden entre a y b.

- En primer lugar, supongamos que $a \leq b$. Si c es un elemento de A, entonces o bien c pertenece a B, y en ese caso $c \leq b$ porque b es una cota superior para B, o bien c es a, y en ese caso $c \leq b$ por nuestra hipótesis. Vemos así que b es una cota superior para A. Por otro lado, sea d un elemento de X tal que $d < b$. Como b es el supremo de B, hay un elemento e de B tal que $d < e$: como $e \in A$, esto nos dice que d no es una cota superior para A. De acuerdo a la Proposición 1.34, b es un supremo para A en X.
- En segundo lugar, supongamos que $b \leq a$. Si c es un elemento de A, entonces bien c pertence a B y, como b es una cota superior para B, es $c \leq b \leq a$, o bien c es a y, por lo tanto, $c \leq a$. Vemos así que a es una cota superior para A. Por otro lado, es claro que un elemento d

menor que a no es una cota superior para A, ya que a pertence a A, y otra vez gracias a la Proposición 1.34 podemos concluir que a es un supremo para A en X.

En cualquiera de los dos casos, entonces, el conjunto A posee un supremo en X. □

Hasta ahora estuvimos hablando de cotas superiores, máximos y supremos, pero hay también versiones «inferiores» de estas nociones:

Definición 1.42. Sea A un subconjunto de X.

- Un elemento c de X es una ***cota inferior*** para A en X si $a \geq c$ cualquiera sea $a \in A$.
- El conjunto A es ***acotado inferiormente*** en X si existe una cota inferior para A en X.
- Un elemento c de X es un ***mínimo*** para A si es una cota inferior para A en X y pertenece a A.
- Un elemento c de X es un ***ínfimo*** para A si
  - c es una cota inferior para A en X, y
  - cada vez que $d \in X$ es una cota inferior para A en X e tiene que $c \geq d$.

Exactamente de la misma forma que probamos la Proposición 1.33 podemos probar que un conjunto posee a lo sumo un ínfimo:

Proposición 1.43. *Sea X un conjunto y sea $\leq$ una relación de orden total sobre X. Un subconjunto A de X que posee un ínfimo posee exactamente uno.* □

En vista de este resultado, siempre que un subconjunto A de X posea ínfimo podemos escribirlo sin ambigüedades $\inf A$. Por otro lado, así como la Proposición 1.34 nos da una una condición útil para verificar que elemento de X es el supremo de un conjunto, el siguiente resultado lo hace para el ínfimo.

Proposición 1.44. *Sea X un conjunto, sea $\leq$ una relación de orden total en X, y sea A un subconjunto de X. Un elemento c de X es el ínfimo de A si y solamente si*

- *c es una cota inferior para A y*
- *si d es un elemento de X tal que $d > c$, entonces d no es una cota inferior para A.* □

Ejercicio 1.45. Pruebe en detalle las Proposiciónes 1.43 y 1.44.

Tenemos la siguiente versión de la Proposición 1.35:

Proposición 1.46. *Sea X un conjunto, sea $\leq$ una relación de orden total en X, y sea A un subconjunto de A. Un elemento c de X es un mínimo para A si y solamente sí es un ínfimo para A en X y pertenece*

a él. □

Se sigue de esto que un conjunto A posee como mucho un mínimo, por supuesto, y cuando posee uno podemos escribirlo mín A sin ambigüedad alguna.

No damos una versión de la noción de completitud para ínfimos, ya que no es necesario, como muestran el siguiente resultado y, de manera más evidente, el del Ejercicio 1.48 que lo sigue.

Proposición 1.47. *Sea X un conjunto dotado de una relación de orden total $\leq$. Si X es completo, entonces todo subconjunto no vacío de X que es acotado inferiormente posee un ínfimo.*

Demostración. Supongamos que X es completo y sea A un subconjunto no vacío de A que es acotado inferiormente. Escribamos B al conjunto de todas las cotas inferiores de A. Como A es acotado inferiormente, el conjunto B no es vacío. Por otro lado, como A no es vacío, podemos elegir un elemento a de A: este elemento es una cota superior para B, ya que todo $b \in B$ es una cota inferior de A y, en particular, es tal que $b \leq a$. Vemos así que el subconjunto B de X es no vacío y acotado superiormente: como estamos suponiendo que X es completo, sabemos entonces que existe en X un supremo para B. Escribamos $c \coloneqq \sup B$ a ese supremo. Mostraremos que c es también un ínfimo para el conjunto A y esto probara la proposición.

- Supongamos por un momento que c no es una cota inferior para el conjunto A, de manera que hay un elemento a de A tal que $a < c$. Como c es el supremo de B, por su parte, esto implica que a no es una cota superior para B y que existe entonces un elemento b de B tal que $a < b$: esto es absurdo, porque b, por pertenecer a B, es una cota superior para A. Vemos así que c es una cota inferior para el conjunto A.
- Sea ahora d un elemento de X tal que $d > c$. Si d es una cota inferior para el conjunto A, entonces d pertenece a B y, por lo tanto, como c es una cota superior para B, tenemos que $d \leq c$: esto es imposible, ya que $d > c$. Esta contradicción nos permite concluir que d no es una cota superior para A.

Hemos probado que el elemento c de X satisface las dos condiciones de la Proposición 1.44, así que se trata del ínfimo de A. □

Esta proposición resuelve la mitad del siguiente ejercicio.

Ejercicio 1.48. Pruebe que un conjunto totalmente ordenado X es completo si y solamente si todo subconjunto no vacío de X que es inferiormente acotado posee un ínfimo.

Antes de continuar en la siguiente sección con nuestro estudio de los cuerpos, demos un resultado que establece una relación entre los ínfimos y supremos en un conjunto ordenado.

Proposición 1.49. *Sea X un conjunto dotado de una relación de orden total $\leq$, y sea A un subconjunto no vacío y acotado superiormente de X. Un elemento c de X es el supremo de A en X. si y solamente si es el mínimo del conjunto de cotas superiores de A.*

Demostración. Escribamos $\mathscr{C}$ al conjunto de todas las cotas superiores el conjunto A. Como A es acotado superiormente, claro, tenemos que $\mathscr{C} \neq \varnothing$.

Supongamos primero que c es el supremo de A en X. Como c es una cota superior para A, tenemos que $c \in \mathscr{C}$. Por otro lado, si d es un elemento de $\mathscr{C}$, entonces d es una cota superior para A en X y, como c es el supremo de A en X, tenemos que $c \leq d$: esto nos dice que c es una cota inferior para el conjunto $\mathscr{C}$. Juntando todo, hemos probado que c es el mínimo del conjunto $\mathscr{C}$ y, por lo tanto, que la condición que da la proposición es necesaria.

Probemos ahora que también es suficiente. Supongamos que c es el mínimo del conjunto $\mathscr{C}$. Como c pertenece entonces a $\mathscr{C}$, se trata de una cota superior para A en X. Por otro lado, si d es una cota superior para A en X, entonces d pertenece a $\mathscr{C}$ y, como c es el mínimo de $\mathscr{C}$, tenemos que $c \leq d$. Esto muestra que c es el ínfimo de A en C, como queremos. □

Por supuesto, hay un resultado análogo al de la proposición que acabamos de probar: en la misma situación, un elemento de X es el ínfimo de un conjunto A que es no vacío y acotado inferiormente si y solamente si es el máximo del conjunto de cotas inferiores de A.

1.4. El cuerpo de los números reales

Después del trabajo de las tres secciones anteriores tenemos por fin todas las definiciones que necesitamos para nuestro propósito original de describir qué entendemos por *número real*.

Como observamos arriba, sobre el conjunto $\mathbb{R}$ de los números reales tenemos definidas dos operaciones $+, \cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ de suma y producto que hacen de él un cuerpo en el sentido de la Definición 1.15. Esto significa, simplemente, que estas operaciones tienen las propiedades básicas que aprendimos todos de niños. Más aún, hay en $\mathbb{R}$ una relación de orden $\leq$ que hace de ese cuerpo un cuerpo ordenado en el sentido de la Definición 1.28 y, otra vez, esto significa simplemente que esa relación de orden interactúa con las dos operaciones aritméticas de $\mathbb{R}$ de la manera esperada.

Es mucho menos claro que todo esto que el conjunto $\mathbb{R}$, cuando lo dotamos de esa relación de orden $\leq$, es un conjunto ordenado completo en el sentido de la Definición 1.39. ¡Ciertamente no es esto algo que nos hayan enseñado cuando éramos niños! La observación de que el conjunto de los números reales es completo con respecto a su orden usual es el resultado final de un largo trabajo de reflexión sobre los fundamentos del análisis por parte de muchos matemáticos. Los historiadores de la matemática identifican el inicio de ese largo proceso en el trabajo de 1585 de Simon Stevin sobre la representación vía fracciones decimales de los números reales, pero el

primero en enunciar explícitamente ese hecho fue David Hilbert. Lo hizo en un célebre trabajo publicado en 1900 titulado *Über den Zahlbegriff* [Hilo0][2] y en esencialmente la misma forma que lo hacemos hoy, motivado por su proyecto de dar bases rigurosas para la geometría.

Sea como fuere, juntando toda esta información podemos afirmar que, cuando dotamos al conjunto $\mathbb{R}$ de sus operaciones usuales de suma y producto y de su orden usual,

$$\mathbb{R} \text{ es un cuerpo ordenado completo.} \tag{1.13}$$

Ahora bien, ¿cómo podemos *probar* esta afirmación? La respuesta a esta pregunta es simple: no podemos. El problema reside en que para probar algo al respecto del conjunto de los números reales y su estructura necesitamos tener una descripción precisa de qué es el conjunto de los números reales y, recordemos, no tenemos ninguna: ¡encontrar alguna es precisamente lo que estamos tratando de hacer! No podemos probar nada sobre algo que no conocemos.

Expliquemos la idea de Hilbert para salir de este atolladero. Primero, probamos el siguiente resultado:

Proposición 1.50. *Existen cuerpos ordenados completos.* □

La forma en que esto se hace es directa: construimos un ejemplo de un cuerpo ordenado completo. Por supuesto, al hacerlo no podemos usar de ninguna forma al cuerpo de los números reales, ya que en este punto seguimos sin saber qué es. De hecho, lo único que necesitamos para hacer esa construcción es tener a nuestra disposición el conjunto $\mathbb{N}$ de los números naturales y saber que satisfacen los llamados *axiomas de Peano*. Esto puede hacerse de varias formas, pero la más usual consiste en varios pasos:

- A partir de $\mathbb{N}$ construimos el conjunto $\mathbb{Z}$ de los enteros dotado de sus operaciones usuales.
- A partir de $\mathbb{Z}$ construimos el conjunto $\mathbb{Q}$, sus operaciones aritméticas y su orden usual, y probamos que de esta forma obtenemos un cuerpo ordenado.
- Finalmente, a partir del cuerpo ordenado $\mathbb{Q}$ que acabamos de construir llevamos a cabo un procedimiento de *completación* cuyo resultado es un cuerpo ordenado completo. Hay varias formas de hacer esto — la más directa, e históricamente la primera, es la de usar los llamados *cortaduras de Dedekind*, una idea usada por Richard Dedekind por primera vez en su trabajo *Stetigkeit und irrationale Zahlen*[3] [Ded60].

Ninguno de estos pasos es particularmente difícil, pero son todos considerablemente laboriosos. El hecho de que es posible hacer todo esto empezando con nada más que el conjunto de los números naturales es la motivación de la célebre frase de Leopold Kronecker «Dios hizo a los enteros, todo lo demás es obra del hombre»[4].

[2] «*Sobre el concepto de número*» en alemán.

[3] «*Continuidad y números irracionales*» en alemán.

[4] La frase original es «Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwer», de acuerdo a Heinrich Weber [Web93].

Una vez que sabemos que existen cuerpos ordenados completos, el segundo paso del plan de Hilbert es establecer el siguiente resultado:

Proposición 1.51. *Hay esencialmente un único cuerpo ordenado completo.* □

Precisemos que significa exactamente esto. Lo que afirma esta proposición es que siempre que tenemos dos cuerpos ordenados y completos K y L, con operaciones $+_K$, $\cdot_K$ y orden $\leq_K$ el primero, y $+_L$, $\cdot_L$ y $\leq_L$ el segundo, hay una y solo una función biyectiva $\phi : K \to L$ tal que para toda elección de x e y en K se tiene que

$$\begin{aligned} &\phi(x +_K y) = \phi(x) +_L \phi(y), \\ &\phi(x \cdot_K y) = \phi(x) \cdot_L \phi(y), \\ &x \leq_K y \iff \phi(x) \leq_L \phi(y). \end{aligned} \tag{1.14}$$

Llamamos a una función con esa propiedad un ***isomorfismo*** de cuerpos ordenados.

En la práctica, la existencia de un isomorfismo entre los cuerpos K y L nos dice que, mientras nos limitemos a hacer en ellos las cosas que la estructura de cuerpo ordenado completo nos permite hacer — operaciones aritméticas, comparaciones de orden, cálculo de supremos de conjuntos no vacíos y acotados — obtendremos los mismos resultados y que, en particular, no podremos distinguirlos. Es por eso que la Proposición 1.51 no dice que hay un único cuerpo ordenado completo sino solamente que hay *esencialmente* un único cuerpo ordenado completo: la palabra *esencialmente* refiere al hecho de que entre dos cuerpos ordenados completos hay un isomorfismo de cuerpos ordenados completos. Que además exista exactamente un tal isomorfismo es algo todavía más fuerte, por supuesto.

Observación 1.52. Mostremos que es falso que exista un único cuerpo ordenado completo. Supongamos que K es un cuerpo ordenado completo, con operaciones $+$ y $\cdot$ y relación de orden $\leq$, y consideremos el conjunto $L \coloneqq K \times \{K\}$, cuyos elementos son los pares ordenados (x, K) cuyas primeras componentes son elementos de K y cuya segunda componente es el conjunto K. Usando las operaciones $+$ y $\cdot$ de K podemos definir operaciones $\oplus$ y $\odot$ en L: para cada elección de x e y en K ponemos

$$(x, K) \oplus (y, K) \coloneqq (x + y, K), \qquad (x, K) \odot (y, K) \coloneqq (x \cdot y, K).$$

De manera similar, usando la relación de orden $\leq$ de K definimos una relación $\preceq$ sobre L de manera que sea

$$(x, K) \preceq (y, K) \iff x \leq y$$

cualesquiera sean x e y en K. Dejamos al lector la verificación de que el conjunto L, con las operaciones $\oplus$ y $\odot$ como suma y producto, respectivamente, y con la relación $\preceq$, es un cuerpo ordenado completo. Esto prueba lo que queremos, ya que este cuerpo L es manifiestamente distinto

que el cuerpo K. De todas maneras, el lector podrá apreciar que K y L no son significativamente distintos.

De hecho, de acuerdo a la Proposición 1.51 tiene que existir un isomorfismo de cuerpos ordenados completos $K \to L$, y es fácil exhibir uno: el lector puede verificar que la función

$$\phi : x \in K \mapsto (x, K) \in L$$

es una biyección que satisface las condiciones de (1.14).

Finalmente, con las Proposiciónes 1.50 y 1.51, con Hilbert hacemos la siguiente definición:

Definición 1.53. $\mathbb{R}$ es un cuerpo ordenado completo.

Lo que queremos decir con esto es que, desde ahora en adelante, denotaremos con $\mathbb{R}$ al conjunto subyacente a algún cuerpo ordenado y completo — sabemos que existe alguno por la Proposición 1.50 y que, si bien hay muchos, la Proposición 1.51 nos dice que cuál elijamos no tiene ninguna consecuencia, ya que entra cada dos de ellos hay un isomorfismo de cuerpos ordenados que garantiza que no haya entre ellos ninguna diferencia sustancial.

Es importante entender qué hicimos aquí. Empezamos haciendo la observación (1.13) de que el conjunto de los números reales, dotado de sus operaciones aritméticas y su relación de orden usuales, es un cuerpo ordenado y completo, observamos que esta afirmación no tiene, de hecho, ningún sentido hasta tener una definición precisa de qué es exactamente el conjunto $\mathbb{R}$ y cuáles son esas operaciones y esa relación de orden, y terminamos por *definir* a $\mathbb{R}$ y sus operaciones y relación de orden de manera — de la única manera posible — de manera que la afirmación (1.13) sea cierta. Transformamos la afirmación que queríamos que fuera cierta en una tautología.

Finalmente, notemos que esta definición del cuerpo de los números reales no da una respuesta a la pregunta de qué es un número real. Por el contrario, la idea de Hilbert es, precisamente, qué no importa qué son los números reales — que alcanza con saber qué podemos hacer con ellos con qué garantías, ya que eso los determina en todos los aspectos que son importantes.

CAPÍTULO 2

Primeras propiedades de $\mathbb{R}$

En el capítulo anterior definimos a $\mathbb{R}$ como el (esencialemente único) cuerpo ordenado completo. Esta definición es sorprendentemente compacta: lo único que nos dice es que en $\mathbb{R}$ tenemos definidas operaciones de suma y producto y una relación de orden, y que estas satisfacen unas pocas condiciones bastante sencillas — conmutatividad, asociatividad, compatibilidad entre la suma y la relación de orden, etc. En la práctica, sin embargo, cuando trabajamos con los números reales necesitamos tener mucha más información sobre esas operaciones y esa relación de orden que la que está incluída en las Definiciones 1.15, 1.28 y 1.39.

Ahora bien, si la idea de Hilbert de definir a $\mathbb{R}$ como hicimos en la Definición 1.53 es correcta, entonces *todo* lo que queramos saber sobre $\mathbb{R}$ tiene que ser consecuencia de que se trata de un cuerpo ordenado completo. En este capítulo mostraremos cómo hacer esto para algunas propiedades que usamos todo el tiempo al trabajar con los números reales.

2.1. Propiedades aritméticas

Empecemos estableciendo las llamadas *leyes de cancelación*:

Proposición 2.1. *Sean x, x' e y elementos de $\mathbb{R}$.*
(*i*) *Si $x + y = x' + y$, entonces $x = x'$.*
(*ii*) *Si $x \cdot y = x' \cdot y$ e $y \neq 0$, entonces $x = x'$.*

Demostración. La primera de las dos afirmaciones es una de las de la Proposición 1.19, así que bastará que probemos la segunda. Supongamos que $x + y = x' + y'$ e $y \neq 0$. Como y no es 0 admite un elemento inverso y^{-1} con respecto al producto y tenemos que

$$\begin{aligned} x &= x \cdot 1 && \text{porque 1 es neutro para el producto } \cdot \\ &= x \cdot y \cdot y^{-1} && \text{porque } y^{-1} \text{ es inverso a } y \text{ con respecto al producto} \\ &= x' \cdot y \cdot y^{-1} && \text{por la hipótesis de que } x \cdot y = x' \cdot y \end{aligned}$$

$= x' \cdot 1$ porque y^{-1} es inverso a y con respecto al producto

$= x'$ porque 1 es neutro para el producto $\cdot$.

Esto prueba la segunda afirmación de la proposición. □

El segundo resultado que probaremos describe dos propiedades básicas del elemento cero.

Proposición 2.2.

(*i*) *Para todo elemento x de $\mathbb{R}$ se tiene que $x \cdot 0 = 0$.*

(*ii*) *Si x e y son dos elementos de $\mathbb{R}$ tales que $x \cdot y = 0$, entonces $x = 0$ o $y = 0$.*

Demostración. La primera de las dos afirmaciones es una de las de la Proposición 1.19. Por otro lado, si x e y son dos elementos de $\mathbb{R}$ tales que $x \cdot y = 0$ y x es distinto de 0, entonces, como $\mathbb{R}$ es un cuerpo, x posee un elemento inverso x^{-1} y

$0 = x^{-1} \cdot 0$ por la primera parte de la proposición

$= x^{-1} \cdot x \cdot y$ por la hipótesis

$= 1 \cdot y$ porque x^{-1} es un elemento inverso de x

$= y$ porque 1 es neutro para el producto.

Esto prueba la segunda afirmación de la proposición. □

En tercer lugar podemos describir la forma en que el producto interactúa con la operación $x \in \mathbb{R} \mapsto -x \in \mathbb{R}$.

Proposición 2.3.

(*i*) *Para todo elemento x de $\mathbb{R}$ se tiene que $-x = (-1) \cdot x$.*

(*ii*) *Si x e y son dos elementos de $\mathbb{R}$, entonces*

$$(-x) \cdot y = x \cdot (-y) = -(x \cdot y), \qquad (-x) \cdot (-y) = x \cdot y.$$

Demostración. (*i*) Sea x un elemento de $\mathbb{R}$. Queremos probar que $-x = (-1) \cdot x$ y esta igualdad significa, explícitamente, que el elemento $y := (-1) \cdot x$ es opuesto a x: para probarla, entonces, tenemos que mostrar que $x + y = 0$. Podemos hacer esto por un cálculo directo:

$x + (-1) \cdot x = 1 \cdot x + (-1) \cdot x$ porque 1 es neutro para el producto $\cdot$

$= (1 + (-1)) \cdot x$ porque vale la ley distributiva en $\mathbb{R}$

$= 0 \cdot x$ porque -1 es opuesto a 1

$= 0$ de acuerdo a la primera parte de la Proposición 2.2.

(*ii*) Sean x e y dos elementos de $\mathbb{R}$. Es

$$\begin{aligned}(-x)\cdot y &= (-1)\cdot x\cdot y && \text{por la parte } (i)\\ &= -(x\cdot y) && \text{otra vez por la parte } (i).\end{aligned} \tag{2.1}$$

Por otro lado, es

$$\begin{aligned}x\cdot(-y) &= (-y)\cdot x && \text{porque el producto es conmutativo}\\ &= -(y\cdot x) && \text{por lo que ya probamos}\\ &= -(x\cdot y) && \text{otra vez porque el producto es conmutativo}\end{aligned} \tag{2.2}$$

y

$$\begin{aligned}(-x)\cdot(-y) &= -(x\cdot(-y)) && \text{por la igualdad (2.1)}\\ &= -\big(-(x\cdot y)\big) && \text{por la igualdad (2.2)}\\ &= x\cdot y && \text{por la primera igualdad de (1.10).}\end{aligned}$$

Con esto hemos probado todas las afirmaciones de (*ii*). □

2.2. Propiedades de monotonía

La Definición 1.28 que dimos para los cuerpos orientados impone una condición de compatibilidad entre la suma y la relación de orden. En esta sección mostraremos que valen otras.

En primer lugar, la primera condición de esa definición está enunciada en términos de la relación $\leq$, pero tiene como consecuencia una completamente similar en términos de la relación $<$ de orden estricto que es útil.

Proposición 2.4. *Si x, y y z son elementos de $\mathbb{R}$ tales que $x < y$, entonces $x + z < y + z$.*

Demostración. Sean x, y y z tres elementos de $\mathbb{R}$ tales que $x < y$. Como es $x \leq y$, de la primera condición de la definición tenemos que $x + z \leq y + z$. Si fuera $x + z = y + z$, entonces tendríamos que

$$\begin{aligned}x &= x + 0 && \text{porque 0 es neutro para la suma}\\ &= x + z + (-z) && \text{porque } -z \text{ es opuesto a } z\\ &= y + z + (-z) && \text{por la hipótesis}\\ &= y + 0 && \text{porque } -z \text{ es opuesto a } z\\ &= y && \text{porque 0 es neutro para la suma,}\end{aligned}$$

y esto es absurdo ya que $x < y$. Tenemos entonces que $x + z \leq y + z$ y que $x + z \neq y + z$, así que $x + z < y + z$, como afirma la proposición. □

En segundo lugar, la primera condición de la Definición 1.28 y la proposición que acabamos de probar nos dicen que sumar un elemento de $\mathbb{R}$ a ambos lados de una desigualdad preserva la desigualdad. Nuestro siguiente resultado generaliza esto:

Proposición 2.5. *Sea K un cuerpo ordenado y sean x, y, z y u cuatro elementos de K.*
(*i*) *Si $x \leq y$ y $z \leq u$, entonces $x + z \leq y + u$.*
(*ii*) *Si $x < y$ y $z \leq u$, entonces $x + z < y + u$.*

Demostración. (*i*) Si $x \leq y$ y que $z \leq u$, entonces usando dos veces la primera condición de la Definición 1.28 vemos que $x + z \leq y + z \leq y + u$, así que $x + z \leq y + u$ porque la relación $\leq$ es transitiva.

(*ii*) Supongamos ahora que $x < y$ y que $z \leq u$. Esto implica que

$$0 = z + (-z) \leq u + (-z). \tag{2.3}$$

Ahora bien, como $x \leq y$, de la primera parte sabemos que $x + z \leq y + u$. Si fuera $x + z = y + u$, tendríamos que

$$\begin{aligned}
y &= y + 0 && \text{porque 0 es neutro para la suma} \\
&\leq y + u + (-z) && \text{por la desigualdad (2.3)} \\
&= x + z + (-z) && \text{por la hipótesis} \\
&= x + 0 && \text{porque } -z \text{ es opuesto a } z \\
&= x && \text{porque 0 es neutro para la suma,}
\end{aligned}$$

de manera que $y \leq x$: esto es absurdo, ya que estamos suponiendo que $x < y$. Vemos así que debe ser $x + z \neq y + u$ y, por lo tanto, que $x + z < y + u$, como afirma la proposición. □

Finalmente, mostremos que la compatibilidad entre la suma y la relación de orden implica una compatibilidad entre esa relación de orden y la función $x \in \mathbb{R} \mapsto -x \in \mathbb{R}$:

Proposición 2.6. *Sean x e y dos elementos de $\mathbb{R}$.*
(*i*) *Si $x < y$, entonces $-y < -x$.*
(*ii*) *Si $x \leq y$, entonces $-y \leq -x$.*

Demostración. Si $x < y$, entonces

$$-y = (-y) + 0 \qquad \text{porque 0 es neutro para la suma}$$

$$
\begin{aligned}
&= (-y) + (-x) + x && \text{porque } -x \text{ es opuesto a } x \\
&= (-x) + (-y) + x && \text{porque la suma es conmutativa} \\
&< (-x) + (-y) + y && \text{por la hipótesis de que } x < y \text{ y la Definición 1.28} \\
&= (-x) + 0 && \text{porque } -y \text{ es opuesto a } y \\
&= -x && \text{porque 0 es neutro para la suma,}
\end{aligned}
$$

y esto es lo que afirma la primera parte de la proposición. Por otro lado, si $x \leq y$, entonces o bien $x < y$ y en ese caso lo que ya hicimos muestra que $-y < -x$, o bien $x = y$ y en ese caso vale, claro que $-y = -x$: en cualquiera de los dos casos tenemos que $-y \leq -x$ y, por lo tantom también es cierta la segunda afirmación de la proposición. □

2.3. Elementos positivos y negativos

Usando la relación de orden de $\mathbb{R}$ podemos hacer la siguiente definición bien familiar:

Definición 2.7. Un elemento x de $\mathbb{R}$ es ***positivo*** si $0 < x$, es ***negativo*** si $x < 0$, y es ***nulo*** si $x = 0$.

Decimos además que un elemento de $\mathbb{R}$ es ***no negativo*** si no es negativo, y que es ***no positivo*** si no es positivo. Aunque estas expresiones son menos que felices, forman parte de nuestra jerga usual.

Una consecuencia inmediata de que el orden de $\mathbb{R}$ es total es la siguiente *ley de tricotomía*:

Proposición 2.8. *Si x es un elemento de $\mathbb{R}$, entonces exactamente una de las siguientes tres afirmaciones es verdadera:*

(*a*) *x es negativo.*
(*b*) *x es nulo.*
(*c*) *x es positivo.*

Demostración. Sea x un elemento de $\mathbb{R}$. El hecho de que la relación de orden $\leq$ de $\mathbb{R}$ es una relación de orden total nos dice que $0 \leq x$ o $x \leq 0$, y esto implica que alguna de las tres afirmaciones del enunciado es cierta.

Si x es negativo, de manera que $x < 0$, entonces de la definición de $<$ sabemos que $x \neq 0$, así que x no es nulo, y de la asimetría de la relación de orden estricto $<$ que no vale que $x > 0$, esto es, que x no es positivo. De manera simétrica, si x es positivo, de manera que $x > 0$, entonces la definición de $>$ implica que $x \neq 0$ y la asimetría de esta relación que no vale que $x < 0$, esto es, que x no es negativo. Finalmente, si x es nulo, de manera que $x = 0$, entonces la definición de la relación $<$ implica que ni $0 < x$ ni $x < 0$ valen, así que x no es ni positivo ni negativo. Esto prueba

que no puede haber dos de las tres afirmaciones del enunciado que sean ciertas. □

La función $x \in \mathbb{R} \mapsto -x \in \mathbb{R}$ intercambia los números positivos y negativos:

Proposición 2.9. *Un elemento x de $\mathbb{R}$ es positivo si y solamente si su opuesto $-x$ es negativo.*

Demostración. Sea x un elemento de $\mathbb{R}$. Si x es positivo, entonces $0 < x$ y la Proposición 2.6 nos dice que $-x < -0 = 0$, esto es, que x es negativo. Recíprocamente, si $-x$ es negativo, de manera que $-x < 0$, entonces esa proposición nos dice que $0 = -0 < -(-x) = x$, esto es, que x es positivo. □

La multiplicación por un elemento positivo preserva las desigualdades:

Proposición 2.10. *Sean x, y, y z tres elementos de $\mathbb{R}$.*
(*i*) *Si $x < y$ y z es positivo, entonces $x \cdot z < y \cdot z$.*
(*ii*) *Si $x \leq y$ y z es positivo, entonces $x \cdot z \leq y \cdot z$.*

Demostración. Supongamos primero que $x < y$ y que $0 < z$. De la primera desigualdad y de la Proposición 2.4 podemos deducir que $0 = x + (-x) < y + (-x)$ y, como $0 < z$ y vale la segunda condición de la Definición 1.28, que además

$$0 < \big(y + (-x)\big) \cdot z. \tag{2.4}$$

Podemos calcular entonces que

$$\begin{aligned}
y \cdot z &= y \cdot z + 0 && \text{porque 0 es neutro para la suma} \\
&= y \cdot z + \big(-(x \cdot z)\big) + x \cdot z && \text{porque } -(x \cdot z) \text{ es opuesto de } x \cdot z \\
&= y \cdot z + (-x) \cdot z + x \cdot z && \text{por la segunda parte de la Proposición 2.3} \\
&= \big(y + (-x)\big) \cdot z + x \cdot z && \text{porque vale la ley distributiva.} \\
&> 0 + x \cdot z && \text{por la desigualdad (2.4) y la Definición 1.28} \\
&= x \cdot z && \text{porque 0 es neutro para la suma.}
\end{aligned}$$

Esto prueba la afirmación (*i*) de la proposición.

Probemos ahora la afirmación (*ii*). Supongamos que $x \leq y$ y que z es positivo. Si $x < y$, entonces lo que ya probamos nos dice que $x \cdot z < y \cdot z$, así que también $x \cdot z \leq y \cdot z$. Si, en cambio, es $x = y$, entonces por supuesto tenemos que $x \cdot z < y \cdot z$ y otra vez que $x \cdot z \leq y \cdot z$. Esto prueba que en cualquier caso es $x \cdot z \leq y \cdot z$, y esto es lo que queríamos probar. □

La multiplicación por elementos negativos, por el contrario, las invierte:

Proposición 2.11. *Sea K un cuerpo ordenado y sean x, y, y z tres elementos de K.*

(*i*) *Si $x < y$ y z es negativo, entonces $x \cdot z > y \cdot z$.*

(*ii*) *Si $x \leq y$ y z es negativo, entonces $x \cdot z \; y \cdot z$.*

Demostración. (*i*) Supongamos que $x < y$ y que z es negativo. De la Proposición 2.9 sabemos entonces que $-z$ es positivo y podemos calcular que

$$\begin{aligned} -(x \cdot z) &= x \cdot (-z) && \text{de acuerdo a la Proposición 2.3} \\ &< y \cdot (-z) && \text{porque } -z \text{ es positivo y vale la Proposición 2.10} \\ &= -(y \cdot z) && \text{otra vez por la Proposición 2.3.} \end{aligned}$$

Usando ahora la Proposición 2.6 podemos concluir que $y \cdot z < x \cdot z$, como queremos.

(*ii*) Supongamos ahora que $x \leq y$ y que z es negativo. Si $x < y$, entonces de la parte (*i*) sabemos que $y \cdot z < x \cdot z$ y, por lo tanto, que $y \cdot z \leq x \cdot z$. Si en cambio es $x = y$, entonces por supuesto es $y \cdot z = x \cdot z$ y, otra vez, $y \cdot z \leq x \cdot z$. Esta última desigualdad vale entonces en cualquier caso, y esto es lo que afirma la proposición. □

Esta proposición tiene un corolario importante:

Corolario 2.12. *En $\mathbb{R}$ es $0 < 1$.*

Demostración. Si fuera $1 < 0$, entonces de acuerdo a la primera parte de la Proposición 2.11 tendríamos que también $0 = 0 \cdot 1 < 1 \cdot 1 = 1$, lo que es absurdo. Como 1 es distinto de 0, la única positivo entonces es que sea $0 < 1$. □

En la Proposición 2.6 describimos cómo interactúa la función $x \in \mathbb{R} \mapsto -x \in \mathbb{R}$ con las desigualdades. Nuestras siguientes proposiciones dan resultados análogos pero para la función $x \in \mathbb{R} \setminus \{0\} \mapsto x^{-1} \in \mathbb{R} \setminus \{0\}$.

Proposición 2.13. *Sean x e y dos elementos de $\mathbb{R}$.*

(*i*) *Si $0 < x$, entonces $0 < x^{-1}$.*

(*ii*) *Si $0 < x < y$, entonces $0 < y^{-1} < x^{-1}$.*

(*iii*) *Si $0 < x \leq y$, entonces $0 < y^{-1} \leq x^{-1}$.*

Notemos que en estas tres afirmaciones las hipótesis implican que $x \neq 0$ e $y \neq 0$, de manera que x e y tienen elementos inversos en $\mathbb{R}$ y, por lo tanto, podemos hablar de x^{-1} y de y^{-1}.

Demostración. (*i*) Supongamos que $0 < x$. Si fuera $x^{-1} \leq 0$, como x es positivo tendríamos de la Proposición 2.10 que $1 = x^{-1} \cdot x \leq 0 \cdot x = 0$, lo que contradice al Corolario 2.12: esto implica que debe ser $0 < x^{-1}$.

(*ii*) Supongamos ahora que $0 < x < y$. Como $0 < x$ y $0 < y$, de la Definición 1.28 sabemos que

$$0 < x \cdot y. \tag{2.5}$$

Si fuera $x^{-1} \leq y^{-1}$, tendríamos que

$$\begin{aligned}
y &= 1 \cdot y && \text{porque 1 es neutro para el producto} \\
&= x^{-1} \cdot x \cdot y && \text{porque } x^{-1} \text{ es inverso de } x \\
&\leq y^{-1} \cdot x \cdot y && \text{por la hipótesis, la desigualdad (2.5) y la Proposición 2.10} \\
&= x \cdot y^{-1} \cdot y && \text{porque el producto es conmutativo} \\
&= x \cdot 1 && \text{porque } y^{-1} \text{ es inverso de } y \\
&= x && \text{porque 1 es neutro para el producto,}
\end{aligned}$$

y esto es absurdo, ya que estamos suponiendo que $x < y$. Debe ser entonces $y^{-1} < x^{-1}$, como afirma la proposición.

(*iii*) Supongamos finalmente que es $0 < x \leq y$. Si $x < y$, entonces la hipótesis de (*ii*) se cumple, así que sabemos que $0 < y^{-1} < x^{-1}$. Si, en cambio, es $x = y$, entonces usando (*i*) sabemos que $0 < y^{-1} = x^{-1}$. En cualquiera de los dos casos tenemos que $0 < y^{-1} \leq x^{-1}$, como queremos. □

La segunda condición de la Definición 1.28 dice que el producto de dos elementos positivos de $\mathbb{R}$ es positivo. De hecho, tenemos el siguiente resultado:

Proposición 2.14. *El producto de dos elementos de $\mathbb{R}$ es positivo si y solamente si ambos factores son positivos o ambos son negativos.*

Demostración. Si $x > 0$ e $y > 0$, la Definición 1.28 nos dice que que $x \cdot y > 0$. Si, por otro lado, $x < 0$ e $y < 0$, entonces de acuerdo a la Proposición 2.9 es $0 < -x$ y $0 < -y$, así que usando la Definición 1.28 y la segunda parte de la Proposición 2.3 vemos que otra vez $0 < (-x) \cdot (-y) = x \cdot y$. Esto prueba la suficiencia de la condición del enunciado.

Supongamos ahora que $x \cdot y > 0$. No puede ser $x = 0$, porque sabemos que $x \cdot y$ no es nulo. Si x es positivo, entonces x^{-1} también lo es, de acuerdo a la Proposición 2.13, y entonces

$$\begin{aligned}
y &= 1 \cdot y && \text{porque 1 es neutro para el producto} \\
&= x^{-1} \cdot x \cdot y && \text{porque } x^{-1} \text{ es inverso de } x \\
&> x^{-1} \cdot 0 && \text{porque } x \cdot y > 0 \text{ y vale la segunda condición de la Definición 1.28} \\
&= 0 && \text{por la Proposición 2.2.}
\end{aligned}$$ □

Por otro lado, si x es negativo, entonces $-x$ es positivo, como sabemos, y es $(-x) \cdot (-y) = x \cdot y > 0$, así que lo que ya hicimos nos dice que $-y$ es positivo y, por lo tanto, que y es negativo. Vemos así

que si $x \cdot y > 0$ entonces y es positivo si x lo es positivo, y que es negativo si x lo es. Esto prueba la necesidad de la condición del enunciado.

Ejercicio 2.15. Determine condiciones necesarias y suficientes sobre dos elementos x e y de $\mathbb{R}$ para que sea el producto $x \cdot y$ sea no negativo.

Usando los elementos positivos de $\mathbb{R}$ podemos dar una caracterización del supremo e ínfimo de un conjunto:

Proposición 2.16. *Sea A un subconjunto no vacío y acotado superiormente de $\mathbb{R}$. Un elemento α de $\mathbb{R}$ es el supremo de A en $\mathbb{R}$ si y solamente si*

- *es una cota superior para A en $\mathbb{R}$ y*
- *para todo elemento positivo ϵ de $\mathbb{R}$ existe hay un elemento a en A tal que $\alpha - \epsilon < a$.*

Demostración. Sea α un elemento de $\mathbb{R}$. Supongamos primero que α es el supremo de A en $\mathbb{R}$. Se trata entonces ciertamente de una cota superior para A en $\mathbb{R}$. Por otro lado, si ϵ es un elemento positivo de $\mathbb{R}$, de manera que $\epsilon > 0$, entonces $\alpha - \epsilon < \alpha$ y, por lo tanto, $\alpha - \epsilon$ no es una cota superior para A: esto es, hay un element a en A tal que $\alpha - \epsilon < a$. Esto prueba que las dos condiciones de la proposición son necesarias.

Veamos que son suficientes. Supongamos que α es un elemento de $\mathbb{R}$ que satisface esas dos condiciones. Si β es un elemento de $\mathbb{R}$ tal que $\beta < \alpha$, entonces $\alpha - \beta$ es un elemento positivo de $\mathbb{R}$ y, por lo tanto la hipótesis nos dice que hay un elemento a en A tal que $\beta = \alpha - (\alpha - \beta) < a$: así, β no es una cota superior para A. Esto prueba que α es el supremo de A en $\mathbb{R}$, ya que, por hipótesis, es una cota superior para él. □

Ejercicio 2.17. Dé una caracterización similar para el ínfimo de un subconjunto no vacío y acotado inferiormente de $\mathbb{R}$.

Terminemos esta sección construyendo la función *valor absoluto*:

Definición 2.18. Si x es un elemento de $\mathbb{R}$, entonces el ***valor absoluto*** o el ***módulo*** de x es

$$|x| \coloneqq \begin{cases} x & \text{si } x \geq 0; \\ -x & \text{en caso contrario.} \end{cases}$$

Como veremos, esta función cumple un rol fundamental en todo lo que haremos más tarde. Demos, por ahora, sus propiedades básicas.

Proposición 2.19. *Si x e y son dos elementos de $\mathbb{R}$, entonces*

$$|x| \geq 0, \tag{2.6}$$
$$|x| = |-x|, \tag{2.7}$$
$$|x| = \max\{x, -x\}, \tag{2.8}$$
$$|x| = 0 \iff x = 0, \tag{2.9}$$
$$|x \cdot y| = |x| \cdot |y|, \tag{2.10}$$
$$|x + y| \leq |x| + |y|. \tag{2.11}$$

Esta última desigualdad es conocida como la ***desigualdad triangular***. Notemos que la igualdad (2.8) implica inmediatamente que $x \leq |x|$ y que $-x \leq |x|$ cualquiera sea x en $\mathbb{R}$.

Demostración. Si $x \geq 0$, entonces $|x| = x$ es positivo, y si en cambio $x < 0$, entonces $|x| = -x$ es positivo, de acuerdo a la Proposición 2.9. En cualquiera de los dos casos vemos que $|x|$ es positivo, y esto prueba la desigualdad (2.6).

Si $x > 0$, entonces $-x < 0$ y tenemos que $|x| = x = -(-x) = |-x|$. De manera simétrica, si $x < 0$, entonces $-x > 0$ y es $|x| = -x = |-x|$. Finalmente, si $x = 0$, entonces $x = -x$ y, por supuesto, también en este caso tenemos que $|x| = |-x|$. Esto prueba la igualdad (2.7).

Si $x \geq 0$, entonces $-x \leq 0$, así que $-x \leq x$ y, por lo tanto, $|x| = x = \max\{x, -x\}$. Si en cambio es $x < 0$, entonces $-x > 0$, así que $-x > x$ y $|x| = -x = \max\{x, -x\}$. Esto prueba (2.8).

Si $x = 0$, entonces ciertamente es $x \geq 0$ y, por lo tanto, $|x| = x = 0$. Por otro lado, si $x \neq 0$, entonces o bien $x > 0$ o bien $x < 0$, y entonces tenemos que o bien $|x| = x > 0$ o bien $|x| = -x > 0$: en cualquera de los dos casos es $|x| \neq 0$. Esto prueba la equivalencia (2.9).

Para probar la igualdad (2.10) consideramos tres casos.

- Si $x \cdot y$ es positivo, entonces $|x \cdot y| = x \cdot y$ y la Proposición 2.14 nos dice que x e y son o bien los dos positivos, o bien los dos negativos. En el primer caso tenemos que $|x| = x$, $|y| = y$ y, por lo tanto, que $|x \cdot y| = x \cdot y = |x| \cdot |y|$. En el segundo caso, tenemos que $|x| = -x$, $|y| = -y$ y, en consecuencia, que $|x \cdot y| = x \cdot y = (-x) \cdot (-y) = |x| \cdot |y|$.
- Si $x \cdot y$ es nulo, entonces la Proposición 2.2 nos dice que alguno de x o y es nulo y, entonces, usando (2.7) sabemos que alguno de $|x|$ o $|y|$ es nulo, así que también lo es el producto $|x| \cdot |y|$. Es entonces $|x \cdot y| = |x| \cdot |y|$.
- Finalmente, supongamos que $x \cdot y$ es negativo. Entonces $(-x) \cdot y$ es positivo, porque es igual a $-(x \cdot y)$, y lo que ya probamos implica que $|x \cdot y| = |-(x \cdot y)| = |(-x) \cdot y| = |-x| \cdot |y| = |x| \cdot |y|$.

Probemos, para terminar, la desigualdad (2.11). Como $x \leq |x|$ e $y \leq |y|$, es $x + y \leq |x| + |y|$. De manera similar, como $-x \leq |x|$ y $-y \leq |y|$, tenemos que $-(x + y) = -x - y \leq |x| + |y|$. Estas dos desigualdades nos dicen que $|x| + |y|$ es una cota superior para el conjunto $\{x + y, -(x + y)\}$, así que es $|x + y| = \max\{x + y, -(x + y)\} \leq |x| + |y|$, como queremos. □

El siguiente resultado nos da dos criterios útiles para probar acotar el valor absoluto de un elemento de $\mathbb{R}$:

Proposición 2.20. *Si x e y son dos elementos de $\mathbb{R}$, entonces*

$$|x| \leq y \iff -y \leq x \leq y, \qquad |x| \geq y \iff x \geq y \text{ o } x \leq -y, \tag{2.12}$$

$$|x| < y \iff -y < x < y, \qquad |x| > y \iff x < -y \text{ o } x > y. \tag{2.13}$$

Demostración. Supongamos primero que $|x| \leq y$. Como $x \leq |x|$, tenemos que $x \leq y$, y como $-x \leq |x|$, tenemos que que $-x \leq y$ y, por lo tanto, que $-y \leq x$. Vemos así que $-y \leq x \leq y$. Recíprocamente, si suponemos que $-y \leq x \leq y$, entonces tenemos que $x \leq y$ y que $-x \leq y$, así que y es una cota superior para el conjunto $\{x, -x\}$ y, en consecuencia, $|x| = \max\{x, -x\} \leq y$. Esto prueba la primera equivalencia de (2.12).

Supongamos ahora que $|x| < y$. Como $x \leq |x|$, es $x < y$, y como $-x \leq |x|$, es $-x < y$, así que $-y < x$: esto prueba que $-y < x < y$. Por otro lado, si $-y < x < y$, entonces es $-y \leq x \leq y$, así que por lo que ya probamos es $|x| \leq y$. Si fuera $|x| = y$ tendríamos que y pertenece a $\{x, -x\}$ y que, entonces, es igual a x o a $-x$, lo que es absurdo. Vemos así que debe ser $|x| < y$. Esto pruba la primera equivalencia de (2.13).

Para probar las segundas equivalencias de (2.12) y (2.13) es suficiente observar ahora que se trata de las afirmaciones contrarrecíprocas de las primeras equivalencias de (2.13) y de (2.12). □

Ejercicio 2.21. Pruebe que cualesquiera sean los elementos x, y y z de $\mathbb{R}$ se tiene que

$$\big||x|\big| = |x|,$$
$$|x - y| = 0 \iff x = y,$$
$$|x - z| \leq |x - y| + |y - z|,$$
$$|x - y| \geq \big||x| - |y|\big|.$$

Ejercicio 2.22. Si x es un elemento de $\mathbb{R}$, el ***signo*** es

$$\operatorname{sgn}(x) = \begin{cases} 1 & \text{si } x > 0; \\ 0 & \text{si } x = 0; \\ -1 & \text{si } x < 0. \end{cases}$$

Pruebe que para todo $x \in \mathbb{R}$ vale que $x = |x| \cdot \operatorname{sgn}(x)$ y $|x| = x \cdot \operatorname{sgn}(x)$, y que si x no es nulo se tiene entonces que

$$\operatorname{sgn}(x) = \frac{x}{|x|} = \frac{|x|}{x},$$

2.4. Números naturales, enteros y racionales

2.4.1. Números naturales

Por el principio de recurrencia, sabemos que hay exactamente una función $v : \mathbb{N}_0 \to \mathbb{R}$ tal que $v(0) = 0$ y que satisface, para cada $n \in \mathbb{N}$, la condición.

$$v(n+1) = v(n) + 1$$

Notemos que cuando aquí escribimos «$v(0) = 0$» el 0 que aparece a la izquierda del signo igual es el elemento 0 de $\mathbb{N}_0$, mientras que el que está a la derecha es el elemento 0 de $\mathbb{R}$. De manera similar en la igualdad «$v(n+1) = v(n) + 1$» el 1 y la operación + que aparecen a la izquierda son los de $\mathbb{N}_0$, mientras que los que están a la derecha son los de nuestro cuerpo ordenado y completo $\mathbb{R}$.

Proposición 2.23. *Siempre que n y m son elementos de $\mathbb{N}_0$ se tiene que*

$$v(n+m) = v(n) + v(m), \qquad v(n \cdot m) = v(n) \cdot v(m).$$

Demostración. Para cada elemento m de $\mathbb{N}_0$ sean $\mathscr{P}(m)$ y $\mathscr{Q}(n)$ las afirmaciones

$$\textit{para todo } n \in \mathbb{N}_0 \textit{ es } v(n+m) = v(n) + v(m)$$

y

$$\textit{para todo } n \in \mathbb{N}_0 \textit{ es } v(n \cdot m) = v(n) \cdot v(m).$$

Para todo $n \in \mathbb{N}_0$ se tiene que

$$v(n+m) = v(n+0) = v(n) = v(n) + 0 = v(n) + v(m),$$

y esto nos dice que la afirmación $\mathscr{P}(0)$ vale. Supongamos, por otro lado, que m es un elemento de $\mathbb{N}_0$ tal que la afirmación $\mathscr{P}(m)$ vale. En ese caso, si n es un elemento cualquiera de $\mathbb{N}_0$ tenemos que

$$\begin{aligned} v(n+m+1) &= v(n+m) + 1 && \text{por la definición de } v \\ &= v(n) + v(m) + 1 && \text{porque vale la afirmación } \mathscr{P}(m) \\ &= v(n) + v(m+1) && \text{por la definición de } v \end{aligned}$$

y, por lo tanto, vale la afirmación $\mathscr{P}(m+1)$. El principio de inducción, entonces, nos dice que vale la afirmación $\mathscr{P}(m)$ cualquiera sea $m \in \mathbb{N}_0$: esto prueba la afirmación de la proposición que involucra sumas.

Si n es un elemento de $\mathbb{N}_0$, entonces

$$v(n \cdot 0) = v(0) = 0 = v(n) \cdot 0 = v(n) \cdot v(0),$$

así que vale la afirmación $\mathscr{Q}(0)$. Supongamos ahora que m es un elemento de $\mathbb{N}_0$ tal que la afirmación $\mathscr{Q}(m)$ es cierta. Si n es un elemento cualquiera de $\mathbb{N}_0$, entonces

$$\begin{aligned} v(n\cdot(m+1)) &= v(n\cdot m+n) \\ &= v(n\cdot m)+v(n) && \text{porque vale la afirmación } \mathscr{P}(n) \\ &= v(n)\cdot v(m)+v(n)\cdot 1 && \text{por vale la afirmación } \mathscr{Q}(m) \\ &= v(n)\cdot\big(v(m)+1\big) && \text{por la ley distributiva} \\ &= v(n)\cdot v(m+1) && \text{por la definición de } v, \end{aligned}$$

y estonos dice que vale la afirmación $\mathscr{Q}(m+1)$. Otra vez, por el principio de inducción podemos concluir que la afirmación $\mathscr{Q}(m)$ vale cualquiera sea $m \in \mathbb{N}_0$. Esto prueba la afirmación de la proposición que involucra productos. □

Esta proposición nos dice que la función v preserva sumas y productos. Usándola podemos probar que además preserva y refleja desigualdades.

Corolario 2.24. *La función $v : \mathbb{N}_0 \to \mathbb{R}$ es estrictamente creciente. Más aún, si n y m son dos elementos de $\mathbb{N}_0$, entonces vale que*

$$n < m \iff v(n) < v(m).$$

En particular, se tiene que $v(n) > 0$ para todo $n \in \mathbb{N}$.

Notemos que esta última afirmación es en efecto un caso particular de la primera — basta tomar $m = 0$ en esta última para obtener aquella.

Demostración. Probemos, para empezar, la última afirmación del corolario, esto es, que para todo $n \in \mathbb{N}$ se tiene que $v(n) > 0$. Esto es cierto si $n = 1$, ya que

$$v(1) = v(0+1) = v(0)+1 = 0+1 = 1 > 0.$$

Por otro lado, si n es un elemento de $\mathbb{N}$ tal que $v(n) > 0$, entonces

$$v(n+1) = v(n)+1 > 0+1 = 1 > 0.$$

Lo que queremos probar se sigue entonces de esto y del principio de inducción.

Probemos ahora la primera afirmación del corolario. Sean n y m dos elementos de $\mathbb{N}_0$. Si $n < m$, entonces $d \coloneqq m - n \in \mathbb{N}$ y, en vista de lo que ya hicimos y del la Proposición 2.23, tenemos que

$$v(m) = v(n+(m-n)) = v(n+d) = v(n)+v(d) > v(n)+0 = v(n).$$

Por otro lado, si $n \geq m$, entonces o bien $n = m$ y en ese caso por supuesto $v(n) = v(m)$, o bien $n > m$, y en ese caso sabemos que $v(n) > v(m)$: en cualquiera caso tenemos que $v(n) \geq v(m)$. Esto prueba la implicación contrarrecíproca de $v(n) < v(m) \implies n < m$, y completa la prueba del corolario. □

Podemos mejorar la última afirmación de este corolario:

Corolario 2.25. *Para todo elemento n de $\mathbb{N}$ se tiene que $v(n) \geq 1$.*

Demostración. En efecto, si n es un elemento de $\mathbb{N}$, entonces o bien $n = 1$, así que

$$v(n) = v(1) = v(0+1) = v(0) + 1 = 1 = 0 + 1,$$

o bien $n > 1$, así que el Corolario 2.24 implica que $v(n) > v(1) = 1$. En cualquiera de los dos casos tenemos que $v(n) \geq 1$. □

Por otro lado, el Corolario 2.24 tiene la siguiente consecuencia inmediata:

Corolario 2.26. *La función $v : \mathbb{N}_0 \to \mathbb{R}$ es inyectiva.*

Demostración. En efecto, si n y m son dos elementos distintos de $\mathbb{N}_0$, entonces o bien $n < m$ o bien $m < n$, y en entonces el corolario nos dice que o bien $v(n) < v(m)$ o bien $v(m) < v(m)$ y que, en cualquier caso, es $v(n) \neq v(m)$. □

Desde ahora haremos la convención de *identificar* a cada elemento n de $\mathbb{N}_0$ con su imagen $v(n)$ por la función $v : \mathbb{N}_0 \to \mathbb{R}$, y tomaremos el punto de vista de que el conjunto $v(\mathbb{N}_0)$ *es* el conjunto $\mathbb{N}_0$. Notemos que el hecho de que la función v sea inyectiva hace que esto no introduzca ninguna ambigüedad, ya que garantiza que cada elemento de $v(\mathbb{N}_0)$ es la imagen por v de exactamente un elemento de $\mathbb{N}_0$. La Proposición 2.23 nos dice que esta identificación preserva las operaciones aritméticas: sumar o multiplicar dos elementos de $\mathbb{N}_0$ en $\mathbb{N}_0$ o, vía nuestra identificación, en $\mathbb{R}$ da el mismo resultado. De manera similar, el Corolario 2.24 nos dice que la relación de orden entre dos elementos de $\mathbb{N}_0$ es exactamante la misma que la relación de sus correspondientes elementos en $\mathbb{R}$.

La propiedad más importante que tiene el subconjunto $\mathbb{N}_0$ de $\mathbb{R}$ es la siguiente:

Proposición 2.27. *Si x e y son elementos de $\mathbb{R}$ y x es positivo, entonces existe $n \in \mathbb{N}_0$ tal que $y < n \cdot x$.*

Llamamos a esto la ***propiedad arquimediana*** de $\mathbb{R}^n$. Para probarla haremos uso por primera vez del hecho de que $\mathbb{R}$ es completo como cuerpo ordenado.

Demostración. Sean x e y dos elementos de $\mathbb{R}$, supongamos que x es positivo, y supongamos que, por el contrario, tenemos que $y \geq n \cdot x$ para todo $n \in \mathbb{N}_0$. Esto nos dice que el subconjunto $A \coloneqq \{n \cdot x : n \in \mathbb{N}_0\}$ de $\mathbb{R}$, que claramente no es vacío, tiene a y como cota superior en $\mathbb{R}$ y que es, por lo tanto, acotado superiormente. Como $\mathbb{R}$ es un completo con respecto a su relación de orden, el conjunto A admite un supremo. Sea $\alpha \coloneqq \sup A$.

Como x es positivo, tenemos que $-x < 0$ y por lo tanto, que $\alpha - x < \alpha + 0 = \alpha$. Como α es el supremo de A, sabemos que esto implica que $\alpha - x$ no es una cota superior para A en $\mathbb{R}$ y, en consecuencia, que existe un elemento de A estrictamente mayor que $\alpha - x$, esto es, que existe $n \in \mathbb{N}_0$ tal que $\alpha - x < n \cdot x$. Tenemos entonces que

$$\alpha = \alpha - x + x < n \cdot x + x = (n+1) \cdot x \in A,$$

y esto es absurdo, ya que α es una cota superior para A. Esta contradicción provino de haber supuesto que $y \geq n \cdot x$ para todo $n \in \mathbb{N}_0$ y, por lo tanto, esta afirmación es falsa y la proposición es cierta. □

Un caso particular de la propiedad arquimediana que usamos con frecuencia es el siguiente:

Corolario 2.28. *Si y es un elemento de $\mathbb{R}$, entonces existe $n \in \mathbb{N}_0$ tal que $y \leq n$.*

Demostración. En efecto, si y es un elemento de $\mathbb{R}$, entonces la Proposición 2.27 nos dice, ya que 1 es positivo, que existe $n \in \mathbb{N}_0$ tal que $y < n \cdot 1 = n$. □

A su vez, este corolario tiene la siguiente consecuencia:

Corolario 2.29. *El conjunto $\mathbb{R}$ no es acotado superiormente.*

Demostración. Si, por el contrario, hubiera una cota superior y para $\mathbb{R}$ en $\mathbb{R}$, el corolario nos diría que hay un elemento n de $\mathbb{N}_0$ tal que $y \leq n$ y, por lo tanto, tendríamos que $y \leq n = n + 0 < n + 1$: esto es absurdo, ya que si y es una cota superior para $\mathbb{R}$ debe ser $n + 1 \leq y$. □

Otra forma en la que usamos frecuentemente la propiedad arquimediana es la que da la siguiente proposición:

Proposición 2.30. *Si x es un elemento positivo de $\mathbb{R}$, entonces existe $n \in \mathbb{N}$ tal que $x > 1/n$.*

Demostración. En efecto, si x es un elemento positivo de $\mathbb{R}$, entonces $1/x$ también lo es, y el Corolario 2.28 nos dice que hay un elemento n de $\mathbb{N}_0$ tal que $1/x < n$. Notemos que de esto y de $1/x > 0$ se deduce que $n > 0$ y, en particular, que n no es nulo, así que podemos considerar su inverso. De acuerdo a la Proposición 2.13, tenemos que $1/n < 1/(1/x) = x$. □

Usando esta proposión podemos dar una versión útil de la Proposición 2.16:

Ejercicio 2.31. Sea A un subconjunto no vacío y acotado superiormente de $\mathbb{R}$. Muestre que un elemento α de $\mathbb{R}$ es el supremo de A en $\mathbb{R}$ si y solamente si

- es una cota superior para A en $\mathbb{R}$ y
- para todo elemento n de $\mathbb{N}$ hay un elemento a en A tal que $\alpha - 1/n < a$.

2.4.2. Números enteros

Si x es un elemento de $\mathbb{Z}$ entonces hay dos posibilidades: o bien es $x \geq 0$, de manera que x pertenece a $\mathbb{N}_0$ y podemos considerar su imagen $v(-x)$ en $\mathbb{R}$, como en la sección anterior, o bien es $x < 0$, y en ese caso $-x$ es un elemento de $\mathbb{N}_0$ y podemos considerar el elemento $-v(-x)$ opuesto a la imagen de $-x$ por v. Así, hay una función $\zeta : \mathbb{Z} \to \mathbb{R}$ que en cada entero $x \in \mathbb{Z}$ toma el valor

$$\zeta(x) = \begin{cases} v(x) & \text{si } x \geq 0; \\ -v(-x) & \text{si } x < 0. \end{cases}$$

Esta función tiene propiedades similares a las de la función v de la sección anterior. Como ζ está definida «por partes», establecer esas propiedades es un poco laborioso, como veremos.

Las siguientes dos proposiciones se ocupan de los análogos a la Proposición 2.23. Empecemos por la compatibilidad con la suma:

Proposición 2.32. *Siempre que x e y son elementos de $\mathbb{Z}$ se tiene que $\zeta(x + y) = \zeta(x) + \zeta(y)$.*

Demostración. Sean x e y dos elementos de $\mathbb{Z}$. Consideramos varios casos:

(*i*) Si $x \geq 0$ e $y \geq 0$, entonces es $x + y \geq 0$, así que tenemos que

$$\zeta(x + y) = v(x + y) = v(x) + v(y) = \zeta(x) + \zeta(y).$$

(*ii*) Si $x \geq 0$ e $y < 0$, hay dos posibilidades:

- o bien y $x + y \geq 0$, y entonces

  $$\zeta(x + y) + \zeta(-y) = v(x + y) + v(-y) = v(x + y + (-y)) = v(x),$$

  de manera que

  $$\zeta(x + y) = v(x) + (-v(-y)) = \zeta(x) + \zeta(y),$$

- o bien es $x + y < 0$, y entonces

  $$v(-y) = v((-(x + y)) + x) = v(-(x + y)) + v(x),$$

  por lo que

  $$\zeta(x + y) = -v(-(x + y)) = v(x) + (-(v(-y))) = \zeta(x) + \zeta(y).$$

En cualquiera de las dos tenemos que $\zeta(x+y) = \zeta(x) + \zeta(y)$.

(*iii*) Si $x < 0$ e $y \geq 0$, entonces

$$\zeta(x+y) = \zeta(y+x) = \zeta(y) + \zeta(x) = \zeta(x) + \zeta(x),$$

usando en la primera y tercera igualdades la conmutatividad de la suma de $\mathbb{N}_0$ y de $\mathbb{R}$, respectivamente, y en la segunda lo que probamos en (*ii*).

(*iv*) Finalmente, si $x < 0$ e $y < 0$, entonces $x + y < 0$ y, por lo tanto,

$$\begin{aligned}\zeta(x) + \zeta(y) &= (-v(-x)) + (-v(-y)) = -(v(-x) + v(-y)) = -v((-x) + (-y)) \\ &= -v(-(x+y)) = \zeta(x+y).\end{aligned}$$

Como estos cuatro casos cubren todas las posibilidades, vemos que la afirmación de la proposición es cierta. □

En segundo lugar, mostremos cómo la función ζ es compatible con los productos de $\mathbb{Z}$ y de $\mathbb{R}$.

Proposición 2.33. *Siempre que x e y son elementos de $\mathbb{Z}$ se tiene que $\zeta(x \cdot y) = \zeta(x) \cdot \zeta(y)$.*

Demostración. Sean x e y dos elementos de $\mathbb{Z}$. Otra vez consideramos varios casos.

(*i*) Si alguno de los dos es nulo, entonces por un lado es $x \cdot y = 0$ y, por otro, alguno de $\zeta(x)$ o $\zeta(y)$ es nulo, de manera que tambien $\zeta(x) \cdot \zeta(y) = 0$.

(*ii*) Si $x > 0$ e $y > 0$, entonces $x \cdot y > 0$ y

$$\zeta(x \cdot y) = v(x \cdot y) = v(x) \cdot v(y) = \zeta(x) \cdot \zeta(y).$$

(*iii*) Si $x > 0$ e $y < 0$, entonces $x \cdot y < 0$, $-y > 0$ y

$$\begin{aligned}\zeta(x \cdot y) &= -v(-(x \cdot y)) = -v(x \cdot (-y)) = -v(x) \cdot v(-y) = v(x) \cdot (-v(-y)) \\ &= \zeta(x) \cdot \zeta(y).\end{aligned}$$

(*iv*) De manera similar, si $x < 0$ e $y > 0$, entonces $x \cdot y < 0$, $-x > 0$ y

$$\begin{aligned}\zeta(x \cdot y) &= -v(-(x \cdot y)) = -v((-x) \cdot y) = -v(-x) \cdot v(y) = (-v(x)) \cdot v(-y) \\ &= \zeta(x) \cdot \zeta(y).\end{aligned}$$

(*v*) Finalmente, si $x < 0$ e $y < 0$, entonces $x \cdot y > 0$, $-x > 0$ y $-y > 0$, así que

$$\begin{aligned}\zeta(x \cdot y) &= v(x \cdot y) = v((-x) \cdot (-y)) = v(-x) \cdot v(-y) = (-v(-x)) \cdot (-v(-y)) \\ &= \zeta(x) \cdot \zeta(y),\end{aligned}$$

Vemos así que en cualquiera de los cinco casos — que cubren todas las posibilidades — vale la igualdad que afirma la proposición. □

Ahora nos ocupamos de la versión del Corolario 2.24 para la función ζ.

Proposición 2.34. *La función $\zeta : \mathbb{Z} \to \mathbb{R}$ es estrictamente creciente. Más aún, si x y y son dos elementos de $\mathbb{Z}$, entonces vale que*

$$x < y \iff \zeta(x) < \zeta(y).$$

Demostración. Sean x e y dos elementos de $\mathbb{Z}$ y supongamos primero que $x < y$, de manera que el entero $y - x$ es positivo. En ese caso, de acuerdo a la Proposición 2.32, tenemos que

$$0 < \zeta(x - y) = \zeta(y) - \zeta(x)$$

y, por lo tanto, que $\zeta(x) < \zeta(y)$. Por otro lado, si $x \geq y$, de manera que el entero $x - y$ es un elemento de $\mathbb{N}_0$, entonces

$$\zeta(x) - \zeta(y) = \zeta(x - y) \geq 0,$$

con lo que ahora es $\zeta(x) \geq \zeta(y)$. Vemos así que vale la implicación $x \geq y \implies \zeta(x) \geq \zeta(y)$, que es la contrarrecíproca de la implicación $\zeta(x) < \zeta(y) \implies x < y$. □

La Proposición 2.34 tiene la siguiente consecuencia inmediata:

Corolario 2.35. *La función $\zeta : \mathbb{Z} \to \mathbb{R}$ es inyectiva.*

Demostración. En efecto, si x e y son dos elementos de $\mathbb{Z}$ tales que $\zeta(x) = \zeta(y)$, entonces la proposición implica que ni $x < y$ ni $y < x$, así que necesariamente debe ser $x = y$. □

Gracias a este corolario, podemos hacer con $\mathbb{Z}$ lo mismo que hicimos con $\mathbb{N}$ en la sección anterior: desde ahora identificaremos a cada entero $x \in \mathbb{Z}$ con su imagen $\zeta(x)$ en $\mathbb{R}$ por la función ζ. Como la función ζ es inyectiva, esto no introduce ninguna ambigüedad en lo que hacemos, y de acuerdo a las Proposiciones 2.32, 2.33 y 2.34 esta identificación es compatible con las operaciones aritméticas de $\mathbb{Z}$ y con la relación de orden usual sobre ese conjunto.

Una propiedad importante del subconjunto $\mathbb{Z}$ de $\mathbb{R}$ es que para sus subconjuntos vale el siguiente resultado:

Proposición 2.36. *Un subconjunto no vacío de $\mathbb{Z}$ que es acotado en $\mathbb{R}$ posee máximo.*

Recordemos que que $\mathbb{R}$ sea un cuerpo ordenado completo nos dice que un tal subconjunto posee necesariamente supremo en $\mathbb{R}$.

Demostración. Sea A un subconjunto no vacío de $\mathbb{Z}$ que es acotado en $\mathbb{R}$, de manera que podemos considerar su supremo $\alpha := \sup A$ en $\mathbb{R}$. Como $\alpha - 1 < \alpha$, sabemos que $\alpha - 1$ no es una cota superior para A, así que hay un elemento a en A tal que $\alpha - 1 < a$.

Afirmamos que a es una cota superior para A en $\mathbb{R}$ y, por lo tanto, un máximo de A, ya que pertence a A. Para verlo, supongamos que, por el contreario, no lo es, de manera que existe un elemento b en A tal que $a < b$. En ese caso la diferencia $b - a$ es un elemento de $\mathbb{Z}$, ya que a y b están en $\mathbb{Z}$, y es positivo, así que $1 \leq b - a$: se sigue de esto y de que $\alpha - 1 < a$ que

$$\alpha = \alpha - 1 + 1 < a + b - a = b,$$

lo que es absurdo, ya que α es una cota superior para A. □

Una aplicacón de esta proposición es la construcción de la función *parte entera*.

Proposición 2.37. *Si x es un elemento de $\mathbb{R}$, entonces existe exactamente un elemento n de $\mathbb{Z}$ tal que $n \leq x < n + 1$. De hecho, n es precisamente el supremo del conjunto $\{m \in \mathbb{Z} : m \leq x\}$.*

Demostración. Sea x un elemento de $\mathbb{R}$ y consideremos el conjunto $S := \{m \in \mathbb{Z} : m \leq x\}$. Es claro que S está acotado superiormente en $\mathbb{R}$ por x. Por otro lado, sabemos que hay un elemento k de $\mathbb{N}$ tal que $-x \leq k$, así que $-k \leq x$ y, por lo tanto $-k \in S$: esto muestra que el conjunto S no es vacío. De acuerdo a la Proposición 2.36, entonces, sabemos que el conjunto S tiene un máximo.

Escribámos n a ese máximo. Como n pertenece a S, es $n \leq x$. Por otro lado, como $n + 1 > n$ y $n = \max S$, no puede ser que $n + 1$ pertenezca a S, así que $x \leq n + 1$. Vemos así que el entero n tiene la propiedad descripta en el enunciado. Para completar la prueba tenemos que mostrar que es el único que la tiene.

Sea n' un elemento de $\mathbb{Z}$ tal que $n' \leq x < n' + 1$. Supongamos que $n < n'$, de manera que $n' - n$ es un elemento de $\mathbb{N}$: como $n' \leq x$ y $x < n + 1$, tenemos que $n' < n + 1$, así que $n' - n < 1$, y esto contradice el Corolario 2.25. De manera similar, si $n' < n$, entonces $n - n'$ es un elemento de $\mathbb{N}$ y, como $n \leq x$ y $x < n' + 1$, es $n < n' + 1$ y $n - n' < 1$, lo que otra vez es absurdo. La única posibilidad, entonces, es que sea $n' = n$. Esto prueba lo que queremos. □

En vista de esta proposición podemos hacer la siguiente definición:

Definición 2.38. Si x es un elemento de $\mathbb{R}$, entonces la ***parte entera*** de x es el único elemento $\lfloor x \rfloor$ de $\mathbb{Z}$ tal que $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$.

Para trabajar con partes enteras es útil tener la siguiente caracterización alternativa.

Proposición 2.39. *Sean x un elemento de $\mathbb{R}$ y n uno de $\mathbb{Z}$. Las siguientes afirmaciones son equivalentes:*

(*a*) $n = \lfloor x \rfloor$.
(*b*) $n \leq x < n + 1$.
(*c*) $x - 1 < n \leq x$.

Demostración. La equivalencia entre (*a*) y (*b*) es consecuencia de la definición de $\lfloor x \rfloor$.

Supongamos que vale (*b*). Como $x < n + 1$, tenemos que $x - 1 < n$, así que $x - 1 < n \leq x$i y vale (*c*). Recíprocamente, si vale (*c*), entonces $x - 1 < n$, así que $x < n + 1$ y, por lo tanto, $n \leq x < n + 1$, es decir, vale (*b*). □

Como ejemplo de cómo manipular expresiones que involucran partes enteras, probemos sus propiedades elementales.

Proposición 2.40.
(*i*) *Para cada* $n \in \mathbb{Z}$ *es* $\lfloor n \rfloor = n$, *y para cada* $x \in \mathbb{R}$ *es* $\lfloor \lfloor x \rfloor \rfloor = \lfloor x \rfloor$.
(*ii*) *Si* $x \in \mathbb{R}$ *y* $n \in \mathbb{Z}$, *entonces*

$$n \leq x \iff n \leq \lfloor x \rfloor, \qquad x < n \iff \lfloor x \rfloor < n, \qquad \lfloor x + n \rfloor = \lfloor x \rfloor + n.$$

(*iii*) *Siempre que* x *e* y *son elementos de* $\mathbb{R}$ *vale que*

$$x \leq y \implies \lfloor x \rfloor \leq \lfloor y \rfloor, \qquad \lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1.$$

Demostración. (*i*) Si n es un elemento de $\mathbb{Z}$, entonces tenemos que $n \leq n < n + 1$, porque $0 < 1$, así que la definición de $\lfloor n \rfloor$ implica inmediatamente que $\lfloor n \rfloor = n$. En particular, si x es un elemento cualquiera de $\mathbb{R}$, entonces $\lfloor x \rfloor$ es uno de $\mathbb{Z}$, así que tenemos que $\lfloor \lfloor x \rfloor \rfloor = \lfloor x \rfloor$.

(*ii*) Sean x y n elementos de $\mathbb{R}$ y de $\mathbb{Z}$, respectivamente. Si $n \leq x$, entonces n pertenece al conjunto $S \coloneqq \{m \in \mathbb{Z} : m \leq x\}$ y, por lo tanto, es $n \leq \sup S = \lfloor x \rfloor$. Recíprocamente, si $n \leq \lfloor x \rfloor$, entonces, como $\lfloor x \rfloor \leq x$, es $n \leq x$. Esto prueba la equivalencia $n \leq \lfloor x \rfloor \iff n \leq x$, que es la primera que aparece en el enunciado, y tambien la segunda, ya que esta es la contrarrecíproca de aquella. Finalmente, como $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$, la monotonía de la suma implica que $\lfloor x \rfloor + n \leq x + n < \lfloor x \rfloor + n + 1$ y, como $\lfloor x \rfloor + n$ es un elemento de $\mathbb{Z}$, esto nos dice que $\lfloor x + n \rfloor = \lfloor x \rfloor + n$.

(*iii*) Sean ahora x e y dos elementos de $\mathbb{R}$. Si $x \leq y$, entonces y es una cota superior para el conjunto $S \coloneqq \{m \in \mathbb{Z} : m \leq x\}$, así que $\lfloor x \rfloor = \sup S \leq y$. Usando la primera parte de la afirmación (*ii*) que acabamos de probar, podemos concluir, entonces, que $\lfloor x \rfloor \leq \lfloor y \rfloor$, ya que $\lfloor x \rfloor$ pertenece a $\mathbb{Z}$. Esto prueba la primera parte de (*iii*).

Como $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$ y $\lfloor y \rfloor \leq y < \lfloor y \rfloor + 1$, tenemos que $\lfloor x \rfloor + \lfloor y \rfloor \leq x + y < \lfloor x \rfloor + \lfloor y \rfloor + 2$. Ahora bien, si $x + y < \lfloor x \rfloor + \lfloor y \rfloor + 1$, tenemos que

$$\lfloor x \rfloor + \lfloor y \rfloor \leq x + y \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$$

y, por lo tanto, que $\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$. Si, por el contrario, es $x + y \geq \lfloor x \rfloor + \lfloor y \rfloor + 1$, entonces

tenemos que

$$\lfloor x \rfloor + \lfloor y \rfloor + 1 \leq x + y \leq \lfloor x \rfloor + \lfloor y \rfloor + 2,$$

así que $\lfloor x+y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor + 1$. En cualquiera de los dos casos vale que $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x+y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$, así que esto prueba la última afirmación de la proposición. □

Ejercicio 2.41. Pruebe que cualquiera sea x en $\mathbb{R}$ vale que

$$\lfloor x \rfloor + \lfloor -x \rfloor = \begin{cases} 0 & \text{si } x \in \mathbb{Z}; \\ -1 & \text{en caso contrario.} \end{cases}$$

Ejercicio 2.42.

(*i*) Muestre que para cada elemento x de $\mathbb{R}$ existe exactamente un elemento n de $\mathbb{Z}$ tal que $n-1 < x \leq n$, al que escribimos $\lceil x \rceil$.

(*ii*) Pruebe que cualesquiera sean $n \in \mathbb{Z}$ y x e y en $\mathbb{R}$ valen las siguientes afirmaciones:

$$\lceil x \rceil = n \iff n-1 < x \leq n \iff x \leq n < x+1,$$

$$\lceil x \rceil = x \iff x \in \mathbb{Z}, \qquad n < x \iff n < \lceil x \rceil,$$

$$x \leq n \iff \lceil x \rceil \leq n, \qquad \lceil x + n \rceil = \lceil x \rceil + n,$$

$$\lceil x \rceil + \lceil y \rceil - 1 \leq \lceil x + y \rceil \leq \lceil x \rceil + \lceil y \rceil, \qquad x \leq y \implies \lceil x \rceil \leq \lceil y \rceil,$$

$$\lceil x \rceil + \lceil -x \rceil = \begin{cases} 0 & \text{si } x \in \mathbb{Z}; \\ 1 & \text{en caso contrario.} \end{cases}$$

(*iii*) Pruebe que para todo $x \in \mathbb{R}$ se tiene que

$$\lfloor x \rfloor \leq \lceil x \rceil, \qquad \lfloor x \rfloor = \lceil x \rceil \iff x \in \mathbb{Z},$$

$$\lfloor x \rfloor + \lceil -x \rceil = 0, \qquad \lceil -x \rceil = -\lfloor x \rfloor,$$

$$\lfloor -x \rfloor = -\lceil x \rceil, \qquad \lceil x \rceil - \lfloor x \rfloor = \begin{cases} 0 & \text{si } x \in \mathbb{Z}; \\ 1 & \text{en caso contrario,} \end{cases}$$

2.4.3. Números racionales

Bibliografía

[BA62] Robert Bourgne and J.-P. Azra, *Ecrits et mémoires mathématiques d'Évariste Galois: Édition critique intégrale de ses manuscrits et publications*, Gauthier-Villars & Cie, Éditeur-Imprimeur-Libraire, Paris, 1962, Préface de J. Dieudonné. MR 150016

[Ded60] Richard Dedekind, *Stetigkeit und irrationale Zahlen*, Friedr. Vieweg & Sohn, Braunschweig, 1960, 6te unveränderte Aufl. MR 114755

[Hil00] David Hilbert, *Über den zahlbegriff.*, Jahresbericht der Deutschen Mathematiker-Vereinigung **8** (1900), 180–183.

[Joh63] Selmer M. Johnson, *Generation of permutations by adjacent transposition*, Math. Comp. **17** (1963), 282–285. MR 159764

[Ste64] Hugo Steinhaus, *One hundred problems in elementary mathematics*, Basic Books, Inc., Publishers, New York, 1964, With a foreword by Martin Gardner. MR 157881

[Tro62] H. F. Trotter, *Algorithm 115: Perm*, Commun. ACM **5** (1962), no. 8, 434–435.

[Web93] H. Weber, *Leopold Kronecker*, Math. Ann. **43** (1893), no. 1, 1–25. MR 1510799

Notaciones

Lista de personas

Índice