Tema 1

Preliminares

1.1. Fundamentos: lógica, conjuntos y aplicaciones

Los contenidos de esta parte, que están en los fundamentos de toda la matemática, se verán de modo extendido en otras asignaturas. Para nuestros propósitos resulta suficiente el Tema 0 del libro de A. Romero, "Álgebra Lineal y Geometría" Ed. La Madraza (1991), en el cual se basa esta sección de los apuntes.

Como notación, usaremos $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ para denotar los números naturales, enteros, racionales y reales, respectivamente.

1.1.1. Algunos elementos y notación de lógica

La Lógica, que subyace en los fundamentos de las Matemáticas, estudia las reglas que permiten hacer razonamientos válidos. Nos restringiremos aquí a algunas ideas intuitivas sobre ella y su lenguaje básico.

Una *proposición* es un enunciado que puede ser verdadero o falso. Partiendo de dos proposiciones p, q, podemos formar otras proposiciones más complejas usando ciertas operaciones lógicas; la verdad o falsedad de cada nueva proposición dependerá de la de p y q, así como de la operación lógica. Concretamente:

- Conjunción: $p \wedge q$, que se lee "p y q".

  Esta proposición es verdadera cuando lo son simultáneamente las dos, p y q, y falsa en caso contrario, esto es, cuando es falsa al menos una de las proposiciones p, q.

- Disyunción: $p \vee q$, que se lee "p ó q".

  Esta proposición es verdadera cuando lo es al menos una de los dos proposiciones p, q y falsa en caso contrario, esto es, cuando son falsas tanto p como q.

- Negación $\neg p$, que se lee "no p".

  Este enunciado es verdadero cuando p es falso, y es falso cuando p es verdadero.

  Nota. En Lógica se supone siempre que si una proposición es verdadera entonces su negación es falsa (y viceversa, de hecho, se entiende que $\neg(\neg p) = p$). Esto no sólo coincide con lo que sugiere nuestra intuición, sino que tiene una raíz más profunda: no es difícil demostrar,

usando reglas lógicas simples, el llamado *principio de explosión*[1]: en el caso de que exista una proposición p tal que p y $\neg p$ sean ciertas, entonces cualquier otra proposición q sería cierta también.

Ejercicio. Discútase si las siguientes afirmaciones son proposiciones y, en caso afirmativo, cuál es su negación en el lenguaje cotidiano: (a) "Puede que llueva mañana", (b) "Esta frase tiene cinco palabras".

- Condicional: $p \Rightarrow q$, que se lee de varios modos alternativos: "si p entonces q", "p implica q", "p es suficiente (o condición suficiente) para q", "q es necesario (o condición necesaria) para p", "q se deduce de p". [2]

  La proposición $p \Rightarrow q$ es verdadera cuando se da uno de los siguientes dos casos[3]: (i) p y q son verdaderas, o (ii) p es falsa, sea q verdadera o no. Así, se tiene:

  (a) Si $p \Rightarrow q$ es verdadera, y p también lo es, entonces q es verdadera. A este modo de razonar se le llama *modus ponendo ponens* ("modo que, afirmando, afirma", entendiendo que al afirmar p se afirma q).

  (b) Si la proposición $p \Rightarrow q$ es verdadera, y q es falsa (esto es, $\neg q$ es verdadera) entonces p es falsa (esto es, $\neg p$ es verdadera). A este modo de razonar se le llama *modus tollendo tollens* ("modo que, negando, niega", entendiendo que al negar q se niega p).

  (c) De los dos puntos anteriores, de deduce que $p \Rightarrow q$ es verdadera si y sólo si lo es $\neg q \Rightarrow \neg p$. A esta última implicación se le llama el *contrarrecíproco* de la primera.

  Para ejercitarse, el lector puede tomar p como la proposición "llueve", q como "la calle está mojada" y aplicar todo lo dicho a la proposición $p \Rightarrow q$ ("si llueve entonces la calle está mojada").

- Condicional recíproco: $p \Leftarrow q$, que se lee "sólo si p entonces q".

  Puede tomarse como una notación alternativa para $q \Rightarrow p$, por lo que se reduce al caso anterior (y puede leerse de modos alternativos similares a los de ese caso).

- Equivalencia: $p \Leftrightarrow q$, que se lee "p equivale a q" o "p si y sólo si q"'.

  Puede tomarse como una notación abreviada de $(p \Rightarrow q) \wedge (p \Leftarrow q)$. Así, $p \Leftrightarrow q$ es verdadera cuando (i) p y q son verdaderas, o (ii) p y q son falsas.

  Como hemos visto, la proposición $p \Rightarrow q$ era equivalente a su contrarrecíproco; esto lo podemos escribir ahora:

  $$(p \Rightarrow q) \iff (\neg p \Leftarrow \neg q),$$

  (por supuesto, el recíproco $p \Leftarrow q$ no es equivalente).

Como notación lógica que también usaremos, se tienen los símbolos:

- Cuantificador universal $\forall$, que se lee "para todo".
- Cuantificador existencial $\exists$, que se lee "existe"; si se escribe $\exists!$ se lee "existe un único".

Estos símbolos se aplicarán a menudo en la próxima sección, lo que servirá como ejemplo de su uso.

[1] En terminología clásica, *ex contradictione quodlibet* (o *ex falso quodlibet*): de la contradicción (se sigue) lo que se quiera.

[2] Para la proposición p se usan nombres como antecedente, prótasis o hipótesis, y para la q consecuente, apódosis o tesis.

[3] Esto no se corresponde totalmente con la idea intuitiva de lo que es una implicación, pero no entraremos en una tal discusión cuyas sutilezas exceden nuestros objetivos.

1.1.2. Conjuntos

Conceptos generales

De manera intuitiva, suficiente para nuestros objetivos, entenderemos por *conjunto* una colección cualquiera de objetos; de cada uno de estos objetos se dirá que es un *elemento* del conjunto. Los elementos de un conjunto pueden determinarse por extensión (esto es, enumerando todos y cada uno de ellos) o por comprensión (enunciando una propiedad que los caracterice inequívocamente). Si X es un conjunto, de cualquiera de sus elementos diremos que *pertenece* a X, lo cual se denota $x \in X$ (equivalentemente, se dice que X *contiene* a x, y se denota $X \ni x$).[4] Diremos que dos conjuntos X, Y son iguales, lo que denotaremos $X = Y$, cuando tienen los mismos elementos, esto es, cuando todo elemento de X también lo es de Y y todo elemento de Y también lo es de X. Así, en notación lógica, $X = Y$ significa:

$$(\forall x \in X, x \in Y) \wedge (\forall y \in Y, y \in X).$$

Dados dos conjuntos A y X, diremos que A es un subconjunto de X si todo elemento de A es un elemento de X, esto es, cuando:

$$\forall x \in A, x \in X, \qquad \text{o, igualmente,} \qquad x \in A \Rightarrow x \in X.$$

En este caso, escribiremos $A \subset X$, que se lee A *incluido* en X (o X incluye a A). Resulta inmediato de las deficiniones que, para cualesquiera conjuntos[5] X, Y:

$$X = Y \qquad \Longleftrightarrow \qquad (X \subset Y) \wedge (Y \subset X)$$

Todo conjunto X admite dos subconconjuntos a los que llamaremos *impropios* el propio conjunto X y el conjunto vacío (esto es, el que no tiene ningún elemento), el cual denotaremos $\emptyset$. Este último se puede admitir sin incurrir en contradicción y resulta útil desde el punto de vista lógico, como se verá más adelante. A cualquier subconjunto de X que no sea impropio, se le llamará *propio*.

Operaciones entre conjuntos

Dado un conjunto X, al conjunto cuyos elementos son todos los subconjuntos de X le llamaremos *conjunto de las partes de* X, y lo denotaremos $\mathcal{P}(X)$. Se tiene así: $A \in \mathcal{P}(X)$ si y sólo si $A \subset X$.

Ejercicio. Dado un número natural n, se define el conjunto $X_n = \{1, 2, \ldots, n\}$. Construir $\mathcal{P}(X_n)$ para $n = 1, 2, 3$. ¿Cuántos elementos tiene? Tratar de generalizar para cualquier valor de n.

Dados $A, B \in \mathcal{P}(X)$, se definen los siguientes subconjuntos de X:

- Intersección, $A \cap B := \{x \in X : (x \in A) \wedge (x \in B)\}$

[4] *Nota.* Para definir los conjuntos, implícitamente se ha supuesto una clase de objetos preexistente. Algunos de estos objetos podrían ser conjuntos previamente definidos, pero no se permite que un conjunto sea elemento de sí mismo (pues no estaría entre los objetos preexistentes) u otras construcciones autorreferentes similares. Lo contrario daría lugar a la conocida *paradoja de Russell*: si a los conjuntos se les permitiera contenerse a sí mismos, entonces podríamos construir el conjunto X de todos los conjuntos que no son elementos de sí mismos; se llega entonces a un absurdo al tratar de determinar si X es un elemento de sí mismo o no (piénsese cuidadosamente qué contradicción ocurriría si se supone que lo es y si se supone que no lo es).

[5] Obsérvese que nuestro uso del símbolo $\subset$ es el mismo que el del símbolo $\subseteq$ (el cual remarca que se puede dar la igualdad). El símbolo $\subsetneq$ denota que se da la inclusión pero no la igualdad (esto es, que la inclusión es *estricta*).

- Unión, $A \cup B := \{x \in X : (x \in A) \bigvee (x \in B)\}$
- Diferencia, $A \setminus B := \{x \in X : (x \in A) \wedge (x \notin B)\}$.

  A la diferencia $X \setminus A$ también se le llama *complementario de A en X*.

Ejercicio. Representar los conjuntos así definidos usando diagramas de Venn (búsquese qué son, si no se conocen).

Nota. A partir de las definiciones anteriores no es difícil definir la intersección o la unión de una colección finita, o incluso infinita, de subconjuntos de X.

Dados dos conjuntos X, Y se define su *producto cartesiano* $X \times Y$ como

$$X \times Y : \{(x,y) : (x \in X) \wedge (y \in Y)\},$$

donde (x,y) es el *par ordenado* formado por x e y (en este orden). Aquí, por par ordenado se entiende un conjunto de dos elementos en el que importa el orden en el que se enumeran; dado (x,y), a x se le llama primer elemento del par, y a y segundo elemento. El producto cartesiano $X \times Y$ es, pues, el conjunto de todos los pares ordenados cuyo primer elemento pertenece a X y cuyo segundo elemento pertenece a Y. [6]

Ejercicio. Explicar la diferencia existente entre los objetos que aparecen en cada caso (a), (b), (c) siguiente: (a) x, $\{x\}$, (x,x); (b) $\{x,y\}$, $\{y,x\}$; (c) (x,y), (y,x).

Ejercicio. Si X e Y tienen un número finito n y m de elementos, respectivamente, ¿cuántos elementos tiene $X \times Y$?

Relaciones binarias

Para definir el concepto de relación binaria en un conjunto X, observemos primero que podemos construir el producto cartesiano $X \times X$ (como un caso particular de la definición general $X \times Y$). Llamaremos *relación binaria* en X a cualquier subconjunto R de $X \times X$. Cuando un par $(x,y) \in X \times X$ pertenezca a X diremos: "x está relacionado con y", y escribiremos $x\mathcal{R}y$.

Algunas posibles propiedades que puede que verifique una relación binaria son:

- *Reflexiva*: todo elemento está relacionado consigo mismo, esto es: $x \in X \Rightarrow x\mathcal{R}x$.
- *Simétrica*: $x\mathcal{R}y \Rightarrow y\mathcal{R}x$.
- *Transitiva*: $(x\mathcal{R}y) \wedge (y\mathcal{R}z) \Rightarrow x\mathcal{R}z$.
- *Antisimétrica:* $(x\mathcal{R}y) \wedge (y\mathcal{R}x) \Rightarrow x = y$.

[6] *Nota.* Aunque la definición anterior de par ordenado es suficiente para nuestros propósitos, es de señalar que la noción de "orden" no ha sido introducida todavía dentro de la teoría de conjuntos. No obstante, se puede definir el par ordenado sin hacer mención explícita al orden, concretamente, $(x,y) := \{\{x\},y\}$. Obsérvese que, conjuntistamente $\{\{x\},y\} = \{y,\{x\}\}$, pero en cualquiera de estas dos expresiones x "se distingue" de y (por lo que se sitúa a x como primera componente del par (x,y)): de hecho, no se considera x en sí mismo como elemento del par, sino el conjunto cuyo único elemento es x.

A partir de esta definición, es fácil formalizar los conjuntos ordenados de un número finito de elementos, que se denominarán ternas, cuadruplas, quintuplas o, en general, n-úplas, según tengan 3, 4, 5 ó n elementos, respectivamente.

Ejercicio. Pónganse ejemplos de dos relaciones que sean a la vez simétricas y antisimétricas, una de ellas que verfique además la propiedad reflexiva, y la otra que no la verifique.

Una relación binaria R se dice que es *de orden* si verifica las propiedades reflexiva, antisimétrica y transitiva. Si en una relación de orden se verifica además:

$$\forall x, y \in X, \quad (x\mathcal{R}y) \vee (y\mathcal{R}x)$$

la relación se llama *de orden total*.

Ejercicio. Compruébese que las siguientes relaciones binarias son relaciones de orden:

(i) En el conjunto $\mathbb{R}$ de los números reales, la relación "ser menor o igual a" (esto es, $\mathcal{R}$ es la relación $\leq$).

(ii) En el conjunto $\mathcal{P}(X)$ de las partes de un conjunto X, la relación 'estar incluido en" (esto es, $\mathcal{R}$ es la relación $\subset$).

¿Es alguna de estas dos relaciones de orden total?

Relaciones de equivalencia

De entre las relaciones binarias, estaremos especialmente interesados en las del siguiente tipo.

Definición 1.1. *Dado un conjunto X, diremos que una relación binaria $R \subset X \times X$ es* de equivalencia *si satisface las propiedades reflexiva, simétrica y transitiva. En este caso, el símbolo $\mathcal{R}$ se sustituirá por el símbolo $\sim$.*

Ejercicio. (i) Se considera en $X = \{1,2,3,4,5,6\}$ la relación binaria $R = \{(1,1),(1,2),(3,5),(6,5)\}$. Se pide completar R hasta una relación de equivalencia, es decir, hallar la única relación binaria R' que verifica las siguientes propiedades: (a) R' incluye a R (esto es, $R \subset R'$), (b) R' es de equivalencia, y (c) R' es la relación binaria más pequeña que verifica estas dos propiedades (más pequeña en el sentido de que si R'' es otra relación binaria que verifica (a) y (b) entonces $R' \subset R''$).

(ii) Discutir si, dado un conjunto arbitrario X y una relación binaria R cualquiera en X, existe una relación binaria R' que complete R hasta una relación de equivalencia (esto es, que satisfaga las propiedades (a), (b) y (c) del apartado anterior).

Definición 1.2. *Sea $(X,\sim)$ un conjunto dotado con una relación de equivalencia. Para cada $x \in X$ se define la* clase de equivalencia de x *por*

$$[x] := \{y \in X : y \sim x\},$$

esto es, $[x]$ es el conjunto de todos los elementos de X que están relacionados[7] *con x. Llamaremos* conjunto cociente $X/\sim$ *al conjunto de todas las clases de equivalencia.*

Obsérvese que cada clase $[x]$ es un subconjunto de X y un elemento de $X/\sim$, y que $X/\sim$ es un subconjunto de $\mathcal{P}(X)$.

Ejercicio. Se considera en $\mathbb{R}^3$ la relación de equivalencia "estar a la misma distancia del origen". Determinar el conjunto cociente.

[7] Debido a la propiedad simétrica, no importa si "estar relacionado" se interpreta en el sentido $x \sim y$, $y \sim x$ o ambos.

Proposición 1.3. *Las clases de equivalencia de* $(X,\sim)$ *verifican:*

(i) $x \in [x]$. *Por tanto, ninguna clase de equivalencia es vacía, y la unión de todas las clases de equivalencia es* X.

(ii) si $y \in [x]$ *entonces* $[x] = [y]$. *En consecuencia, las clases de equivalencia son disjuntas dos a dos, esto es:*

$$[x] \neq [y] \quad \Rightarrow \quad [x] \cap [y] = \emptyset.$$

Demostración. (i) Como por la propiedad reflexiva $x \sim x$, se sigue $x \in [x]$. Así, la clase de un elemento nunca puede ser vacía (pues el propio elemento está en la clase) y la unión de todas las clases es el conjunto X.

(ii) Para demostrar $[y] \subset [x]$, sea $z \in [y]$, esto es, $z \sim y$. Como, por hipótesis, $y \sim x$, aplicando la propiedad transitiva se sigue $z \sim x$, esto es, $z \in [x]$, como se quería.

Para demostrar $[x] \subset [y]$, sea $z \in [x]$, esto es, $z \sim x$. Por hipótesis, $y \sim x$, y por la propiedad simétrica $x \sim y$. Aplicando la propiedad transitiva a $z \sim x$, $x \sim y$, se sigue $z \sim y$, esto es, $z \in [y]$, como se quería.

Para la última afirmación, razonando por el contrarrecíproco si $\exists z \in [x] \cap [y]$ entonces $[z] = [x]$ y $[z] = [y]$ (aplíquese dos veces la afirmación anterior) por lo que $[x] = [y]$, como se quería. □

Como consecuencia de la proposición 1.3, las clases de equivalencia que forman $X/\sim$ satisfacen:

(1) No son vacías.

(2) Son disjuntas dos a dos.

(3) Su unión es todo X.

En general, dado el conjunto X, una *partición* P de X es una colección de subconjuntos de X que satisfacen las propiedades (1), (2) y (3). La proposición anterior implica por tanto que el conjunto cociente $X/\sim$ es una partición de X. El siguiente ejercicio muestra que, de hecho, toda partición de X puede verse como el conjunto cociente para una $\sim$ canónicamente determinada.

Ejercicio. Sea P una partición de X, y se considera la relación binaria en X: "x está relacionado con y si y sólo si x, y pertenecen a un mismo elemento de P". Demostrar que esta relación binaria es de equivalencia y que su conjunto cociente coincide con P.

Nota. A cada elemento y de un clase $[x]$ se le llama *representante de la clase*. El hecho de que si $y \in [x]$ entonces $[y] = [x]$ sugiere que todos los representantes de la clase son "igualmente buenos" a la hora de denotar esa clase.

1.1.3. Aplicaciones entre conjuntos

Concepto

Sean X, Y dos conjuntos. Una *aplicación* f de X a Y es una regla que asigna a cada elemento de X un único elemento de Y. La aplicación se representa $f : X \to Y$, y escribiremos $x \mapsto y$ o bien $f(x) = y$ si y es el único elemento de Y que se asigna a x mediante f. Al conjunto X se le llama *dominio* (o conjunto inicial) de la aplicación, a Y el *codominio* (o conjunto final) y a $f(x)$ *imagen por* f *de* x. La *imagen* de la aplicación f, $\mathrm{Im} f$, es el subconjunto del codominio que contiene las imágenes de todos los elementos de X, esto es:

$$\mathrm{Im} f := \{f(x) : x \in X\} = \{y \in Y \,|\, \exists x \in X : y = f(x)\} \subset Y.$$

El *grafo* o *gráfico* de la aplicación f se define como el siguiente subconjunto del producto cartesiano $X \times Y$:

$$G(f) := \{(x, f(x)) | x \in X\} = \{(x,y) \in X \times Y | y = f(x)\}$$

Observación. Una aplicación queda caracterizada totalmente por su dominio, codominio y grafo (esto es, si estos tres objetos son iguales para dos aplicaciones f, $\bar{f}$ entonces $f = \bar{f}$).

No obstante, dos aplicaciones pueden ser distintas incluso si sus dominios y grafos coinciden. De hecho, son diferentes las aplicaciones $f_1 : \mathbb{N} \to \mathbb{N}$, $x \mapsto x^2$, y $f_2 : \mathbb{N} \to \mathbb{R}$, $x \mapsto x^2$. También es distinta la aplicación $f_3 : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$, a pesar de que tanto su codominio como su regla para asignar imágenes coincidan con los de f_2.

Proposición 1.4. *(i) El grafo $G(f)$ satisface:*
(a) $\forall x \in X$, $\exists y \in Y : (x,y) \in G(f)$.
(b) $(x,y), (x,y') \in G(f) \Rightarrow y = y'$.
Recíprocamente, si C es un subconjunto de $X \times Y$ que verifica las propiedades (a) y (b) del grafo entonces existe una única aplicación $f : X \to Y$ tal que $C = G(f)$.

Demostración. (a) Dado x, su imagen $f(x)$ es el elemento $y \in Y$ buscado.

(b) Por la definición del grafo, $y = f(x)$ y también $y' = f(x)$. Como por la definición de aplicación la imagen de x es única, se sigue $y = y'$. Para la última afirmación, obsérvese primero que C satisface la siguiente propiedad, que equivale a (a) y (b):

$$\forall x \in X,\ \exists! y \in Y :\ (x,y) \in C. \tag{1.1}$$

Por tanto, basta con definir $f : X \to Y$ como la aplicación que asigna a cada $x \in X$ el único $y \in Y$ determinado por la propiedad (1.1). Esta propiedad asegura directamente tanto que f es una aplicación como que C es su grafo. La unicidad de f se debe a que cualquier otra aplicación $\bar{f} : X \to Y$ tal que $G(\bar{f}) = C$ tendría el mismo dominio, codominio y grafo que f, por lo que sería igual a f. □ [8]

Generación de aplicaciones a partir de otras

Dada una aplicación $f : X \to Y$ y un subconjunto A de su dominio ($A \subset X$), se define la *restricción de f a A*, denotada $f|_A$, por:

$$f|_A : A \to Y, \qquad x \mapsto f(x),$$

esto es, la regla que asigna a cada elemento x su imagen es la misma que la de f, pero $f|_A$ la aplica sólo a los elementos de A. [9]

La aplicación $f : X \to Y$ también permite definir aplicaciones entre los correspondientes conjuntos de las partes. Concretamente, la aplicación *imagen directa*,

$$f_* : \mathcal{P}(X) \to \mathcal{P}(Y). \qquad A \mapsto f_*(A) := \{f(x) : x \in A\}$$

[8] *Nota.* La proposición 1.4 permite eliminar la ligera imprecisión que se cometió al definir el concepto de aplicación usando la expresión "una regla que asigna". En efecto, se puede definir de manera totalmente formal una aplicación como una terna (X,Y,C) en la que X,Y son conjuntos y C es un subconjunto de $X \times Y$ que satisface (1.1).

Si se adoptara esta definición de aplicación, la proposición 1.4 dejaría de tener sentido (esencialmente, estaría incluida en la definición). No obstante, la demostración de su última parte serviría como motivación para recuperar la idea intuitiva de que, gracias a las propiedades de C, la aplicación f "asigna" a cada elemento de X uno de Y.

[9] Análogamente, si se considera cualquier $B \subset Y$ que incluya $\mathrm{Im} f$, se puede obtener una aplicación $f|^B$ restringiendo el codominio, esto es, $f|^B : X \to B$, $x \mapsto f(x)$.

y la imagen recíproca,

$$f^* : \mathcal{P}(Y) \to \mathcal{P}(X). \qquad B \mapsto f^*(B) := \{x \in X : f(x) \in B\}.$$

Nota. En ocasiones se abusa de la notación escribiendo $f(A)$ en lugar de $f_*(A)$, y $f^{-1}(B)$ en lugar de $f^*(B)$. Esto no es formalmente correcto, por lo que no debe de hacerse (al menos mientras no se tenga la suficiente práctica para entender inequívocamente cuándo se está abusando de la notación).

Observación. De la definición se sigue:
(a) $f_*(A) \subset Y$, por lo que $f_*(A) \in \mathcal{P}(Y)$,
(b) $f^*(B) \subset X$, por lo que $f^*(B) \in \mathcal{P}(X)$,
(c) $f_*(X) = \text{Im} f$, $f^*(Y) = X$,
(d) cuando $B \subset Y$ verifica $B \cap \text{Im } f = \emptyset$ entonces $f^*(B) = \emptyset$ (el cual es un subconjunto de X y, de hecho, de cualquier otro conjunto).

Definición 1.5. *Se consideran las aplicaciones $f : X \to Y, g : Y \to Z$, en la que el codominio de f coincide con el dominio de g. Se define su* composición $g \circ f$ *por:*

$$g \circ f : X \to Z, \qquad x \mapsto (g \circ f)(x) := g(f(x)),$$

esto es, cada $(g \circ f)(x)$ se obtiene aplicando a x primero f (que por este motivo aparece notacionalmente a la derecha en $g \circ f$) y luego aplicando g a la imagen $f(x)$.

Ejercicio. (i) Sean $f, g : \mathbb{R} \to \mathbb{R}$ definidas por:

$$f(x) = x^2 + 1, \qquad g(x) = e^x, \qquad \forall x \in \mathbb{R}.$$

Calcular $g \circ f$ y $f \circ g$.

(ii) Sean $f : X \to Y$ y $g : X' \to Y'$ dos aplicaciones entre conjuntos. Supongamos que se puede definir $g \circ f$, ¿bajo qué condiciones se puede definir también $f \circ g$?

(iii) Compruébese que la definición de composición se puede extender naturalmente al caso de funciones $f : X \to Y, g : Y' \to Z$ tales que Im $f \subset Y'$.

Proposición 1.6. *Se consideran las aplicaciones $f : X \to Y, g : Y \to Z, h : Z \to W$. Entonces*

$$(h \circ g) \circ f = h \circ (g \circ f). \tag{1.2}$$

Demostración. Claramente, ambos miembros de la igualdad están bien definidos como aplicaciones y tienen igual dominio y codominio. La regla de asignación de imágenes también coincide pues:

$$[(h \circ g) \circ f] = (h \circ g)(f(x)) = h(g(f(x))), \quad [h \circ (g \circ f)](x) = h((g \circ f)(x)) = h(g(f(x))), \qquad \forall x \in X \,\square$$

Nota. La proposicion 1.6 se puede enunciar diciendo que la composición es *asociativa*. La proposicion también justifica que la notación $h \circ g \circ f$ es inequívoca, pues se puede usar para indicar cualquiera de las dos expresiones (1.2).

Tipos notables de aplicaciones y descomposición canónica

Definición 1.7. *Sea $f : X \to Y$ una aplicación. Se dice que f es:*

- Inyectiva*: si elementos distintos de X tienen imágenes distintas en Y, esto es, para todo $x, x' \in X$ tales que $x \neq x'$ se tiene $f(x) \neq f(x')$ (equivalentemente, cuando $f(x) = f(x') \Rightarrow x = x'$).*
- Suprayectiva, sobreyectiva, sobre *o* exhaustiva*: si todo elemento de Y es imagen de alguno de X, esto es, $\forall y \in Y$, $\exists x \in X : f(x) = y$ (equivalentemente, si* Im f=Y*).*
- Biyectiva*: si f es inyectiva y suprayectiva, esto es, $\forall y \in Y$, $\exists! x \in X$: $y = f(x)$.*

  En este caso, se define la aplicación inversa *de f, que denotaremos f^{-1}, estableciendo que $f^{-1}(y)$ es el único $x \in X$ tal que $f(x) = y$.*

Ejemplos generales de estos tipos de aplicaciones son:

- La inclusión i de un subconjunto: dado $A \subset X$, $i : A \to X$, $x \mapsto x$. La inclusión i es inyectiva.
- La proyección canónica π sobre un conjunto cociente: dado $(X, \sim)$,

$$\pi : X \to X/\sim, \qquad x \mapsto \pi(x) := [x].$$

  La proyección π es suprayectiva.

- La aplicación identidad I_X: dado un conjunto X, $I_X : X \to X, x \mapsto x$ (caso particular e la inclusión cuando $A = X$). La identidad I_X es biyectiva.

Ejercicio. Tómese como $f : D \to \mathbb{R}$ cada una de las siguientes cuatro funciones elementales: $x \mapsto x^2, e^x, \sqrt{x}$, $\ln(x)$, siendo en cada caso $D \subset \mathbb{R}$ su dominio natural. Determínese cuáles de ellas son inyectivas, suprayectivas o biyectivas. ¿Es alguna de estas aplicaciones la inversa de otra?

Proposición 1.8. *La composición de dos aplicaciones inyectivas (respectivamente, suprayectivas, biyectivas es inyectiva (respectivamente, suprayectiva, biyectiva).*

Demostración. Hágase como ejercicio. □

Podemos caracterizar la aplicación inversa como sigue.

Lema 1.9. *Sean $f : X \to Y$, $g : Y \to Z$.*

- *Si $g \circ f$ es inyectiva entonces f es inyectiva.*
- *Si $g \circ f$ es suprayectiva entonces g es suprayectiva.*

Por tanto, si $g \circ f$ es biyectiva entonces f es inyectiva y g es suprayectiva.

Demostración. Para la primera afirmación, si f no fuera inyectiva existirían $x, x' \in X$, $x \neq x'$ tales que $f(x) = f(x')$. En consecuencia, $(g \circ f)(x) = g(f(x)) = g(f(x')) = (g \circ f)(x')$, y $g \circ f$ no es inyectiva.

Para la segunda, sea $z \in Z$. Como g es suprayectiva, existe $x \in X$ tal que $z = (g \circ f)(x) = g(f(x))$. Por tanto, z es la imagen por g de $f(x) \in Y$. □

Proposición 1.10. *Sean $f : X \to Y$, $g : Y \to X$ dos aplicaciones tales que*

$$g \circ f = I_X, \qquad f \circ g = I_Y.$$

Entonces f, g son biyectivas y $g = f^{-1}$.

Demostración. Aplicando el lema anterior a la primera igualdad se obtiene la inyectivdad de f y la suprayectividad de g y, aplicándolo a la segunda, la inyectivdad de g y la suprayectividad de f, de donde se sigue la biyectividad de ambas.

Claramente, g y f^{-1} tienen igual dominio y codominio. Sea $y \in Y$ y $x = f^{-1}(y)$, esto es, $f(x) = y$. Se tiene entonces $g(y) = g(f(x)) = (g \circ f)(x) = I_X(x) = x = f^{-1}(y)$, por lo que g y f^{-1} coinciden. □

Una aplicación arbitraria no tiene por qué ser inyectiva o suprayectiva. No obstante, toda aplicación se puede escribir como composición de una aplicación inyectiva, una biyectiva y una suprayectiva, del modo canónico que se describe a continuación.

Teorema 1.11 (Descomposición canónica de una aplicación)**.** *Sea $f : X \to Y$ una aplicación. Se define la relación de equivalencia en X: $x \sim x' \Leftrightarrow f(x) = f(x')$, y se considera su proyección canónica $\pi : X \to X/\sim$, que es sobre. Asimismo, se considera* Im f *y su inclusión i :* Im $f \to Y$*, que es inyectiva.*

Se tiene entonces que la aplicación

$$b : (X/\sim) \longrightarrow \mathrm{Im} f, \qquad b([x]) := f(x)$$

está bien definida, es biyectiva y verifica:

$$f = i \circ b \circ \pi.$$

Demostración. En primer lugar, obsérvese que, efectivamente, la relación binaria $\sim$ es (trivialmente) una relación de equivalencia.

Mostrar que b está correctamente definida como aplicación requiere una cierta discusión. Al definirse la imagen por b de toda la clase $[x]$ como la imagen por f del representante x (éste es el significado de $b([x]) := f(x)$), uno podría preguntarse qué ocurriría si tomáramos un representante distinto x' para esa clase. Esto es, si $x' \sim x$ entonces $[x'] = [x]$ y también se tendría $b([x]) = b([x']) = f(x')$. No obstante, el hecho de que $x \sim x'$ significa precisamente $f(x') = f(x)$ (por la definición de la relación de equivalencia), la imagen que de $[x]$ se obtiene por b es independiente del representante escogido, esto es, b está bien definida como aplicación.

La inyectividad de b se sigue entonces porque si $b([x]) = b([y])$ entonces $f(x) = f(y)$ y, por tanto, $x \sim y$, esto es, $[x] = [y]$.

Para la suprayectividad de b, si $z \in$ Im f entonces existe un $x \in X$ tal que $z = f(x)$. Por tanto $b([x]) = z$, esto es, $z \in$ Im b.

Finalmente, es inmediato que f y $i \circ b \circ \pi$ tienen igual dominio y codominio. Por tanto, su igualdad se deduce de

$$i \circ b \circ \pi(x) = i(b(\pi(x))) = i(b([x]) = i(f(x)) = f(x), \qquad \forall x \in X. \qquad \square$$

Como un último comentario, obsérvese que f es inyectiva si y sólo si π lo es, y que f es suprayectiva si y sólo si i lo es.

1.2. Grupos y cuerpos

Abstrayendo las operaciones y propiedades conocidas en el conjunto $\mathbb{R}$ de los números reales, introducimos en esta sección el concepto de cuerpo y las estructuras algebraicas previas (grupos, anillos) necesarias para su comprensión.

Nuestro objetivo aquí sólo es proporcionar el concepto de cuerpo para poder definir en general el de espacio vectorial, así como el de grupo, por ser una estructura geométrica básica. En otras asignaturas del grado se desarrollarán con detalle todas las estructuras que veremos aquí. Así, aunque el lector tenga ahora en mente sólo la intuición de un cuerpo como $\mathbb{R}$, podrá entender con facilidad que las propiedades de los espacios vectoriales construidos sobre $\mathbb{R}$ se extienden con generalidad a espacios vectoriales sobre cualquier cuerpo.

1.2.1. Grupos

Sea G un conjunto. Una *operación* o *ley de composición interna* es cualquier aplicación del tipo $\cdot : G \times G \to G$. Usaremos la notación[10]:

$$\begin{array}{rcl} \cdot : G \times G & \to & G \\ (x,y) & \mapsto & x \cdot y \end{array}$$

Obsérvese que las operaciones usuales $+$, $\cdot$ en $\mathbb{R}$ (esto es, la suma $+$ y el producto usual $\cdot$), verifican nuestra definición y convenios.

Algunas posibles propiedades que puede tener la operación $\cdot$ son:

1. *Asociativa*: $x \cdot (y \cdot z) = (x \cdot y) \cdot z$, $\forall x, y, z \in G$.
2. *Elemento neutro*: $\exists e \in G$ (al que llamaremos *elemento neutro*) tal que $e \cdot x = x \cdot e = x$, $\forall x \in G$.
3. *Elemento simétrico* (supuesta la existencia de un elemento neutro $e \in G$):

   $\forall x \in G$, $\exists \bar{x} \in G$ (al que llamaremos *elemento simétrico* de x) tal que $x \cdot \bar{x} = \bar{x} \cdot x = e$.
4. *Conmutativa*: $x \cdot y = y \cdot x$, $\forall x, y \in G$.

Un grupo es el par $(G, \cdot)$ formado por un conjunto G y una operación $\cdot$ en G que verifica las tres primeras propiedades anteriores. Si además verifica la cuarta, el grupo se dirá *conmutativo* o *abeliano*.

Proposición 1.1. *En todo grupo $(G, \cdot)$:*

(a) El elemento neutro e es único,

(b) Se puede "simplificar", esto es, $x \cdot y = x \cdot y' \Rightarrow y = y'$ y también $x \cdot y = x' \cdot y \Rightarrow x = x'$, y

(c) El recíproco $\bar{x}$ de cada elemento x es único. Más aún, si dos elementos x, y del grupo verifican $x \cdot y = e$ entoces x es el recíproco de y (e y es el recíproco de x).

Demostración. (a) Si e' fuera otro elemento neutro: $e' = e' \cdot e = e$, la primera igualdad usando que e es neutro, y la segunda que e' lo es.

(b) Para demostrar la primera implicación, operando ambos miembros por el simétrico $\bar{x}$ de x por la izquierda, se tiene:

$$\bar{x} \cdot (x \cdot y) = \bar{x} \cdot (x \cdot y')$$

[10] Obsérvese el convenio de denotar $x \cdot y$ a la imagen $\cdot((x,y))$. Se pueden usar otros símbolos (p.ej., $\star$), para denotar operaciones con el mismo convenio.

por la propiedad asociativa:

$$(\bar{x}\cdot x)\cdot y = (\bar{x}\cdot x)\cdot y'$$

por la elemento simétrico:

$$e\cdot y = e\cdot y'$$

y por la elemento neutro $y = y'$, como se quería demostrar. La otra implicación se demuestra análogamente, operando ambos miembros por el simétrico $\bar{y}$ de y por la derecha.

(c) Consecuencia sencilla de (a) y (b). □

Suele denotarse al (único) elemento recíproco de x como x^{-1}, y llamársele también *elemento inverso*; en algunos grupos particulares se le da un nombre distinto. Algunos ejemplos de grupos son:

- $(\mathbb{R},+)$. Claramente, el neutro es $e=0$, y el elemento simétrico de x es $-x$, al cual se le llama elemento *opuesto* de x.
- $\mathbb{R}\setminus\{0\}$, con la restricción natural del producto usual de $\mathbb{R}$ (obviamente, $e=1$).
- Dado un conjunto X consideremos el conjunto Biy (X) formado por todas las aplicaciones biyectivas de X en X. Claramente, la composición $\circ$ es una operación en Biy (X), y se verifica que el par $(\text{Biy }(X),\circ)$ es un grupo cuyo neutro es la aplicación identidad.

Cuestión: ¿Cuáles de los grupos anteriores son conmutativos?

1.2.2. Anillos y cuerpos

Consideremos ahora un conjunto A dotado de dos operaciones, que denotaremos $+$, . ; esto es, una terna $(A,+,.)$. Diremos que $(A,+,.)$ es un *anillo* si verifica las siguientes propiedades:

1. $(A,+)$ es un grupo conmutativo.

   (*Convenio*: si no se especifica lo contrario, al elemento neutro se le denotará 0 y a la operación $+$ se le llamará *suma* en A.)

2. $(A,.)$ verifica la propiedad asociativa.

   (*Convenio:* si no se especifica lo contrario, a la operación . se le llamará *producto* en A.)

3. $(A,+,.)$ verifica la *propiedad distributiva de la suma respecto al producto*, esto es[11]:

$$\begin{array}{rcll} x.(y+z) & = & x.y+x.z & \text{(distributiva por la izquierda) y}\\ (y+z).x & = & y.x+z.x & \text{(distributiva por la derecha),}\end{array}$$

   para todo $x,y,z\in A$.

Es fácil comprobar que en todo anillo se verifica $0\,.\,x = x\,.\,0 = 0$ (obsérvese que $0.x = (0+0).x = 0.x + 0.x$ y simplifíquese por el simétrico de $0.x$). Casos particulares de anillos son:

- Anillo unitario: anillo cuyo producto tiene elemento neutro, esto es, $\exists 1\in A : x\,.\,1 = 1\,.\,x = x$, para todo $x\in A$.

  Al elemento neutro para el producto se le llamará *elemento unidad* (y se le denotará 1).

[11] *Convenio*: extenderemos la notación sobre prelación de operaciones usual en $\mathbb{R}$, de modo que $(x.y)+(x.z)$ se denotará simplemente $x.y+x.z$.

- *Anillo unitario no trivial*: anillo unitario en el que $1 \neq 0$.

  Nota: si un anillo unitario no verifica esta propiedad, es decir, $1 = 0$ (es un anillo trivial), se tiene que $A = \{0\}$ (pues $x = 1.x = 0.x = 0$ para todo $x \in A$).

- *Anillo conmutativo*: anillo en el que el producto es conmutativo[12], esto es, $x.y = y.x, \forall x, y \in A$.

Es sencillo comprobar que en un anillo unitario $(-1)\cdot x = -x$ (pues sumados a $1\cdot x$ dan el neutro para la operación $+$) así como $(-1)(-x) = x$ (pues se puede aplicar la propiedad anterior a $-x$ y se sabe que para la operación de grupo $+$ se sabe $-(-x) = x$).

Con estos conceptos previos podemos ya definir el de cuerpo, que usaremos continuadamente.

Definición 1.2. *Un* cuerpo $(K,+,.)$ *es un anillo unitario no trivial en el que el producto verifica la propiedad elemento simétrico.*

El cuerpo $(K,+,.)$ *se dirá* conmutativo *si el producto . verifica la propiedad conmutativa.*

Es fácil comprobar que $(K,+,.)$ es un *cuerpo conmutativo si y sólo si*:

1. $(K,+)$ es un grupo conmutativo
2. $K \setminus \{0\}$ es un grupo con la restricción natural de la operación producto definida en todo[13] K.
3. Se verifica la propiedad distributiva de la suma respecto al producto.

Algunos ejemplos de anillos y cuerpos son los siguientes:

- $(\mathbb{Z},+,.)$ es un anillo unitario (no trivial), pero no un cuerpo. Estas mismas propiedades las tiene el conjunto de matrices reales cuadradas de un orden fijo $n \times n$, con la suma y producto usuales de matrices.

- Sea $p \in \mathbb{N}$ un número natural. El conjunto $p\mathbb{Z}$ de los múltiplos de p, con su suma y producto naturales (restricción de los de $\mathbb{Z}$) forma un anillo. Si $p \neq 1$ este anillo no es unitario[14].

- El conjunto $\mathbb{Z}/p\mathbb{Z}$ de los enteros módulo $p\mathbb{Z}$ (esto es, el conjunto cociente, que denotaremos $\mathbb{Z}/p\mathbb{Z}$, para la relación de equivalencia en $\mathbb{Z}$ "dos enteros están relacionados si y sólo si su resto al dividir por p es el mismo", el cual está formado por p clases de equivalencia), tiene una estructura natural de anillo unitario conmutativo (con operaciones en el cociente inducidas por las de $\mathbb{Z}$). Para p primo este anillo es un cuerpo. En el caso $p = 2$, este cuerpo $K = \mathbb{Z}/2\mathbb{Z}$ tendría dos elementos $K = \{[0],[1]\}$ y las operaciones se definirían por:

$$\begin{array}{llll} [0]+[0]=[0], & [0]+[1]=[1], & [1]+[0]=[1], & [1]+[1]=[0] \\ [0].[0]=[0], & [0].[1]=[0], & [1].[0]=[0], & [1].[1]=[1] \end{array}$$

  Puede comprobarse directamente como ejercicio que $K = \{[0],[1]\}$ con las operaciones anteriores es un cuerpo conmutativo[15].

[12] Recuérdese que la operación suma $+$ era siempre conmutativa en un anillo.

[13] En particular, esta propiedad impedirá que $(K,+,.)$ pueda ser un anillo unitario trivial.

[14] Como convenio, supondremos que los naturales no incluyen el 0. (Obsérvese que en el ejemplo que estamos considerando arriba, si se tomara $p = 0$ se obtendría un anillo unitario trivial.)

[15] En este cuerpo, al operar el elemento unidad consigo misma se obtiene 0. En genereal, se dice que la *característica* de un cuerpo K es $p \in \mathbb{N}$ si p es el menor natural tal que al operar p veces la unidad consigo misma se obtiene 0, esto es, $1 + \cdots +^{(p)} 1 = 0$; en caso de que esto no ocurra para ningún natural, se dice que la característica de K es 0. Para p primo, los cuerpos $\mathbb{Z}/p\mathbb{Z}$ tienen carcterística p, mientras que los cuerpos con los que trabajaremos usualmente $(\mathbb{Q},\mathbb{R},\mathbb{C})$ tienen característica 0.

- $(\mathbb{Q},+,.),(\mathbb{R},+,.)$ son cuerpos conmutativos.

En adelante, trabajaremos siempre con **cuerpos conmutativos**, denotados simplemente por K, salvo mención explícita de lo contrario.

1.2.3. El cuerpo $\mathbb{C}$ de los números complejos

Por su gran importancia en Matemáticas (incluso a un nivel muy elemental) definiremos aquí el cuerpo $\mathbb{C}$ de los números complejos, el cual se estudirará con detalle en otras asignaturas del grado.

Al igual que los números reales se definen como una extensión de los racionales la cual, permite, por ejemplo, considerar como un número (real) a la raíz de 2 (esto es, que la ecuación $x^2 = a$ siempre admita alguna solución cuando $a \geq 0$), los complejos se definen a partir de los reales para dotar de sentido a la raíz de números negativos (esto es, que la ecuación $x^2 = a$ siempre admita alguna solución incluso cuando $a < 0$). Para ello, se introduce la llamada *unidad imaginaria i*, que desempeña el papel de ser una solución de $\sqrt{-1}$, y se extienden las operaciones $+,.$ de $\mathbb{R}$ de manera natural a cualquier combinación de números reales y la unidad imaginaria, teniendo siempre en cuenta que $i^2 = -1$.

Formalmente, se define el cuerpo $\mathbb{C}$ de los números complejos como $(\mathbb{R}^2,+,.)$ donde para cada número complejo $z = (x,y) \in \mathbb{R}^2$ a x (resp. y) se le llama la *parte real* (resp. *parte imaginaria*) de z, y las operaciones se definen por:

$$\begin{array}{rcl}(x,y)+(x',y') & := & (x+x',y+y')\\ (x,y).(x',y') & := & (x.x'-y.y',x.y'+y.x')\end{array}$$

para todo $(x,y),(x',y') \in \mathbb{R}^2$ (en estas definiciones, los símbolos $+$, . a la izquierda de las igualdades denotan, respectivamente, la suma y producto de complejos que se está definiendo sobre $\mathbb{R}^2$, mientras que a la derecha representan la suma y producto usuales en $\mathbb{R}$). Se define la *unidad imaginaria* como

$$i := (0,1).$$

Usando i, simplificamos la notación escribiendo x en lugar de $(x,0)$ de modo que $(0,y) = y.i$ (que también se denotará indistintamente como $y\ i$, así como por $i\ y$). Así, podemos escribir cada número complejo (x,y) como

$$(x,y) \equiv x+iy,$$

de modo que las definiciones anteriores se reescriben:

$$\begin{array}{rcl}(x+iy)+(x'+iy') & = & (x+x')+i(y+y')\\ (x+iy).(x'+iy') & = & (x.x'-y.y')+i(x.y'+y.x').\end{array}$$

Intuitivamente, el papel de multiplicar por i un complejo z equivale a rotar z en el plano $\mathbb{R}^2$ $\pi/2$ radianes (90 grados sexagesimales), usando el sentido positivo de giro (opuesto al del movimiento de las agujas del reloj). Dado un complejo $z = x+iy$ se define su *conjugado*

$$\bar{z} = x-iy$$

(que es el simétrico de z con respecto al eje de abscisas) y su módulo (o valor absoluto) como

$$|z| = \sqrt{x^2+y^2}\ (= \sqrt{z.\bar{z}}).$$

No es difícil demostrar que todo complejo $z = x+iy$ admite una *representación polar*, del tipo

$$z = r(\cos\theta + i\,\mathrm{sen}\,\theta), \tag{1.3}$$

donde r no es más que el módulo de z y θ su *argumento*[16] (este último, cuando $x > 0$, puede calcularse como $\theta = \arctan(y/x)$, y resulta sencilla dar fórmulas para los casos $x \leq 0$). Dado un segundo número complejo dado en forma polar $z' = r'(\cos\theta' + i\,\mathrm{sen}\,\theta')$ se verifica de las propiedades del producto y suma:

$$z.z' = rr'\left((\cos\theta\cos\theta' - \mathrm{sen}\,\theta\,\mathrm{sen}\,\theta') + i(\mathrm{sen}\,\theta\cos\theta' + \cos\theta\,\mathrm{sen}\,\theta')\right) = rr'\left(\cos(\theta+\theta') + i\,\mathrm{sen}(\theta+\theta')\right)$$

(la última igualdad usando las fórmulas conocidas del seno y coseno de una suma). Esto es, el producto de dos números complejos es otro complejo cuyo módulo es el producto de los módulos, y su argumento puede escogerse como la suma de los argumentos.

Usando las propiedades anteriores no es difícil comprobar:

$\mathbb{C}$ *es un cuerpo conmutativo.*

De hecho, la suma y producto definidos en $\mathbb{C}$ heredan de manera natural las propiedades de cuerpo que verifican la suma y el producto en $\mathbb{R}$.

Nota 1 *(Expresión exponencial).* Definiendo,

$$e^{i\theta} := \cos\theta + i\,\mathrm{sen}\,\theta$$

(lo que se justifica cuando se estudia el desarrollo en serie de potencias de la exponencial, $e^w = \sum_{n=0}^{\infty} w^n/n!$, y se compara con el de las funciones seno y coseno), la representación polar se reescribe

$$z = r.e^{i\theta}.$$

Dado un segundo complejo $z' = r'.e^{i\theta'}$ se tiene entonces $z.z' = (r.r').e^{i(\theta+\theta')}$, consistentemente con fórmulas anteriores.

Nota 2 *(Cuaterniones).* De un modo similar a como se construyen los números complejos a partir de los reales, se define el cuerpo de los números *cuaterniones* (o *cuaternios*). En este caso, el conjunto es $\mathbb{R}^4$, donde se definen

$$i := (0,1,0,0),\ j := (0,0,1,0),\ k := (0,0,0,1)$$

de modo que podemos reescribir cada $(x,y,z,t) \in \mathbb{R}^4$ como:

$$(x,y,z,t) = x + iy + jz + kt.$$

Se define la suma usual, componente a componente, mientras que para el producto se opera de manera natural imponiendo las relaciones:

$$i^2 = j^2 = k^2 = i.j.k = -1.$$

(usando la notación $i^2 = i.i$, etc.) De estas relaciones no es difícil demostrar $i.j = k$; $j.i = -k$; $i.k = -j$; $k.i = j$; $j.k = i$; $k.j = -i$. Las operaciones resultantes $+$, . dotan a $\mathbb{R}^4$ de una estructura de cuerpo, el cual *no es conmutativo*, y a $\mathbb{H} := (\mathbb{R}^4, +, .)$ se le llama *cuerpo de los cuaterniones*.[17]

[16] Obsérvese que cuando $z \neq 0$, el argumento está definido unívocamente salvo la suma de un número entero de veces 2π.

[17] Este cuerpo también se puede construir a partir de $\mathbb{C}$ de un modo análogo a como construimos $\mathbb{C}$ a partir de $\mathbb{R}$ (esto es, como "complejos de los números complejos"). Para ello denotamos $z + jw$ al par de complejos (z,w), consideramos la suma componente a componente, e introducimos el siguiente producto (extendiendo al de $\mathbb{C}$): $(z_1 + jw_1).(z_2 + jw_2) := (z_1.z_2 - \bar{w}_1.w_2) + j(\bar{z}_1 w_2 + w_1.z_2)$. Denotando por k a $i.j$, esto es, $k := (i + j0).(0 + j1) = j(-i)$, se reobtiene $\mathbb{H}$.