Geometría I: Tema 0

Juan de Dios Pérez

1. Conjuntos. Operaciones entre conjuntos.

Un conjunto es una colección o reunión de objetos que llamaremos elementos del conjunto. Utilizaremos letras mayúsculas, A, B, ..., para designar conjuntos y letras minúsculas, x, y, ..., para designar los elementos de un conjunto.
Si x es un elemento del conjunto A, diremos que x "pertenece" a A y lo escribiremos $x \in A$.
Si y no es un elemento del conjunto A, diremos que y "no pertenece" a A y lo escribiremos $y \notin A$.
Conoceremos un conjunto si conocemos todos y cada uno de sus elementos.
Aunque parezca una contradicción, por motivos de utilidad, definiremos como "vacío" al conjunto que no tiene ningún elemento y lo notaremos como $\emptyset$.
Hay dos formas de definir (ó conocer) un conjunto:

1. Por extensión, dando todos y cada uno de sus elementos. Por ejemplo, $A = \{1, 5, 7, 9, 14\}$ denota el conjunto cuyos cinco elementos son los que aparecen entre llaves y no tiene más elementos. Otro ejemplo sería $B = \{\text{Almería}, \text{Cádiz}, \text{Granada}, \text{Huelva}, \text{Jaén}, \text{Málaga}, \text{Sevilla}\}$.

2. Por comprensión, dando una regla o propiedad que verificarán los elementos del conjunto y solo ellos. Así, el conjunto B anterior sería posible definirlo como el conjunto de las provincias de Andalucía. Hay casos, como cuando el conjunto tiene un número no finito de elementos, en que solo podemos definirlo de esta forma. Esto ocurre con los conjuntos numéricos de los números naturales $\mathbb{N}$, los enteros $\mathbb{Z}$, los racionales $\mathbb{Q}$ ó los reales $\mathbb{R}$.

Dados dos conjuntos A y B, diremos que A es un subconjunto de B si cada elemento de A es un elemento de B. Esto lo escribiremos de esta forma: $x \in A \Rightarrow x \in B$, y leeremos "si $x \in A$ entonces $x \in B$". Si A es un subconjunto de B lo representaremos como "$A \subset B$" y leeremos "A es un subconjunto de B" ó "A está contenido en B".
Dado un conjunto arbitrario B, al menos tiene siempre dos subconjuntos: él mismo y el vacío, ya que por convención, como no tiene ningún elemento, todos los elementos del conjunto vacío $\emptyset$ son elementos de B. Por tanto, siempre B y $\emptyset$ con subconjuntos de B. Estos subconjuntos de B se llaman impropios. Cualquier otro subconjunto de B se llamará propio.
Como dos conjuntos A y B serán iguales cuando tengan, exactamente, los mismos elementos, ocurrirá que cada elemento de A será un elemento de B, es decir, $A \subset B$ ó $x \in A \Rightarrow x \in B$ y, a la vez, cada elemento de B será un elemento de A; por tanto, $B \subset A$ ó $x \in B \Rightarrow x \in A$. Tenemos, pues, que si $A = B$,

$x \in A \Rightarrow x \in B$ y $x \in B \Rightarrow x \in A$. Esta doble condición la escribiremos $x \in A \Leftrightarrow x \in B$y la leeremos "$x$ pertenece a A si y solo si x pertenece a B".

Ejemplos:

Empezaremos introduciendo los cuantificadores:

1. $\forall$ (cuantificador universal): se lee "para todo" e indica que cualquier elemento de un conjunto afectado por $\forall$ verificará la condición que aparezca a continuación. Así, si $[0, 2\pi] = \{x \in \mathbb{R} / \ 0 \leq x \leq 2\pi\}$, donde el símbolo "/" lo leeremos como "tal que" ó "que verifica", podremos escribir $\forall x \in [0, 2\pi]$, $-1 \leq \cos(x) \ \leq 1$.

2. $\exists$ (cuantificador existencial): se lee "existe algún" e indica que, al menos, podremos encontrar un elemento en el conjunto que estemos considerando que verificará la condición que aparezca a continuación. Así, escribiremos $\exists x \in [0, 2\pi] \,/\, \cos(x) = \frac{\sqrt{2}}{2}$, pues sabemos que $x = \frac{\pi}{4}$ lo satisface, aunque también lo verifica $x = -\frac{\pi}{4}$.

3. $\exists_1$ (cuantificador existencial de unicidad)[1]: se lee "existe un único" e indica que en el conjunto que estemos considerando hay un elemento y solo ese que verifica la propiedad que aparezca a continuación. Por ejemplo, $\exists_1 x \ \in \left[0, \frac{\pi}{2}\right]$ tal que $\cos(x) = \frac{\sqrt{2}}{2}$, puesto que solamente $x = \frac{\pi}{4}$ verifica esa condición.

Consideremos el conjunto de los números enteros pares, $2\mathbb{Z} = \{2m \,/\, m \in \mathbb{Z}\}$. Entonces el conjunto de los números enteros múltiplos de 4, $4\mathbb{Z} = \{4n \,/\, n \in \mathbb{Z}\}$ es un subconjunto de $2\mathbb{Z}$, pues $4n = 2 \cdot (2n)$ y, si $n \in \mathbb{Z}$, $2n$ también. Luego $4\mathbb{Z} \subset 2\mathbb{Z}$. Sin embargo, $2\mathbb{Z}$ no es un subconjunto de $4\mathbb{Z}$, pues $2 \in 2\mathbb{Z}$, pero $2 \notin 4\mathbb{Z}$, ya que no podemos encontrar ningún entero n tal que $2 = 4n$. Luego, $4\mathbb{Z} \not\subseteq 2\mathbb{Z}$, indicando $\not\subseteq$ que como $4\mathbb{Z}$ no es vacío y no coincide con $2\mathbb{Z}$, entonces es un subconjunto propio de $2\mathbb{Z}$.
Por otro lado, $A = \{1, 2, 4, 6, 8, 10\}$ no es un subconjunto de $2\mathbb{Z}$, ya que $1 \in A$, pero $1 \notin 2\mathbb{Z}$.
Supongamos que A y B son dos conjuntos.

- Definimos la unión de A y B, y la notaremos como $A \cup B$, como el conjunto de elementos que ó bien son de A ó son de B. Es decir, $A \cup B = \{x \,/\, x \in A \text{ ó } x \in B\}$. Como si $x \in A$, entonces $x \in A \cup B$, tenemos que $A \subset A \cup B$ y si $y \in B$, entonces $y \in A \cup B$, luego $B \subset A \cup B$. Es decir, A y B son ambos subconjuntos de $A \cup B$. Asimismo, si $A \subset B$, $A \cup B = B$. También $A \cup \emptyset = A$.
  Esta definición, que hemos dado para dos conjuntos, la podemos extender a una familia arbitraria de conjuntos. SI I es un conjunto de índices arbitrario (pensad en cualquier conjunto finito como $I = \{1, 2, 3, 4, 5, 6, 7, 8\}$ ó $\mathbb{N}$ ó un conjunto cualquiera) y para cada elemento $i \in I$ disponemos de un conjunto A_i, definimos la unión de tales A_i como

$$\bigcup_{i \in I} A_i = \{x \,/\, \exists j \in I \text{ tal que } x \in A_j\}.$$

[1] También se suele denotar coomo $\exists!$.

- Definimos la intersección de A y B, y la notaremos como $A \cap B$, como el conjunto cuyos elementos son, a la vez, elementos de A y de B. Esto es, $A \cap B = \{x \,/\, x \in A \text{ y } x \in B\}$. Está claro que si $y \in A \cap B$, entonces $y \in A$, luego $A \cap B$ es un subconjunto de A, $A \cap B \subset A$.
  También si $y \in A \cap B$, $y \in B$. Luego $A \cap B \subset B$. Es decir, $A \cap B$ es, a la vez, un subconjunto de A y un subconjunto de B. Puede ocurrir que $A \cap B = \emptyset$ (es decir, no tenga ningún elemento). En este caso, diremos que A y B son subconjuntos disjuntos, como ocurre si, por ejemplo, $A = \{2, 4, 6, 8\}$ y $B = \{1, 3, 5, 7, 9, 11\}$.
  Como en el caso anterior, si I denota un conjunto arbitrario de índices y para cada $i \in I$ disponemos de un conjunto A_i, podemos definir la intersección de tales A_i como
  $$\bigcap_{i \in I} A_i = \{x \,/\, \forall j \in I, x \in A_j\}.$$
- Definimos el complementario de A en B y lo notamos $B \setminus A$ ó $B - A$, como el conjunto formado por todos los elementos de B que no pertenecen a A. De ese modo, $B \setminus A = \{x \in B \,/\, x \notin A\}$. Trivialmente, $B \setminus B = \emptyset$, $B \setminus \emptyset = B$, para cualquier conjunto B.
  Si, por ejemplo, $A = \{1, 5, a, b, 8, c, d\}$ y $B = \{3, 5, a, 9, d, z, y\}$, entonces $B \setminus A = \{3, 9, z, y\}$ y $A \setminus B = \{1, b, 8, c\}$.
  Hay propiedades que nos relacionan estas "operaciones" entre conjuntos. Por ejemplo, dados conjuntos A, B y C tenemos que $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.
  Como es una igualdad entre conjuntos, necesitamos ver que cada uno de ellos es un subconjunto del otro. Es decir, tenemos que probar que $(A \cup B) \cap C \subset (A \cap C) \cup (B \cap C)$ y que $(A \cap C) \cup (B \cap C) \subset (A \cup B) \cap C$.
  Sea entonces $x \in (A \cup B) \cap C$. Esto nos dice que $x \in A \cup B$ y $x \in C$. Por tanto, o bien $x \in A$ y $x \in C$ o bien $x \in B$ y $x \in C$. Es decir, o bien $x \in A \cap C$ o bien $X \in B \cap C$. Luego $x \in (A \cap C) \cup (B \cap C)$ y tenemos la primera condición.
  Por otro lado, si $x \in (A \cap C) \cup (B \cap C)$, tenemos que o bien $x \in A$ y $x \in C$ o bien $x \in B$ y $x \in C$. Esto nos dice que $x \in A$ ó $x \in B$, pero siempre $x \in C$. Luego $x \in A \cup B$ y $x \in C$ y, así, $x \in (A \cup B) \cap C$.

Como **ejercicios**, demostrar las siguientes propiedades para cualquiera conjuntos A, B y C:

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

Introducimos ahora, dado un conjunto X, un nuevo conjunto, llamado conjunto de las partes de X, cuyos elementos son todos los subconjuntos de X. (Aquí cada elemento es un conjunto). Lo notamos como:

$$\mathcal{P}(X) = \{A \,/\, A \subset X\}.$$

Por ejemplo, si $X = \{1, 2, 3\}$, entonces $\mathcal{P}(X) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, X\}$.
Si el conjunto X tiene n elementos, el conjunto $\mathcal{P}(X)$ tiene 2^n elementos.

Dado un conjunto X, en $\mathcal{P}(X)$ podemos considerar como "operaciones" la unión, la intersección y el complementario de un elemento $A \in \mathcal{P}(X)$ en X.

Dados dos conjuntos A, B, definimos su producto cartesiano, notado $A \times B$ como el conjunto de todos los pares ordenados (x, y) donde x es un elemento arbitrario de A e y es un elemento arbitrario de B. Es decir,

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

El hecho de que el par sea "ordenado" significa que (x, y) e (y, x) son elementos distintos. Esto está claro si A y B son distintos, pues si $(x, y) \in A \times B$ nadie nos puede asegurar que (y, x) pertenezca también a $A \times B$. Si $B = A$, los pares (x, y) y (z, w) coincidirán si y solo si $x = z$ e $y = w$.

Ejemplo:

Si $A = \{1, 2, 3\}$ y $B = \{a, b, c\}$ entonces $A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c), (3, a), (3, b), (3, c)\}$.

Esta definición la podemos generalizar a un número finito de conjuntos. Si A_1, A_2, ..., A_n son conjuntos entonces:

$$A_1 \times A_2 \times \cdots \times A_n = \{(x_1, x_2, \ldots, x_n) \,/\, \forall i \in \{1, \ldots, n\}, x_i \in A_i\}.$$

Un elemento $(x_1, x_2, \ldots, x_n)$ se llama n-tupla. Por ejemplo, si $n \in \mathbb{N}$ entonces

$$\mathbb{R}^n = \mathbb{R} \times \overbrace{\cdots}^{n} \times \mathbb{R} = \{(x_1, x_2, \ldots, x_n) \,/\, \forall i \in \{1, \ldots, n\}, x_i \in \mathbb{R}\}.$$

Los elementos de $\mathbb{R}^n$ se llaman n-tuplas de números reales.

2. Aplicaciones entre conjuntos. Tipos de aplicaciones. Composición de aplicaciones.

Sean X e Y dos conjuntos arbitrarios. Una correspondencia $\mathcal{C}$ entre X e Y es un subconjunto arbitrario del producto cartesiano $X \times Y$. Es decir, $\mathcal{C} \subset X \times Y$. Si el par ordenado $(x, y) \in \mathcal{C}$, diremos que y le corresponde a x por $\mathcal{C}$, o que $\mathcal{C}(x) = y$.

Por ejemplo, si $X = \{1, 2, 3, 4\}$ e $Y = \{a, b, c\}$, entonces $\mathcal{C} = \{(1, a), (2, c), (1, c), (3, b)\}$ es una correspondencia entre X e Y y tenemos $\mathcal{C}(1) = a$, $\mathcal{C}(2) = c$, $\mathcal{C}(1) = c$, $\mathcal{C}(3) = b$. Fijémonos en que en este caso, al elemento 1 de X le corresponden tanto el elemento a de Y como el elemento c, mientras que al elemento 4 no le corresponde ningún elemento de Y.

Si esto no ocurre, es decir si f es una correspondencia entre X e Y de manera que $\forall x \in X \; \exists_1 y \in Y$ de forma que $(x, y) \in f$ ó $f(x) = y$, diremos que f es una aplicación de X en Y y lo notamos $f : X \longrightarrow Y$. En este caso X se llamará el dominio de f e Y se llamará el codominio ó recorrido de f. Si $f(x) = y$, diremos que y es la imagen de x por f. Así, una aplicación de X en Y está definida cuando, además de conocer X e Y conocemos el valor de $f(x)$ $\forall x \in X$.

Dado un conjunto X y un subconjunto propio suyo $A \subset X$ podemos destacar dos aplicaciones:

1. La aplicación identidad en X, que notaremos $1_X : X \longrightarrow X$, definida de forma que $\forall x \in X, 1_X(x) = x$.

2. La aplicación de inclusión de A en X que notaremos $i_A : A \longrightarrow X$, definida de forma que $\forall a \in A$, $i_A(a) = a$.

Debemos fijarnos en que, aunque $\forall a \in A$, $1_X(a) = i_A(a) = a$, las dos aplicaciones anteriores no son iguales, puesto que sus dominios no coinciden. Es decir, si $f : X \longrightarrow Y$ y $g : Z \longrightarrow W$ son aplicaciones de X en Y y de Z en W, respectivamente, diremos que $f = g$ si y solo si coinciden los dominios ($X = Z$), los codominios ($Y = W$) y, como $X = Z$, $\forall x \in X$, $f(x) = g(x)$.
Otros ejemplos de aplicaciones serían:

- En el caso anterior de $X = \{1, 2, 3, 4\}$, $Y = \{a, b, c\}$, si $f(1) = a$, $f(2) = c$, $f(3) = c$, $f(4) = c$, f nos da una aplicación de X en Y.

- Si definimos $g : X \longrightarrow Y$ mediante $g(1) = g(2) = g(3) = g(4) = b$, g serían también una aplicación de X en Y y, en este caso, las imágenes de todos los elementos de X son iguales a b.

- En general, si X e Y son dos conjuntos y elegimos un elemento (fijo) $y \in Y$ la aplicación $C_y : X \longrightarrow Y$ tal que $\forall x \in X$, $C_y(x) = y$, se llama la aplicación constante de valor y de X en Y.

- Todas las funciones trigonométricas sen, cos, tan, cot, sec, csc son aplicaciones de $\mathbb{R}$ en $\mathbb{R}$.

Sean ahora dos aplicaciones $f : X \longrightarrow Y$ y $g : Y \longrightarrow Z$ (nótese que el dominio de g coincide con el codominio de f). A partir de ambas, podemos definir una nueva aplicación $g \circ f$, cuyo dominio será el dominio de f y cuyo codominio será el codominio de g, de manera que $\forall x \in X$, $(g \circ f)(x) = g(f(x))$. Es decir, a x le aplicamos f y obtenemos un elemento (único) de Y. Por tanto, a este elemento de Y le aplicamos g y, al resultado, $g(f(x))$ es a lo que llamamos la imagen de x por $g \circ f$, que claramente es una aplicación con dominio X y codominio Z, $g \circ f : Y \longrightarrow Z$ y que llamaremos la composición de f y g (nótese que "leemos" las aplicaciones de $g \circ f$ de derecha a izquierda, primero f y luego g).
Si ahora $h : Z \longrightarrow W$ es otra aplicación, por un lado podemos considerar la composición $h \circ (g \circ f)$, que sería una aplicación con dominio X y codominio W, y por otro lado, también podemos considerar la aplicación $(h \circ g) \circ f$ (como $h \circ g : Y \longrightarrow W$ y $f : X \longrightarrow Y$, las podemos componer) cuyo dominio también es X y cuyo codominio es W. Veremos que ambas aplicaciones son la misma (como ya sabemos que tienen el mismo dominio y el mismo codominio, bastará ver que $\forall x \in X$ obtenemos la misma imagen al aplicarle cualquiera de las dos). Así tenemos que $\forall x \in X$, $(h \circ (g \circ f))(x) = h((g \circ f)(x))$, por la definición de la composición de $g \circ f$ y h. Pero la definición de $g \circ f$ nos da que $(h \circ (g \circ f))(x) = h(g(f(x)))$. Por otro lado, $((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x)))$. Comprobamos que, en ambos casos, el resultado es aplicarle f a x, entonces le aplicamos g a $f(x)$ y, para finalizar, le aplicamos h a $g(f(x))$, obteniendo el mismo resultado en los dos casos.
Diremos, pues, que la composición de aplicaciones (siempre que sea posible) es asociativa.
Podríamos pensar que la composición de aplicaciones también es conmutativa, pero si tenemos $f : X \longrightarrow Y$

y $g : Y \longrightarrow Z$, de manera que podemos considerar $g \circ f$, en general, Z no coincidirá con X, con lo que no tendría sentido pensar en $f \circ g$.
Incluso cuando consideremos aplicaciones cuyo dominio y codominio coinciden y que, por tanto, siempre podremos componer en los dos sentidos, no tiene porqué darse la igualdad.
Por ejemplo, sean las aplicaciones $f : \mathbb{R} \longrightarrow \mathbb{R}$ tal que $\forall x \in \mathbb{R}$, $f(x) = 2x$ y $g : \mathbb{R} \longrightarrow \mathbb{R}$ dada por $g(x) = \cos(x)$. Entonces $g \circ f : \mathbb{R} \longrightarrow \mathbb{R}$ verifica que $(g \circ f)(x) = \cos(2x)$, mientras que $f \circ g : \mathbb{R} \longrightarrow \mathbb{R}$ es tal que $(f \circ g)(x) = 2\cos(x)$. Si estas dos aplicaciones fueran la misma, habrían de tomar el mismo valor $\forall x \in \mathbb{R}$, pero $(g \circ f)(0) = \cos(2 \cdot 0) = \cos(0) = 1$, mientras que $(f \circ g)(0) = 2\cos(0) = 2$.
Por tanto, la composición de aplicaciones, aunque la podamos realizar en ambos sentidos, en general no es conmutativa.

Dada una aplicación $f : X \longrightarrow Y$, diremos que f es inyectiva si cada par de elementos distintos de X tienen imágenes distintas, es decir, si $\forall x, z \in X$ tales que $x \neq z$, entonces $f(x) \neq f(z)$. (Esta condición es equivalente a la siguiente: $\forall x, z \in X$ tales que $f(x) = f(z)$, entonces $x = z$. Ha de tener cuidado de no mezclar ambas).
Por ejemplo, $\forall A \subset X$ propio, $i_A : A \longrightarrow X$ es una aplicación inyectiva, puesto que si $a, b \in A$ y $a \neq b$, entonces $i_A(a) = a \neq b = i_A(b)$.
La aplicación anterior $f : \mathbb{R} \longrightarrow \mathbb{R}$ dada por $f(x) = 2x$ $\forall x \in \mathbb{R}$ es inyectiva, puesto que si $x \neq y$, $f(x) = 2x \neq 2y = f(y)$. Sin embargo, la aplicación $g : \mathbb{R} \longrightarrow \mathbb{R}$, $g(x) = \cos(x)$ no es inyectiva, ya que $\cos(0) = \cos(2\pi)$, pero $0 \neq 2\pi$.

Consideremos $f : X \longrightarrow Y$. Diremos que f admite una inversa por la izquierda si podemos encontrar una aplicación $g_L : Y \longrightarrow X$ tal que $g_L \circ f = 1_X$.
Veamos que una aplicación $f : X \longrightarrow Y$ es inyectiva si y solo si f admite una inversa por la izquierda. Para demostrar este hecho, hemos de considerar que tenemos que ver dos propiedades:

1. La primera propiedad nos diría que si f es inyectiva, hemos de encontrar una inversa por la izquierda g_L de f. Supongamos, pues que f es inyectiva. Para la definición de $g_L : Y \longrightarrow X$, si $y \in Y$ es la imagen de algún elemento de X por f, ese elemento es único, ya que f es inyectiva. Es decir, si $y = f(x)$, x es único y definiríamos $g_L(y) = x$. Por otro lado, elegimos un $x_0 \in X$ fijo, y si $y \in Y$ no es la imagen de ningún elemento de X por f, definimos $g_L(y) = x_0$.
   Así, $g_L : Y \longrightarrow X$ es una aplicación y ahora, $\forall x \in X$, $(g_L \circ f)(x) = g_L(f(x)) = x$ (ya que x se aplica por f en $f(x)$).

2. La segunda propiedad que hemos de ver es que si f admite una inversa por la izquierda, entonces f es inyectiva. Supongamos entonces que $\exists g_L : Y \longrightarrow X$ tal que $g_L \circ f = 1_X$. Sean entonces $x, z \in X$ tales que $x \neq z$. Ahora $(g_L \circ f)(x) = g_L(f(x)) = x \neq z = g_L(f(z)) = (g_L \circ f)(z)$, mientras que si suponemos que $f(x) = f(z)$, $g_L(f(x)) = x = g_L(f(z)) = z$, lo que nos daría una contradicción. Por tanto, si $x \neq z$, entonces $f(x) \neq f(z)$ y f es inyectiva.

Diremos que la aplicación $f : X \longrightarrow Y$ es sobreyectiva si cada $y \in Y$ es imagen de algún elemento

$x \in X$. Esto es, $\forall y \in Y \; \exists \, x \in X \,/\, f(x) = y$.
Por ejemplo, si consideramos $\cos : \mathbb{R} \longrightarrow [-1, 1]$, donde $[-1, 1] = \{x \in \mathbb{R} \,/\, -1 \leq x \leq 1\}$, esta aplicación es sobreyectiva claramente.
También es inmediato ver que dicha aplicación no es inyectiva. Es decir, los conceptos de aplicación inyectiva y aplicación sobreyectiva no están relacionados en general: la aplicación $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ dada por $f(x) = 2x$ es inyectiva, pero no sobreyectiva ($1 \in \mathbb{Z}$ no admite $x \in \mathbb{Z}$ tal que $2x = 1$).

Dada una aplicación $f : X \longrightarrow Y$, diremos que f admite una inversa por la derecha si existe $g_R : Y \longrightarrow X$ tal que $f \circ g_R = 1_Y$.
Veamos que la aplicación $f : X \longrightarrow Y$ es sobreyectiva si y solo si admite una inversa por la derecha. Como en el caso anterior, se trata de una doble implicacion, con lo que tendremos que ver que se verifican dos condiciones:

1. En primer lugar, supongamos que $f : X \longrightarrow Y$ es sobreyectiva. Hemos de encontrar una inversa por la derecha de f.
   Como f es sobreyectiva, $\forall y \in Y \; \exists \, x \in X$ tal que $f(x) = y$. Podría ocurrir que para un cierto y hubiera más de un elemento x en X que se aplicara en y. En este caso elegiríamos uno de ellos y lo llamaríamos x_y. Si solo hay un $x \in X$ tal que $f(x) = y$, a ese x también lo llamamos x_y, y definimos $g_R : Y \longrightarrow X$ mediante $g_R(y) = x_y$. (Ahora sí que $\forall y \in Y$, x_y es único, lo que nos dice que g_R es una aplicación). Además, $\forall y \in Y$, $(f \circ g_R)(y) = f(g_R(y)) = f(x_y) = y$, ya que cada x_y se aplica por f en y.

2. Ahora debemos ver que si $\exists \, g_R : Y \longrightarrow X$ tal que $f \circ g_R = 1_Y$, entonces f es sobreyectiva: sea $y \in Y$, y consideremos $x = g_R(y)$. Este es un elemento de X tal que $f(x) = f(g_R(y)) = (f \circ g_R)(y) = 1_Y(y) = y$. Esto directamente nos dice que f es sobreyectiva.

Aunque hemos visto que los conceptos de inyectividad y sobreyectividad de aplicaciones no están relacionados, podemos considerar aplicaciones que verifiquen ambas propiedades.
Así, diremos que una aplicación $f : X \longrightarrow Y$ es <u>biyectiva</u> si, a la vez, es inyectiva y sobreyectiva. En este caso, para cada $y \in Y$, como f es sobreyectiva, $\exists \, x \in X$ tal que $f(x) = y$. Pero si existiera otro $z \in X$ tal que $f(z) = y$, como $f(z) = y = f(x)$, y f es inyectiva, tendríamos que $z = x$. Por tanto, si f es biyectiva entonces $\forall y \in Y \; \exists_1 \, x \in X$ tal que $f(x) = y$.

<u>Ejemplos:</u>

- Dado cualquier conjunto X, $1_X : X \longrightarrow X$ es claramente biyectiva.
- La aplicación $f : \mathbb{R} \longrightarrow \mathbb{R}$ dada por $f(x) = 2x$ es biyectiva, pues $\forall r \in \mathbb{R}$ únicamente el número real $\frac{r}{2}$ se aplica por f en r.
- Sin embargo, la aplicación $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ dada por $f(x) = 2x$ no es biyectiva.

- $f : \mathbb{R} \longrightarrow \mathbb{R}$ dada por $f(x) = 2x+3$ es biyectiva. En primer lugar es inyectiva porque si $2x+3 = 2y+3$, entonces $2x = 2y$ y por tanto $x = y$. Por otro lado es sobreyectiva porque $\exists\, r \in \mathbb{R}$, $x = \frac{r-3}{2} \in \mathbb{R}$ y $f(x) = r$. Por tanto, es biyectiva.

Si $f : X \longrightarrow Y$ es una aplicación biyectiva, por ser f inyectiva admitirá una inversa por la izquierda $g_L : Y \longrightarrow X$ y, por ser f sobreyectiva, admitirá una inversa por la derecha $g_R : Y \longrightarrow X$. Tendremos entonces que $g_L \circ f = 1_X$ y que $f \circ g_R = 1_Y$. Vamos a ver que en este caso $g_L = g_R$.

Demostración. Claramente $g_L \circ 1_Y = g_L$ ya que $(g_L \circ 1_Y)(y) = g_L(1_Y(y)) = g_L(y) \forall y \in Y$. Entonces $g_L = g_L \circ 1_Y = g_L \circ (f \circ g_R) \overset{(*)}{=} (g_L \circ f) \circ g_R = 1_X \circ g_R \overset{(**)}{=} g_R$, donde en $(*)$ hemos aplicado la asociatividad de la composición de aplicaciones y $(**)$ es cierto porque $\forall y \in Y\ (1_X \circ g_R)(y) = 1_X(g_R(y)) = g_R(y)$. □

Así pues, si f es biyectiva $\exists\, g : Y \longrightarrow X$ tal que $g \circ f = 1_X$ y $f \circ g = 1_Y$. Una tal g se llama inversa de f y, a partir de ahora, la notaremos f^{-1}.
La definición de $f^{-1} : Y \longrightarrow X$ es clara: si $y \in Y$, $\exists_1\, x \in X \,/\, f(x) = y$. Entonces se define $f^{-1}(y) = x$. Como para f^{-1} la aplicación f vuelve a ser una inversa tanto por la izquierda como por la derecha, obtenemos que esta aplicación es también biyectiva.
Ejemplos:

- Claramente para cada conjunto X se tiene que $1_X^{-1} = 1_X$.
- Para la aplicación $f : \mathbb{R} \longrightarrow \mathbb{R}$ dada por $f(x) = 2x$, $f^{-1} : \mathbb{R} \longrightarrow \mathbb{R}$ vendría dada por $f^{-1}(x) = \frac{x}{2}$.
- En el caso de la aplicación $f : \mathbb{R} \longrightarrow \mathbb{R}$ dada por $f(x) = 2x + 3$, $f^{-1} : \mathbb{R} \longrightarrow \mathbb{R}$ vendría dada por $f^{-1}(x) = \frac{x-3}{2}$.

Como **ejercicio**, demostrar que si componemos dos aplicaciones inyectivas, obtenemos una aplicación inyectiva; si se componen dos aplicaciones sobreyectivas, el resultado es otra aplicacion sobreyectiva y, por tanto, al componer dos aplicaciones biyectivas se obtiene una aplicación biyectiva. En este último caso, si $f : X \longrightarrow Y$ y $g : Y \longrightarrow Z$ son dos aplicaciones biyectivas, $g \circ f : X \longrightarrow Z$ es biyectiva. Por ser f biyectiva, $\exists\, f^{-1} : Y \longrightarrow X$, inversa de f y $\exists\, g^{-1} : Z \longrightarrow Y$, inversa de g. Como $g \circ f$ es biyectiva, también tendrá una inversa, $(g \circ f)^{-1}$. Se verifica entonces que $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ (comprobad que ambas aplicaciones tienen el mismo dominio y el mismo codominio), ya que

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ (1_Y \circ f) = f^{-1} \circ f = 1_X,$$

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = (g \circ 1_Y) \circ g^{-1} = g \circ g^{-1} = 1_Z.$$

Si consideramos un conjunto cualquiera X, podemos considerar el conjunto $\mathcal{F}(X) = \{f : X \longrightarrow X \,/\, f$ es biyectiva$\}$. A este conjunto lo llamaremos el conjunto de las permutaciones de X, por lo que cada elemento suyo será una permutación de X. Nótese que en este caso, podremos componer dos permutaciones arbitrarias de X y su resultado seguirá siendo una permutación de X.

3. Relaciones en un conjunto. Relaciones de equivalencia.

Sea X un conjunto arbitrario. Una relación R sobre X es un subconjunto $R \subset X \times X$ de manera que si $x, y \in X$ verifican que $(x, y) \in R$, diremos que x está relacionado con y, y lo notaremos xRy.
Sea, por ejemplo, $X = \{1, 2, 3, 4\}$. Entonces $R = \{(1, 1), (1, 3), (2, 4), (4, 1)\}$ es una relación sobre X en la que $1R1$, $1R3$, $2R4$, $4R1$.
Si la relación R verifica ciertas propiedades, R puede tomar "apellidos" concretos. Así aparecen, por ejemplo, las relaciones de orden que se estudian en Análisis. Nosotros nos ceñiremos a ciertas relaciones especiales, que llamaremos relaciones de equivalencia y que estudiaremos detenidamente.
Sea R una relación sobre (en) X. Diremos que R es:

- Reflexiva si $\forall x \in X$, xRx.
- Simétrica si dados $x, y \in X$ tales que xRy, entonces yRx.
- Transitiva si dados $x, y, z \in X$ tales que, a la vez, xRy, yRz entonces xRz.

La relación R que antes hemos definido no verifica ninguna de estas propiedades.
Si una relación R satisface, a la vez, las 3 propiedades anteriores diremos que R es una relación de equivalencia sobre X.
Ejemplos:

1. Considerad el conjunto de estudiantes de Geometría I del doble grado Informática-Matemáticas. En dicho conjunto podemos definir la siguiente relación: el alumno x estará relacionado con el alumno y si y solo si o bien x e y provienen de la misma provincia de España (son "paisanos") o bien ambos provienen de un país distinto de España. Es inmediato comprobar que esto nos define una relación de equivalencia sobre el conjunto de los estudiantes de Geometría I del doble grado Informática-Matemáticas.

2. Sea ahora $\mathbb{Z}$ el conjunto de los número enteros y $p \in \mathbb{N}$ un número natural. Sobre $\mathbb{Z}$ definimos la siguiente relación R_p: $x, y \in \mathbb{Z}$ verifican que xR_py si y solo si $\exists\, k \in \mathbb{Z}$ tal que $x - y = kp$. Veamos que R_p es una relación de equivalencia sobre $\mathbb{Z}$:

   - R_p es reflexiva porque $\forall x \in \mathbb{Z}$, $x - x = 0 = 0 \cdot p$ y como $0 \in \mathbb{Z}$, se cumple la propiedad.
   - R_p es simétrica: dados $x, y \in \mathbb{Z}$ tales que xR_py, $\exists\, k \in \mathbb{Z}$ tal que $x - y = kp$. Entonces $y - x = -(x - y) = -(kp) = (-k)p$, y como $k \in \mathbb{Z}$, entonces $-k \in \mathbb{Z}$ lo que nos dice que yR_px.
   - R_p es transitiva: dados $x, y, z \in \mathbb{Z}$ tales que xR_py, yR_pz, $\exists\, k_1 \in \mathbb{Z}$ tal que $x - y = k_1p$ y $\exists\, k_2 \in \mathbb{Z}$ tal que $y - z = k_2p$. Entonces $x - z = (x - y) + (y - z) = k_1p + k_2p = (k_1 + k_2)p$, pero siendo $k_1, k_2 \in \mathbb{Z}$, entonces $k_1 + k_2 \in \mathbb{Z}$, y así, xR_pz.

   Esta relación se llama relación de equivalencia módulo p sobre $\mathbb{Z}$. En el caso en que $p = 1$, obtenemos una relación trivial, porque dos números enteros cualesquiera están relacionados mediante R_1, ya que su diferencia sería otro número entero y, por tanto, sería igual que el producto de ese entero y

1.

Sin embargo, en la relación módulo 2, tendríamos que todos los enteros pares estarían relacionados entre sí, todos los enteros impares también estarían relacionados entre sí, pero un entero par no estaría relacionado con ninguno impar.

Sea, pues, R una relación de equivalencia sobre el conjunto X. Dado un elemento $x \in X$, definimos su clase de equivalencia respecto de R y la notamos $[x]$ como el subconjunto de R dado por $[x] = \{y \in X \,/\, yRx\}$. Diremos que x es un representante de la clase de equivalencia $[x]$ (la palabra un significa que dicho representante no es, en general, único, pues si $y \in X$ es distinto de x pero yRx, y es también un representante de $[x]$, como veremos a continuación). Supongamos, pues, que yRx. Hemos de ver que $[y] = [x]$. Como se trata de subconjuntos de X, hemos de comprobar que se da la doble inclusión.
Sea, pues, $z \in [y]$. Esto significa que zRy, pero como hemos supuesto que yRx, la propiedad transitiva nos asegura que zRx y, por definición, $z \in [x]$. Así, $[y] \subset [x]$.
Si ahora $z \in [x]$, tendremos que zRx. Como yRx, la propiedad simétrica nos asegura que xRy. Entonces la transitividad nos da que como zRx, xRy entonces zRy, con lo que $z \in [y]$, y por lo tanto $[x] \subset [y]$.

Es más, si tengo dos clases de equivalencia para la relación de equivalencia R, $[x]$ e $[y]$, entonces o bien $[x] = [y]$ o bien $[x] \cap [y] = \emptyset$. Para demostrarlo, supongamos que $[x] \cap [y] \neq \emptyset$. Esto nos dice que $\exists\, z \in [x] \cap [y]$. Entonces $z \in [x]$ y $z \in [y]$, con lo que zRx y zRy. Pero si zRx, por la simetría xRz y, como además, zRy, la transitividad asegura que xRy y, por lo que hemos visto, $[x] = [y]$.

Dado un conjunto X, una partición de X es una familia de subconjuntos de X disjuntos dos a dos cuya unión es todo X. Es decir, $\{A_1, A_2, \ldots, A_n\}$ donde $\forall j \in \{1, \ldots, n\}$ $A_j \subset X$ es una partición de X si:

1. $\forall i, j \in \{1, \ldots, n\}$ tales que $i \neq j$, $A_i \cap A_j = \emptyset$,
2. $\bigcup_{i \in \{1,\ldots,n\}} A_i = X$.

Por lo que acabamos de ver, si sobre X tenemos definida una relación de equivalencia, $\{[x] \,/\, x \in X\}$ nos da una partición de X.
Con la siguiente definición hemos de tener cuidado porque en ella $[x]$ va a tener un significado distinto del que acabamos de ver: sea X un conjunto y R una relación de equivalencia. Definiremos el conjunto cociente de X por R y lo notaremos X/R como el conjunto cuyos elementos son las clases de equivalencia por R de elementos de X ($[x]$ es un subconjunto de X, pero en el conjunto X/R no es más que un elemento).
Si consideramos la primera relación de equivalencia que introdujimos, para un alumno x su clase de equivalencia estaría formada por todos los alumnos que han nacido en la misma provincia que él, o si no ha nacido en España, por todos los alumnos de fuera de España. Así, el conjunto cociente tendría como elementos las provincias españolas en las que haya nacido algún alumno y el resto del mundo.
En el caso de R_2 tenemos que $\mathbb{Z}/R_2 = \{[0], [1]\}$ sólo tiene dos elementos, $[0]$, donde están todos los números enteros pares y $[1]$, donde aparecen todos los enteros impares. Este conjunto con dos elementos

lo notaremos $\mathbb{Z}_2$.

Para R_3, $\mathbb{Z}/R_3 = \{[0], [1], [2]\}$. Este caso $[0]$ está formada por todos los múltiplos eneros de 3,

$$[1] = \{\dots, 3l+1, \dots, -8, -5, -2, 1, 4, 7, 10, \dots, 3k+1, \dots\}_{k\in\mathbb{N}, -l\in\mathbb{N}},$$

$$[2] = \{\dots, 3l+2, \dots, -10, -7, -4, -1, 2, 5, 8, 11, \dots, 3k+2, \dots\}_{k, -l\in\mathbb{N}},$$

este conjunto lo notaremos $\mathbb{Z}_3$.

En general, si $p \in \mathbb{N}$, $\mathbb{Z}_p = \mathbb{Z}/R_p = \{[0], [1], \dots, [p-1]\}$ puesto que $[p] = [0]$, $[p+1] = [1]$, etc.

Sean dos conjuntos X e Y y una aplicación $f : X \longrightarrow Y$. Sobre X podemos definir la siguiente relación a partir de f, R_f: si $x, z \in X$, diremos que x está relacionado con z por R_f, xR_fz, si y solo si $f(x) = f(z)$. R_f es una relación de equivalencia:

- Es reflexiva porque como $\forall\, x \in X$, $f(x) = f(x)$, siempre xR_fx.
- Es simétrica: si xR_fz, entonces $f(x) = f(z)$. Esto nos da que $f(z) = f(x)$ y, por tanto, zR_fx.
- Es transitiva: si xR_fz y zR_fw, siendo $x, z, w \in X$, sabemos que $f(x) = f(z)$ y que $f(z) = f(w)$. Por tanto, $f(x) = f(w)$, luego xR_fw.

Consideremos entonces X/R_f. Fijaos que cada clase de equivalencia (como subconjunto de X) contiene a todos los elementos de X que tienen la misma imagen por f. Podemos definir una nueva aplicación con dominio X/R_f y con codominio Y, $\overline{f}$, de la siguiente forma: $\overline{f} : X/R_f \longrightarrow Y$ vendrá dada $\forall\, [x] \in X/R_f$ mediante $\overline{f}([x]) = f(x)$. Hemos de señalar que para ver que, efectivamente, $\overline{f}$ es una aplicación, cada clase en X/R_f tiene una única imagen en Y. El problema está en que si tomamos dos representantes distintos de una misma clase, podría ocurrir que las imágenes por f de dichos representantes fueran distintas, en cuyo caso $\overline{f}$ no estaría bien definida. Es decir, hemos de ver que si $[x] = [z]$, entonces $\overline{f}([x]) = f(x) = f(z) = \overline{f}([z])$, pero eso, en este caso, es inmediato porque si $[x] = [z]$, tenemos que xR_fz y, entonces, $f(x) = f(z)$, que es lo que queríamos.
La propiedad importante que tiene $\overline{f}$ es que, independientemente del carácter de f, $\overline{f}$ siempre es inyectiva, como vamos a demostrar:

Demostración. Supongamos que $[x], [z] \in X/R_f$ son tales que $\overline{f}([x]) \neq \overline{f}([z])$. Esto nos dice que $f(x) \neq f(z)$. Pero por la definición de R_f, como $f(x) \neq f(z)$, x no está relacionado con z; luego $[x] \neq [z]$. □

Veamos un caso concreto de este hecho: sea $\mathbb{R}_0^+ = \{x \in \mathbb{R} \,/\, 0 \leq x\}$. Definimos la aplicación parte entera como $E : \mathbb{R}_0^+ \longrightarrow \mathbb{N} \cup \{0\}$, de la siguiente manera: $\forall\, r \in \mathbb{R}_0^+$, $E(r)$ es el mayor elemento de $\mathbb{N} \cup \{0\}$, m, tal que $m \leq r$. Es decir, cada elemento de $\mathbb{R}_0^+$ será un número decimal $r = m, \ldots$, siendo $m \in \mathbb{N} \cup \{0\}$. Entonces $E(r) = m$. La relación R_E sobre $\mathbb{R}_0^+$ nos da que si $r, r' \in \mathbb{R}_0^+$, $rR_Er' \iff E(r) = E(r')$. Así, tendremos tantas clases de equivalencia como elementos hay en $\mathbb{N} \cup \{0\}$. De hecho, si $m \in \mathbb{N} \cup \{0\}$, $[m] = [m, m+1[^2 = \{r \in \mathbb{R}_0^+ \,/\, m \leq r < m+1\}$, ya que $m+1$ no está relacionado con m, pues $E(m+1) = m+1 \neq m$.
Entonces $\overline{E} : \mathbb{R}_0^+/R_E \longrightarrow \mathbb{N} \cup \{0\}$ es una aplicación inyectiva dada por $\overline{E}([r]) = E(r)$. Además es sobreyectiva, porque dado $n \in \mathbb{N} \cup \{0\}$, $[n] \in \mathbb{R}_0^+/R_E$ y $\overline{E}([n]) = E(n) = n$.

Sea ahora $I = [0, 1] = \{x \in \mathbb{R} \,/\, 0 \leq x \leq 1\}$. Podemos dar una relación de equivalencia sobre I definiendo, para cada elemento de I, su clase de equivalencia (deberemos asegurarnos de que las clases de equivalencia forman una partición de I; esto es válido no solo para este ejemplo, sino en general).
Definamos sobre I la relación de equivalencia R de la siguiente forma: $\forall\, x \in]0, 1[= \{x \in \mathbb{R} \,/\, 0 < x < 1\}$,

[2] Es probable que os suene más la notación $[m, m+1)$ para los intervalos semiabiertos, sin embargo los notaremos así ya que es la notación que suelen usar en Análisis.

su clase de equivalencia será $[x] = \{x\}$ (tales elementos solo están relacionados consigo mismos), mientras que $[0] = [1] = \{0, 1\}$ (es decir, $0R1$ y $1R0$).
Consideremos el conjunto cociente I/R. En este conjunto cociente cada punto (elemento) de $]0, 1[$ nos da un único elemento, mientras que 0 y 1 nos dan también un único punto. ¿Con qué conjunto podemos identificar I/R? Consideremos $\mathbb{S}^1 = \{(x_1, x_2) \in \mathbb{R}^2 \,/\, x_1^2 + x_2^2 = 1\}$ (el círculo en $\mathbb{R}^2$ de centro $(0, 0)$ y radio 1). Podemos definir la siguiente aplicación: $f : I/R \longrightarrow \mathbb{S}^1$, $\forall\, [x] \in I/R$, definimos $f([x]) = (\cos(2\pi x), \text{sen}(2\pi x))$. Como $\cos^2(2\pi x) + \text{sen}^2(2\pi x) = 1$, $\forall\, [x] \in I/R$, $f([x]) \in \mathbb{S}^1$. Como antes, para que f esté bien definida hemos de asegurarnos que no depende del representante de la clase que estemos tomando en I/R. Si $[x]$ la obtenemos para $x \in]0, 1[$ no tenemos problema, porque en este caso el único representante de esa clase es x. Si tomamos $[0]$ el único representante suyo que no es 0 es 1. Es decir, $[0] = [1]$. En este caso $f([0]) = (\cos(0), \text{sen}(0)) = (1, 0)$ y $f([1]) = (\cos(2\pi), \text{sen}(2\pi)) = (1, 0)$. Así, efectivamente, f está bien definida.
Es inmediato ver que esta aplicación es biyectiva, de manera que, como conjuntos, podemos identificar I/R con $\mathbb{S}^1$.

4. Operaciones sobre un conjunto. Estructuras sobre un conjunto: grupos, cuerpos.

Sea X un conjunto. Una ley de composición interna (u operación) sobre X es una aplicación $\square : X \times X \longrightarrow X$. Si $(x, y) \in X \times X$ (es decir, $x, y \in X$) notaremos $\square(x, y) = x \square y$, que será el resultado de aplicar la operación $\square$ a x e y.

Ejemplos:

1. $+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ es una operación, donde $+(n, m) = n + m$, la suma de m y n. Esta operación verifica las siguientes propiedades:

   a) Es asociativa, pues $\forall n, m, p \in \mathbb{N}$ se verifica $(n + m) + p = n + (m + p)$.

   b) Es conmutativa, ya que $\forall n, m \in \mathbb{N}$, se verifica $n + m = m + n$.

2. $\cdot : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ es una operación sobre $\mathbb{N}$, dada por $\cdot(n, m) = n \cdot m$. Ahora tenemos las siguientes propiedades:

   a) Asociativa: $\forall n, m, p \in \mathbb{N}$ se verifica $(n \cdot m) \cdot p = n \cdot (m \cdot p)$.

   b) Conmutativa: $\forall n, m \in \mathbb{N}$ se verifica $n \cdot m = m \cdot n$.

   c) Existe un elemento neutro, $1 \in \mathbb{N}$, tal que $1 \cdot n = n \cdot 1 = n$, $\forall n \in \mathbb{N}$.

Las dos operaciones anteriores verifican, además, la siguiente propiedad distributiva: $\forall m, n, p \in \mathbb{N}$, $(m + n) \cdot p = m \cdot p + n \cdot p$.
Podemos definir, asimismo, la suma y el producto de número enteros, $+ : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$, $\cdot : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$. La suma de números enteros tienes dos propiedades que no tenía la de números naturales. Por un lado,

la existencia de elemento neutro, $0 \in \mathbb{Z}$, tal que $0 + m = m + 0 = m$, $\forall m \in \mathbb{Z}$ y, para cada $m \in \mathbb{Z}$, la existencia de un opuesto (o simétrico), $-m$, verificando $m + (-m) = (-m) + m = 0$.
Si consideramos la suma y el producto de números racionales $+ : \mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{Q}$, $\cdot : \mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{Q}$, además de las propiedades que verifican la suma y el producto en los casos anteriores, tenemos otra propiedad nueva. Recordad que

$$\mathbb{Q} = \left\{ \frac{p}{q} \,\middle/\, p, q \in \mathbb{Z},\ q \neq 0 \right\}.$$

Entonces $\forall \frac{q}{p} \in \mathbb{Q} \setminus \{0\}$[3], tendremos que $p, q \in \mathbb{Z}$ con $p, q \neq 0$. Así, $\frac{q}{p} \in \mathbb{Q} \setminus \{0\}$ y $\frac{p}{q} \cdot \frac{q}{p} = \frac{p \cdot q}{q \cdot p} = 1$. Luego cada elemento $\frac{p}{q} \in \mathbb{Q} \setminus \{0\}$ admite un inverso (ó simétrico para el producto), $\frac{q}{p}$.
Si consideramos la suma y el producto de números reales tendremos las mismas propiedades que se verifican para los enteros.
Sea X un conjunto y consideremos $\mathcal{B}(X)$ el conjunto de las aplicaciones biyectivas del conjunto X en sí mismo (o permutaciones de X). Definimos $\circ : \mathcal{B}(X) \times \mathcal{B}(X) \longrightarrow \mathcal{B}(X)$ mediante $\circ(g, f) = g \circ f$. Esto nos da una operación sobre $\mathcal{B}(X)$, que tiene las siguientes propiedades:

- Asociativa, pues se da, en general, para la composición de aplicaciones.
- Existe un elemento neutro, la aplicación identidad en X, 1_X, tal que $f \circ 1_X = 1_X \circ f = f$, $\forall f \in \mathcal{B}(X)$.
- Existe un inverso, $\forall f \in \mathcal{B}(X)\ \exists\, f^{-1} \in \mathcal{B}(X)$ tal que $f \circ f^{-1} = f^{-1} \circ f = 1_X$.
- Sabemos, sin embargo, que la operación de composición no es conmutativa.

Consideremos $p \in \mathbb{N}$ y $\mathbb{Z}_p$ el conjunto de los enteros módulo p. Podemos definir ahora una suma en $\mathbb{Z}_p$ de la siguiente manera: $\forall\, [m], [n] \in \mathbb{Z}_p$, $[m] + [n] = [m + n]$ (la suma de dos clases consiste en tomar la suma de sus representantes y quedarnos con la clase del resultado). Como vimos anteriormente, para que esta suma esté bien definida, necesitamos comprobar que no depende de los representantes de cada clase. Es decir, si $[m] = [r]$ y $[n] = [s]$, tenemos que ver que $[m] + [n] = [m + n] = [r + s] = [r] + [s]$. Si esto no ocurriera, la suma de las dos clases nos daría dos elementos distintos en $\mathbb{Z}_p$ y la suma no estaría bien definida. Veamos por tanto que sí que sucede:

Demostración. Partimos de que $[m] = [r]$, es decir, mR_pr y, por tanto, $\exists\, k_1 \in \mathbb{Z}$ tal que $m - r = k_1 p$. Como, además, $[n] = [s]$, nR_ps, luego $\exists\, k_2 \in \mathbb{Z}$ tal que $n - s = k_2 p$.
Hemos de ver que $[m + n] = [r + s]$, es decir, que $(m + n)R_p(r + s)$. Entonces $(m + n) - (r + s) \overset{(*)}{=} (m - r) + (n - s) = k_1 p + k_2 p = (k_1 + k_2)p$, y como $k_1, k_2 \in \mathbb{Z}$, entonces $k_1 + k_2 \in \mathbb{Z}$, lo que prueba lo que queríamos. (En $*$ hemos aplicado la asociatividad y conmutatividad de números enteros y la distributividad del producto con respecto a la suma). □

Es fácil ver ahora que esta suma de clases hereda las propiedades de la suma en $\mathbb{Z}$:

- $\forall\, [m], [n], [r] \in \mathbb{Z}_p$, se tiene $([m]+[n])+[r] = [m]+([n]+[r])$, ya que $([m]+[n])+[r] = [m+n]+[r] = [(m + n) + r] \overset{(*)}{=} [m + (n + r)] = [m] + [n + r] = [m] + ([n] + [r])$, donde en $*$ hemos aplicado la asociatividad de la suma de números enteros.

[3] También notado como $\mathbb{Q}^*$.

- $\exists\,[0] \in \mathbb{Z}_p$ tal que $\forall\,[m] \in \mathbb{Z}_p$ se verifica $[0]+[m]=[m]+[0]=[m]$. Veamos una de las igualdades: $[0]+[m]=[0+m] \overset{(**)}{=} [m]$, donde en $**$ hemos aplicado que 0 es el elemento neutro de la suma de números enteros. La otra igualdad se prueba análogamente.

- $\forall\,[m] \in \mathbb{Z}_p$, $\exists\,[-m] \in \mathbb{Z}_p$ tal que $[m]+[-m]=[-m]+[m]=[0]$. En efecto, tenemos por un lado que $[m]+[-m]=[m+(-m)] \overset{(***)}{=} [0]$, donde en $***$ lo que aplicamos es que $-m$ es el opuesto de m en $\mathbb{Z}$. La otra igualdad se demuestra análogamente y, a partir de ahora podemos escribir $[-m]=-[m]$.

- $\forall\,[n],[m] \in \mathbb{Z}_p$, $[n]+[m]=[n+m] \overset{(****)}{=} [m+n]=[m]+[n]$, donde en $****$ aplicamos la conmutatividad de la suma de enteros.

Para cada p, podemos representar esta suma de clases mediante una tabla. En los casos $p=2$ ó $p=3$ se tiene:

1. Caso $(\mathbb{Z}_2,+)$:

$+$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

   Donde en la intersección de cada fila y cada columna colocamos el resultado de la suma de las correspondientes clases.
   Así, como la tabla es simétrica respecto de la diagonal, $+$ es conmutativa; como la fila a cuya izquierda aparece $[0]$ (2^{a} fila) coincide con la fila a cuya izquierda aparece el signo $+$ (1^{a} fila), la suma tiene como elemento neutro $[0]$ y para cada elemento de la 1^{a} columna vemos que en la correspondiente fila hay solo un $[0]$, el elemento de la primera fila que está sobre ese $[0]$ es el opuesto del elemento en cuestión.

2. Caso $(\mathbb{Z}_3,+)$:

$+$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$[0]$
$[2]$	$[2]$	$[0]$	$[1]$

   Podéis comprobar que lo dicho para $\mathbb{Z}_2$ se cumple también aquí.

Por otro lado, a partir del producto de números enteros, podemos definir un producto en $\mathbb{Z}_p$ de la siguiente forma: $\forall\,[m],[n] \in \mathbb{Z}_p$, $[m]\cdot[n]=[m\cdot n]$. Igual que antes, hemos de asegurarnos que esta definición es buena; esto es, si $[m]=[r]$ y $[n]=[s]$, tenemos que comprobar que $[m]\cdot[n]=[m\cdot n]=[r\cdot s]=[r]\cdot[s]$.

Demostración. Partimos de que como $[m]=[r]$, $\exists\,k_1 \in \mathbb{Z}$ tal que $m-r=k_1p$ y al ser $[n]=[s]$ entonces $\exists\,k_2 \in \mathbb{Z}$ tal que $n-s=k_2p$. Hemos de demostrar que $m\cdot nR_pr\cdot s$.

Entonces $m \cdot (n - s) = (mk_2) \cdot p = m \cdot n - m \cdot s$ y $(m - r) \cdot s = (k_1 s)p = m \cdot s - r \cdot s$. De manera que, si sumamos ambas expresiones, tenemos:

$$(m \cdot n - m \cdot s) + (m \cdot s - r \cdot s) = (mk_2) \cdot p + (k_1 s) \cdot p.$$

Esto nos da $m \cdot n - r \cdot s = (mk_2 + k_1 s) \cdot p$ y, al ser $m, k_2, k_1, s \in \mathbb{Z}$ entonces $mk_2 + k_1 s \in \mathbb{Z}$, con lo que, efectivamente, $[m \cdot n] = [r \cdot s]$. □

Como en el caso de la suma, el producto de clases módulo p hereda las propiedades del producto de números enteros, a saber:

- $\forall\, [m], [n], [r] \in \mathbb{Z}_p$ se tiene $([m]\cdot[n])\cdot[r] = [m\cdot n]\cdot[r] = [(m\cdot n)\cdot r] = [m\cdot(n\cdot r)] = [m]\cdot[n\cdot r] = [m]\cdot([n]\cdot[r])$.
- $\forall\, [m], [n] \in \mathbb{Z}_p$, $[m] \cdot [n] = [m \cdot n] = [n \cdot m] = [n] \cdot [m]$.
- $[1] \in \mathbb{Z}_p$ (suponemos $p > 1$, pues el caso de $p = 1$ es trivial), verifica que $\forall\, [m] \in \mathbb{Z}_p$, $[1] \cdot [m] = [m] \cdot [1] = [m]$.

De nuevo podemos construir $\forall\, p \in \mathbb{N}$ una tabla para el producto en $\mathbb{Z}_p$.

1. En el caso de $(\mathbb{Z}_2, \cdot)$ sería:

$\cdot$	$[0]$	$[1]$
$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$

2. Y en el caso de $(\mathbb{Z}_3, \cdot)$ sería:

$\cdot$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$
$[2]$	$[0]$	$[2]$	$[1]$

Considerando la primera tabla vemos que el único elemento distinto de [0] sería [1] y este admite como inverso a él mismo.
En la segunda tabla los elementos distintos de [0] son [1] y [2]. [1] admite como inverso a [1] y [2] admite como inverso a [2].
Esto no ocurre, por ejemplo, cuando consideramos $p = 4$. Para $(\mathbb{Z}_4, \cdot)$ tendríamos la tabla:

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

En este caso, en la fila de [2] no aparece [1], lo que nos indica que [2] no tiene inverso.
Por otro lado en $\mathbb{Z}_p$ también tendremos la distributividad del producto de clases con respecto a la suma de clases. Es decir, $\forall\, [m], [n], [r] \in \mathbb{Z}_p$, $([m]+[n])\cdot[r] = [m]\cdot[r]+[n]\cdot[r]$, ya que $([m]+[n])\cdot[r] = [m+n]\cdot[r] = [(m+n)\cdot r] = [m\cdot r + n\cdot r] = [m\cdot r] + [n\cdot r] = [m]\cdot[r] + [n]\cdot[r]$.

4.1. Definición de grupo

Un grupo es un par $(G, \square)$, donde G es un conjunto no vacío y $\square$ una ley de composición interna sobre G, es decir, $\square : G \times G \longrightarrow G$ que verifica las siguientes propiedades:

1. Asociativa: $\forall\, g_1, g_2, g_3 \in G$, $(g_1 \square g_2) \square g_3 = g_1 \square (g_2 \square g_3)$.

2. Existencia de elemento neutro: $\exists\, e \in G$ tal que $\forall\, g \in G$ se tiene $e \square g = g \square e = g$.

3. Existencia de elementos simétricos: $\forall\, g \in G\ \exists\, \overline{g} \in G$ tal que $g \square \overline{g} = \overline{g} \square g = e$.

Si además se verifica la conmutatividad de $\square$, esto es, $\forall\, g_1, g_2 \in G$, $g_1 \square g_2 = g_2 \square g_1$, diremos que el grupo $(G, \square)$ es conmutativo o abeliano[4].
Las primeras propiedades que se derivan de la definición de grupo son las siguientes:

1. En un grupo el elemento neutro es único: si suponemos que $\exists\, e, e' \in G$ tales que $\forall\, g \in G$, $e \cdot g = g \cdot e = g$ y que $e' \cdot g = g \cdot e' = g$ tendremos que $e \overset{(*)}{=} e \cdot e' \overset{(**)}{=} e'$, donde en $*$ utilizamos que e' es elemento neutro y en $**$ que lo es e.

2. En un grupo, el simétrico de cada elemento es único: sea $g \in G$ y sean $\overline{g}$, $g' \in G$ tales que $g \square \overline{g} = \overline{g} \square g = e$ y $g \square g' = g' \square g = e$. Entonces

$$\overline{g} = e \,\square \overline{g} \overset{(*)}{=} (g' \square g) \square \overline{g} \overset{(**)}{=} g' \square (g \square \overline{g}) \overset{(***)}{=} g' \square e = g',$$

   donde hemos aplicado en $*$ que g' es simétrico de g, en $**$ la propiedad asociativa y en $***$ que $\overline{g}$ es simétrico de g.

Normalmente, las operaciones que se definen sobre un conjunto para dotarlo de estructura de grupo son sumas o productos. Si $(G, +)$ es un grupo, diremos que el grupo es aditivo y, en este caso, al elemento neutro lo notaremos 0 y al simétrico de cada $g \in G$ lo llamaremos el opuesto de G y lo notaremos $-g$.
Si la operación que tenemos es un producto, a $(G, \cdot)$ lo llamaremos grupo multiplicativo, al elemento neutro lo llamaremos unidad y lo notaremos 1 y al simétrico de cada $g \in G$ lo llamaremos el inverso de G y lo notaremos g^{-1}.

No necesariamente un grupo ha de ser aditivo o multiplicativo. Por los ejemplos que hemos visto anteriormente, dado un conjunto X, el grupo $(\mathcal{B}(X), \circ)$, es decir, las permutaciones del conjunto X con la composición nos proporciona un grupo que no es aditivo ni es multiplicativo. Como vimos este grupo no es abeliano.

Ejemplos:

- $(\mathbb{N}, +)$ no es un grupo porque no hay elemento neutro.

- $(\mathbb{N}, \cdot)$ no es un grupo porque, aunque ahora 1 sí es el elemento neutro, $2 \in \mathbb{N}$ y no tiene inverso.

[4] En honor al matemático noruego Niels Henrik Abel (1802-1829).

- $(\mathbb{Z}, +)$ es un grupo aditivo abeliano.
- $(\mathbb{Z}, \cdot)$ no es un grupo por la misma razón de antes.
- $(\mathbb{Q}, +)$ es un grupo abeliano.
- $(\mathbb{Q}, \cdot)$ no es un grupo porque $0 \in \mathbb{Q}$ no admite inverso. Sin embargo si nos restringimos a $(\mathbb{Q} \setminus \{0\}, \cdot)$ sí es un grupo multiplicativo porque $\forall\, \frac{p}{q} \in \mathbb{Q} \setminus \{0\}$, $p, q \in \mathbb{Z} \setminus \{0\}$ y entonces $\frac{q}{p} \in \mathbb{Q}$ y $\frac{p}{q} \cdot \frac{q}{p} = 1$. Además es un grupo abeliano.
- $(\mathbb{R}, +)$ es un grupo abeliano.
- $(\mathbb{R}, \cdot)$ no es un grupo por la misma razón que en el caso de los racionales. Como en el caso anterior, si nos restringimos a $(\mathbb{R} \setminus \{0\}^5, \cdot)$, obtenemos un grupo multiplicativo y abeliano.
- $(\mathbb{Z}_p, +)$, $p \in \mathbb{N}$, es un grupo aditivo abeliano.
- $(\mathbb{Z}_p, \cdot)$, $p \in \mathbb{N}$ no es un grupo multiplicativo, pues $[0]$ no tiene inverso.

Sea $(G, \square)$ un grupo y $H \subsetneq G$. Si tomamos dos elementos h_1 y h_2 en H, estos son también elementos de G y podemos considerar $h_1 \square h_2$. Este será un elemento de G, pero no podemos asegurar que $h_1 \square h_2 \in H$. Si H verifica que $\forall\, h_1, h_2 \in H$ se tiene $h_1 \square h_2 \in H$, diremos que H es cerrado para la operación $\square$.
Análogamente, si $h \in H$, $h \in G$ y como $(G, \square)$ es un grupo, h tiene un simétrico para $\square$, h^{-1}, que será un elemento de G, pero que no podremos asegurar que pertenezca a H. Como antes, diremos que H es cerrado para los elementos simétricos si $\forall\, h \in H$, $\overline{h} \in H$.
Entonces si H es un subconjunto de $(G, \square)$ que es cerrado para $\square$ y para los elementos simétricos, podemos restringir $\square$ a H, $\square : H \times H \longrightarrow H$ (tiene sentido por ser H cerrado para la operación $\square$), además, como $\square$ sobre G era asociativa y todos los elementos de H lo son de G, seguirá siendo asociativa cuando la consideremos sobre H. Como $\forall\, h \in H$, $\overline{h} \in H$ de modo que $h \square \overline{h} = e \in H$, con lo que el mismo neutro en G para $\square$ nos sirve como neutro para H y, además $\forall\, h \in H$ $\overline{h} \in H$. En este caso diremos que $(H, \square)$ es un subgrupo de $(G, \square)$ o, simplemente que H es un subgrupo de G. Si $(G, \square)$ es abeliano también lo será $(H, \square)$.
Las dos condiciones que hemos impuesto antes las podemos condensar en una: si $H \subsetneq G$ y $(G, \square)$ es un grupo, H será un subgrupo de G si y solo si $\forall\, h_1, h_2 \in H$ se tiene $h_1 \square \overline{h_2} \in H$, siendo $\overline{h_2}$ el simétrico de H (en principio sería un elemento de G). Vamos a demostrar este hecho:

Demostración. $\Longrightarrow$) Claramente, si suponemos que H es un subgrupo de G, se verifica la otra condición.
$\Longleftarrow$) Supongamos ahora que $\forall\, h_1, h_2 \in H$ se cumple $h_1 \square \overline{h_2} \in H$. Hemos de ver que H es un subgrupo de G.
Si tomamos $h_1 \in H$, ha de verificarse que $h_1 \square \overline{h_1} \in H$. Pero ese elemento es e (neutro de G para $\square$) lo que nos indica que $e \in H$. Entonces $\forall\, h \in H$, $e \square \overline{h} = \overline{h} \in H$. Luego el simétrico de cada elemento de H pertenece a H. Como $\forall\, h \in H$ se tiene que $\overline{\overline{h}} = h$, dados $h_1, h_2 \in H$ sabemos que $h_1, \overline{h_2} \in H$. Si aplicamos la propiedad tendremos que $h_1 \square \overline{\overline{h_2}} = h_1 \square h_2 \in H$ y, efectivamente, H es un subgrupo de G. $\square$

[5] También notado como $\mathbb{R}^*$.

Así, por ejemplo, $(\mathbb{Z}, +)$ es un subgrupo de $(\mathbb{Q}, +)$ que es, a su vez, un subgrupo de $(\mathbb{R}, +)$.
Sin embargo, $(\mathbb{Z} \setminus \{0\}, \cdot)$ no es un subgrupo de $(\mathbb{Q} \setminus \{0\}, \cdot)$ pues, aunque el producto de números enteros nos da un entero ($\mathbb{Z} \setminus \{0\}$ es cerrado para el producto de $\mathbb{Q} \setminus \{0\}$), $2 \in \mathbb{Z} \setminus \{0\} \subset \mathbb{Q} \setminus \{0\}$ tiene como inverso en $\mathbb{Q} \setminus \{0\}$ a $\frac{1}{2} \notin \mathbb{Z} \setminus \{0\}$.
$(\mathbb{Q} \setminus \{0\}, \cdot)$ sí que es un subgrupo de $(\mathbb{R} \setminus \{0\}, \cdot)$.

4.2. Estructura de cuerpo

Un cuerpo será un triplete (ó terna) $(K, +, \cdot)$, siendo K un conjunto no vacío, $+$ y $\cdot$ leyes de composición interna sobre K, es decir, $+ : K \times K \longrightarrow K$, $\cdot : K \times K \longrightarrow K$ verificando las siguientes condiciones:

1. $(K, +)$ es un grupo abeliano.
2. $\cdot$ es asociativa.
3. $\exists\, 1 \in K$, elemento neutro para $\cdot$; así, $\forall\, k \in K$, $k \cdot 1 = 1 \cdot k = k$.
4. $\forall\, k \in K \setminus \{0\}$, $\exists\, k^{-1} \in K$ tal que $k \cdot k^{-1} = k^{-1} \cdot k = 1$; es decir, cada elemento de K distinto del elemento neutro para la suma admite un inverso.
5. Se verifican las propiedades de distributividad del producto con respecto a la suma:
   - $x \cdot (y + z) = x \cdot y + x \cdot z$,
   - $(x + y) \cdot z = x \cdot y + x \cdot z$,

   $\forall\, x, y, z \in K$.

Como $(K, +)$ es un grupo ya sabemos que su elemento neutro, 0, y el opuesto $-x$ de cada $x \in K$ son únicos.
Análogamente se puede ver que 1 y k^{-1} $\forall\, k \in K$ son únicos. Además, si $1 = 0$, $\forall\, k \in K$ tendríamos $1 \cdot k = k = 0 \cdot k = (0+0) \cdot k = 0 \cdot k + 0 \cdot k$. Entonces $0 = 0 \cdot k + (-(0 \cdot k)) = 0 \cdot k + 0 \cdot k + (-(0 \cdot k)) = 0 \cdot k + 0 = 0 \cdot k$. Por tanto, $1 \cdot k = 0 \cdot k + 0 \cdot k = 0 + 0 = 0 = k$, y el único elemento de K sería 0. Este caso es trivial y por tanto, como consideramos cuerpos que no se reduzcan a $\{0\}$, podremos afirmar que $1 \neq 0$.
Si, además, se verifica que

6. El producto es conmutativo: $\forall\, x, y \in K$, $x \cdot y = y \cdot x$,

entonces decimos que $(K, +, \cdot)$ es un cuerpo conmutativo.
Como, en cada caso, $+$ y $\cdot$ estarán definidos y los conoceremos, a partir de ahora escribiremos simplemente K cuando nos refiramos a un cuerpo.

Ejemplos:

1. Aunque en $\mathbb{N}$ podamos considerar la suma y el producto conocidos, estas operaciones no dotan a $\mathbb{N}$ de estructura de cuerpo (no existe el opuesto de un número natural arbitrario).
2. Lo mismo ocurre con la suma y el producto conocidos en $\mathbb{Z}$ (en este caso lo que falla es la existencia de un inverso para cada número entero no nulo).
3. Como habíamos visto que $(\mathbb{Q}, +)$ es un grupo abeliano, que $(\mathbb{Q} \setminus \{0\}, \cdot)$ es también un grupo abeliano y además se verifica la propiedad distributiva del producto respecto de la suma (al ser el producto conmutativo las dos condiciones anteriores se convierten en una sola), podemos afirmar que $(\mathbb{Q}, +, \cdot)$ es un cuerpo conmutativo.

4. Al igual que el caso anterior, $(\mathbb{R}, +, \cdot)$ es un cuerpo conmutativo.

Analicemos ahora el caso de $(\mathbb{Z}_p, +, \cdot)$, siendo $+$ la suma de clases que definimos anteriormente y $\cdot$ el producto de clases asimismo definido.
Ya sabemos que $\forall\, p \in \mathbb{N}$ (como dijimos, supondremos $p \neq 1$, porque el caso $p = 1$ es trivial), $(\mathbb{Z}_p, +)$ es un grupo abeliano. Por tanto, hemos de fijarnos en $(\mathbb{Z}_p, \cdot)$. Además, las propiedades distributivas del producto con respecto a la suma también se verifican. Luego $\mathbb{Z}_p$ será un cuerpo si y solo si $(\mathbb{Z}_p \setminus \{[0]\}, \cdot)$ es un grupo. En definitiva, tendremos que ver si

$$\forall\, [m] \in \mathbb{Z}_p \setminus \{[0]\},\ \exists\, [m]^{-1} \text{ tal que } [m] \cdot [m]^{-1} = [m]^{-1} \cdot [m] = [1].$$

Para los casos $p = 2$ ó $p = 3$, podemos mirar las tablas que construimos y ver que, en el caso $p = 2$, como la única clase que tenemos distinta de la clase $[0]$ es $[1]$, $[1]^{-1} = [1]$ y podemos afirmar que, efectivamente, $(\mathbb{Z}_2, +, \cdot)$ es un cuerpo conmutativo.
En el caso $p = 3$, las únicas clases distintas de la clase $[0]$ son $[1]$ y $[2]$. Fijándonos en la tabla de la multiplicación para $\mathbb{Z}_3$, que reproducimos a continuación, comprobamos que $[1]^{-1} = [1]$ y, como $[2] \cdot [2] = [1]$, entonces $[2]^{-1} = [2]$.

$\cdot$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$
$[2]$	$[0]$	$[2]$	$[1]$

Por tanto, también $(\mathbb{Z}_3, +, \cdot)$ es un cuerpo conmutativo.
Veamos que el caso $p = 4$ es completamente distinto. $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$ y su tabla para la multiplicación es:

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

Como los elementos distintos de la clase $[0]$ son $[1], [2], [3]$, observamos que para $[1]$, en la fila que empieza con este elemento (2^{a} fila), aparece $[1]$, resultado de hacer $[1] \cdot [1]$. Por tanto, $[1]^{-1} = [1]$. Para $[3]$, de nuevo en la fila que empieza con $[3]$ (última fila), aparece $[1]$, resultado de hacer $[3] \cdot [3]$. Luego $[3]^{-1} = [3]$. Sin embargo, en la fila que empieza con $[2]$ (3^{a} fila), no aparece $[1]$. Esto nos dice que $\nexists\, [m]$, $m = 1, 2, 3$, tal que $[2] \cdot [m] = [1]$. Por tanto, no existe el inverso de $[2]$ y podemos afirmar que $(\mathbb{Z}_4, +, \cdot)$ no es un cuerpo.

Podéis comprobar que $(\mathbb{Z}_5, +, \cdot)$ y $(\mathbb{Z}_7, +, \cdot)$ son cuerpos conmutativos, pero que $(\mathbb{Z}_6, +, \cdot)$ no lo es. En este caso si hacéis el producto de $[2]$ por las diferentes clases obtenéis $[0], [2], [4], [0], [2]$ y $[4]$, y como no aparece $[1]$, concluid que $[2]$ no tiene inverso. Si repetís el proceso con $[3]$ se obtienen $[0], [3], [0], [3], [0]$ y

[3] y así, [3] tampoco tiene inverso.
¿Qué diferencia las situaciones que tenemos hasta ahora? Que 2, 3, 5 y 7 son números primos, mientras que 4 y 6 no lo son.
De hecho, tenemos que $(\mathbb{Z}_p, +, \cdot)$ es un cuerpo (conmutativo) si y solo si p es un número primo. Para ver esto, si $p \in \mathbb{N}$, $p > 1$ no es primo, entonces $\exists\, q, r \in \mathbb{N}$, $q, r \geq 2$, $q, r < p$ tales que $q \cdot r = p$. Por tanto en $\mathbb{Z}_p$, $[q], [r] \neq [0]$ y $[q] \cdot [r] = [p] = [0]$. Si suponemos que $\exists\, [q]^{-1}$, tendríamos de lo anterior que $[q]^{-1} \cdot ([q] \cdot [r]) = ([q^{-1}] \cdot [q]) \cdot [r] = [1] \cdot [r] = [1 \cdot r] = [r] = [q]^{-1} \cdot [0] = [0]$, en contradicción con lo que habíamos supuesto. Si suponemos que $\exists\, [r]^{-1}$, entonces $([q] \cdot [r]) \cdot [r]^{-1} = [q] \cdot ([r] \cdot [r]^{-1}) = [q] \cdot [1] = [q \cdot 1] = [q] = [0] \cdot [r]^{-1} = [0]$, y, por tanto $[r]$ tampoco admite inverso.
Si p es primo, construimos la tabla de $(\mathbb{Z}_p, \cdot)$ y comprobamos que, efectivamente, se verifica nuestra condición.

Introducimos ahora un nuevo conjunto numérico, el de los números complejos, que notaremos $\mathbb{C}$. Como sabemos la raíz cuadrada de un número real negativo no es un número real. Llamemos $i = \sqrt{-1}$ (no es un número real), de manera que $i^2 = -1$. Definimos, entonces

$$\mathbb{C} = \{a + bi \,/\, a, b \in \mathbb{R}\}.$$

A i la llamaremos unidad imaginaria, y dado $z \in \mathbb{C}$, z será de la forma $z = a + bi$, con $a, b \in \mathbb{R}$; a se llama la parte real de z, y lo notaremos $a = \mathrm{Re}(z)$[6], mientras que b se llama la parte imaginaria de z, $b = \mathrm{Im}(z)$[7]. Nótese que si $b = 0$, entonces $z = a$ es un número real. Luego $\mathbb{R} \subsetneq \mathbb{C}$. Vamos a introducir en $\mathbb{C}$ una suma $+$ y un producto $\cdot$ y comprobaremos que $(\mathbb{C}, +, \cdot)$ es un cuerpo conmutativo.
Dados $z_1 = a_1 + b_1 i$, $z_2 = a_2 + b_2 i$ números complejos, definimos $z_1 + z_2 = (a_1 + b_1 i) + (a_2 + b_2 i) := (a_1 + a_2) + (b_1 + b_2)i$[8]. Es decir, $\mathrm{Re}(z_1 + z_2) = \mathrm{Re}(z_1) + \mathrm{Re}(z_2)$ mientras que $\mathrm{Im}(z_1 + z_2) = \mathrm{Im}(z_1) + \mathrm{Im}(z_2)$.
Vamos a comprobar que $(\mathbb{C}, +)$ es un grupo abeliano:

1. Asociatividad: $((a_1 + b_1 i) + (a_2 + b_2 i)) + (a_3 + b_3 i) = ((a_1 + a_2) + (b_1 + b_2)i) + (a_3 + b_3 i) = ((a_1 + a_2) + a_3) + ((b_1 + b_2) + b_3)i$ y puesto que $(a_1 + a_3) + a_3$ y $(b_1 + b_2) + b3$ son sumas de 3 números reales y la suma de reales es asociativa entonces lo anterior es igual a $(a_1 + (a_2 + a_3)) + (b_1 + (b_2 + b_3))i$ que, por la definición de suma de números complejos es igual a $(a_1 + b_1 i) + ((a_2 + a_3) + (b_2 + b_3)i) = (a_1 + b_1 i) + ((a_2 + b_2 i) + (a_3 + b_3 i))$.

2. Conmutatividad: $(a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2)i \overset{(*)}{=} (a_2 + a_1) + (b_2 + b_1)i = (a_2 + b_2 i) + (a_1 + b_1 i)$, donde en $*$ hemos usado que a_1, a_2, b_1 y b_2 son números reales y por tanto $a_1 + a_2 = a_2 + a_1$ y $b_1 + b_2 = b_2 + b_1$.

3. Existencia de elemento neutro: consideremos el número complejo 0 tal que $\mathrm{Re}(0) = \mathrm{Im}(0) = 0 \in \mathbb{R}$. Es decir, $0 = 0 + 0i$. Veamos que este es el elemento neutro para $(\mathbb{C}, +)$. Como hemos visto que la suma de números complejos es conmutativa, basta con comprobar una de las dos igualdades. Así,

[6] También notado como $a = \Re(z)$.
[7] También notado como $b = \Im(z)$.
[8] Es habitual en matemáticas denotar las definiciones con el símbolo :=, como acabamos de ver.

$\forall\, z = a+bi \in \mathbb{C}$ se tiene $(a+bi)+0 = (a+bi)+(0+0i) = (a+0)+(b+0)i = a+bi$, pues $a+0=0$ y $b+0=0$, $\forall\, a, b \in \mathbb{R}$.

4. Existencia del opuesto de cada número complejo: sea $z = a+bi \in \mathbb{C}$. Llamaremos $-z = (-a)+(-b)i = -a-bi$. Entonces $z+(-z) = (a+bi)+((-a)+(-b)i) = (a+(-a)+(b+(-b))i) = 0+0i = 0$.

De este modo hemos comprobado que en efecto $(\mathbb{C}, +)$ es un grupo abeliano.
Ahora definiremos el producto de dos números complejos. Si $z_1 = a_1+b_1i$, $z_2 = a_2+b_2i$, donde $a_i, b_i \in \mathbb{R}$, $i = 1, 2$ entonces definimos el producto, $z_1 \cdot z_2$, como

$$z_1 \cdot z_2 = (a_1+b_1i)\cdot(a_2+b_2i) := (a_1a_2 - b_1b_2) + (a_1b_2 + b_1a_2)i.$$

Es decir, $\mathrm{Re}(z_1 \cdot z_2) = \mathrm{Re}(z_1)\,\mathrm{Re}(z_2) - \mathrm{Im}(z_1)\,\mathrm{Im}(z_2)$ e $\mathrm{Im}(z_1 \cdot z_2) = \mathrm{Re}(z_1)\,\mathrm{Im}(z_2) + \mathrm{Im}(z_1)\,\mathrm{Re}(z_2)$. Comprobemos las propiedades de este producto:

1. Es asociativo: sean $z_1 = a_1+b_1i$, $z_2 = a_2+b_2i$, $z_3 = a_3+b_3i$, $a_i, b_i \in \mathbb{R}$, $i \in \{1,2,3\}$. Entonces:

$$(z_1 \cdot z_2)\cdot z_3 = ((a_1a_2 - b_1b_2) + (a_1b_2 + b_1a_2)i)\cdot(a_3+b_3i) =$$

$$= ((a_1a_2 - b_1b_2)a_3 - (a_1b_2 + b_1a_2)b_3) + ((a_1a_2 - b_1b_2)b_3 + (a_1b_2 + b_1a_2)a_3)i =$$

$$= (a_1a_2a_3 - b_1b_2a_3 - a_1b_2b_3 - b_1a_2b_3) + (a_1a_2b_3 - b_1b_2b_3 + a_1b_2a_3 + b_1a_2a_3)i.$$

   Por otra parte,

$$z_1 \cdot (z_2 \cdot z_3) = (a_1+b_1i)\cdot((a_2+b_2i)\cdot(a_3+b_3i)) = (a_1+b_1i)\cdot((a_2a_3 - b_2b_3) + (a_2b_3 + b_2a_3)i) =$$

$$= (a_1(a_2a_3 - b_2b_3) - b_1(a_2b_3 + b_2a_3)) + (a_1(a_2b_3 + b_2a_3) + b_1(a_2a_3 - b_2b_3))i =$$

$$= (a_1a_2a_3 - a_1b_2b_3 - b_1a_2b_3 - b_1b_2a_3) + (a_1a_2b_3 + a_1b_2b_3 + b_1a_2a_3 - b_1b_2b_3)i.$$

   Podéis comprobar que tanto las partes reales como las partes imaginarias de ambos números complejos coinciden de modo que $z_1 \cdot (z_2 \cdot z_3) = (z_1 \cdot z_2)\cdot z_3$.

2. Es conmutativo: si $z_1 = a_1+b_1i$ y $z_2 = a_2+b_2i$ son números complejos entonces $z_1 \cdot z_2 = (a_1a_2 - b_1b_2) + (a_1b_2 + b_1a_2)i = (a_2a_1 - b_2b_1) + (a_2b_1 + b_2a_1)i = (a_2+b_2i)\cdot(a_1+b_1i) = z_2 \cdot z_1$.

3. Existencia de elemento neutro: $\exists$ el número complejo $1 = 1+0i$ (en realidad sería el número real 1) tal que $\forall\, a+bi \in \mathbb{C}$ se verifica $1\cdot(a+bi) = (1+0i)\cdot(a+bi) = (1\cdot a + 0\cdot 0) + (1\cdot b + 0\cdot a)i = a+bi$ (como hemos visto que el producto es conmutativo no necesitamos comprobar la segunda igualdad).

4. Existencia de inversos para cada número complejo distinto de 0: en primer lugar $z \in \mathbb{C}$ será distinto de cero ($z \neq 0$) si $\mathrm{Re}(z) \neq 0$ ó $\mathrm{Im}(z) \neq 0$. Dado cualquier $z = a+bi \in \mathbb{C}$, definimos su conjugado y lo denotamos por $\overline{z}$ a $\overline{z} = a-bi$. Es decir, $\mathrm{Re}(\overline{z}) = \mathrm{Re}(z)$, pero $\mathrm{Im}(\overline{z}) = -\,\mathrm{Im}(z)$. Así, $\overline{z} \in \mathbb{C}$ y se verifica que $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$ puesto que

$$\overline{(a_1+b_1i)+(a_2+b_2i)} = \overline{(a_1+a_2)+(b_1+b_2)i} = (a_1+a_2) - (b_1+b_2)i =$$

$$= (a_1 + a_2) + (-b_1 - b_2)i = (a_1 - b_1 i) + (a_2 - b_2)i = \overline{z_1} + \overline{z_2}.$$

Análogamente podemos ver que $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$:

$$\overline{(a_1 + b_1 i) \cdot (a_2 + b_2 i)} = \overline{(a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2)i} = (a_1 a_2 - b_1 b_2) - (a_1 b_2 + b_1 a_2)i,$$

por otro lado:

$$\overline{z_1} \cdot \overline{z_2} = (a_1 - b_1 i) \cdot (a_2 - b_2 i) = (a_1 a_2 - b_1 b_2) + (a_1(-b_2) + (-b_1 a_2))i = (a_1 a_2 - b_1 b_2) - (a_1 b_2 + b_1 a_2)i,$$

obteniendo lo mismo.

Sea ahora $z = a + bi \in \mathbb{C} \setminus \{0\}$. Fijaos, entonces, que al menos uno entre a y b es no nulo. Tenemos que $z \cdot \overline{z} = \overline{z} \cdot z = (a + bi) \cdot (a - bi) = a^2 + b^2 + (-ab + ba)i = a^2 + b^2$ y como $a, b \in \mathbb{R}$ entonces $a^2 + b^2 \in \mathbb{R}$ y siendo, al menos, $a \neq 0$ ó $b \neq 0$, se tiene $a^2 + b^2 > 0$. Podemos considerar entonces el número complejo

$$\frac{1}{a^2 + b^2} \cdot \overline{z} = \frac{1}{a^2 + b^2}(a - bi) = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i.$$

Así,

$$z \cdot \left(\frac{1}{a^2 + b^2} \cdot \overline{z} \right) = (a + bi) \left(\frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i \right) = \left(\frac{a^2}{a^2 + b^2} + \frac{b^2}{a^2 + b^2} \right) + \left(-\frac{ab}{a^2 + b^2} + \frac{ab}{a^2 + b^2} \right) i =$$

$$= \frac{a^2 + b^2}{a^2 + b^2} + 0 \cdot i = 1 + 0 \cdot i = 1.$$

Por tanto, si $z \in \mathbb{C} \setminus \{0\}$, hemos visto que $z^{-1} = \frac{1}{a^2 + b^2} \cdot \overline{z}$ (como el producto en $\mathbb{C}$ es conmutativo la otra igualdad también es cierta). El producto de $z \cdot \overline{z}$ se llama el módulo de z y, como hemos visto, siempre es un número real ≥ 0.

Para completar la demostración de que $(\mathbb{C}, +, \cdot)$ es un cuerpo conmutativo hemos de demostrar las propiedades distributivas del producto con respecto de la suma. Como ya sabemos que el producto es conmutativo, basta con ver que una de ellas es cierta. Sean entonces $z_1 = a_1 + b_1 i$, $z_2 = a_2 + b_2 i$, $z_3 = a_3 + b_3 i$, $z_1, z_2, z_3 \in \mathbb{C}$. Se tiene:

$$(z_1 + z_2) \cdot z_3 = ((a_1 + b_1 i) + (a_2 + b_2 i)) \cdot (a_3 + b_3 i) = ((a_1 + a_2) + (b_1 + b_2)i) \cdot (a_3 + b_3 i) =$$

$$= ((a_1 + a_2)b_3 - (b_1 + b_2)b_3) + ((a_1 + a_2)b_3 + (b_1 + b_2)a_3)i = (a_1 a_3 + a_2 a_3 - b_1 b_3 - b_2 b_3) + (a_1 b_3 + a_2 b_3 - b_1 a_3 - b_2 a_3)i.$$

Por otro lado,

$$z_1 \cdot z_3 + z_2 \cdot z_3 = (a_1 + b_1 i) \cdot (a_3 + b_3 i) + (a_2 + b_2 i) \cdot (a_3 + b_3 i) =$$

$$= ((a_1 a_3 - b_1 b_3) + (a_1 b_3 + b_1 a_3) + (a_1 b_3 + b_1 a_3)i) + ((a_2 a_3 - b_2 b_3) + (a_2 b_3 + b_2 a_3)i) =$$

$$= (a_1 a_3 - b_1 b_3 + a_2 a_3 - b_2 b_3) + (a_1 b_3 + b_1 a_3 + a_2 b_3 + b_2 a_3)i.$$

Es inmediato ver que las partes reales y las partes imaginarias de ambos números complejos coinciden y, por tanto, acabamos de comprobar que $(\mathbb{C}, +, \cdot)$ es un cuerpo conmutativo.

A partir de ahora, y en los temas siguientes, aunque demos las definiciones para un cuerpo cualquiera, trabajaremos con los cuerpos de los números reales $\mathbb{R}$ ó de los números complejos $\mathbb{C}$.
Todos los cuerpos que hemos introducido hasta ahora han resultado ser conmutativos. Podríamos pensar que cualquier cuerpo que consideremos ha de ser conmutativo. Esto no es cierto. Vamos a introducir someramente un cuerpo que no es conmutativo:
Consideremos

$$\mathbb{H} = \left\{a + bi + cj + dk \,/\, a, b, c, d \in \mathbb{R},\ i^2 = j^2 = k^2 = -1,\ ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j\right\}.$$

A cada uno de estos elementos $a + bi + cj + dk$ lo llamaremos un cuaternión y, así, $\mathbb{H}$ es el conjunto de los cuaterniones (lo notamos con una $\mathbb{H}$ porque fueron introducidos por el matemático británico William Rowan Hamilton (1805-1865)). Fijaos que si $b = c = d = 0$ entonces $a \in \mathbb{R}$ y, por tanto, $\mathbb{R} \subsetneq \mathbb{H}$. Asimismo, si $c = d = 0$ entonces $a + bi \in \mathbb{C}$, luego $\mathbb{C} \subsetneq \mathbb{H}$. Si tomamos $w = a + bi + cj + dk$, a se llama la parte real de w y $bi + cj + dk$ se llama su parte imaginaria. Llamaremos 0 al cuaternión $0 + 0i + 0j + 0k$ (es en realidad el 0 real) y 1 al cuaternión $1 + 0i + 0j + 0k$ (es el 1 real). Además, si $w = a + bi + cj + dk$, llamaremos el conjugado cuaterniónico de w a $\overline{w} = a - bi - cj - dk$.
Queremos introducir una suma y un producto en $\mathbb{H}$ de manera que $(\mathbb{H}, +, \cdot)$ sea un cuerpo. Para ello, dados $w_1 = a_1 + b_1 i + c_1 j + d_1 k$, $w_2 = a_2 + b_2 i + c_2 j + d_2 k$, donde $a_i, b_i, c_i, d_i \in \mathbb{R}$, $\forall\, i \in \{1, 2\}$, definimos la suma de w_1 y w_2 como:

$$w_1 + w_2 := (a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k.$$

Es decir, en cada componente para la parte real, para i, para j y para k sumamos las correspondientes componentes de w_1 y w_2. Es inmediato comprobar (similarmente al caso de $\mathbb{C}$) que $(\mathbb{H}, +)$ es un grupo abeliano cuyo elemento neutro es el cuaternión 0 y tal que si $w = a + bi + cj + dk$ entonces $-w = -a - bi - cj - dk$.
Por otro lado, queremos que el producto de dos cuaterniones preserve el hecho de que $i^2 = j^2 = j^2 = -1$ y que $ij = -ji = k$, $jk = -kj = i$ y $ki = -ik = j$. Así, dados w_1 y w_2 como antes se define el producto, $w_1 \cdot w_2$, como:

$$w_1 \cdot w_2 = (a_1 + b_1 i + c_1 j + d_1 k) \cdot (a_2 + b_2 i + c_2 j + d_2 k) :=$$

$$= (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) + (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)i + (a_1c_2 + c_1a_2 - b_1d_2 + d_1b_2)j + (a_1d_2 + d_1a_2 - b_1c_2 + c_1b_2)k.$$

Este producto generaliza el hecho de que $ij = -ji = k$, etc. (su comprobación se deja como **ejercicio**) luego podemos afirmar que no es conmutativo.
Sí tenemos que 1 es el elemento neutro. En efecto:

$$1 \cdot (a_1 + b_1 i + c_1 j + d_1 k) = (1 + 0i + 0j + 0k) \cdot (a_1 + b_1 i + c_1 j + d_1 k) =$$

$$= (1 \cdot a_1 - 0 \cdot b_1 - 0 \cdot c_1 - 0 \cdot d_1) + (1 \cdot b_1 + 0 \cdot a_1 + 0 \cdot d_1 - 0 \cdot c_1)i + (1 \cdot c_1 + 0 \cdot a_1 - 0 \cdot d_1 + 0 \cdot b_1)j + (1 \cdot d_1 + 0 \cdot a_1 + 0 \cdot c_1 - 0 \cdot b_1)k =$$

$$= a_1 + b_1 i + c_1 j + d_1 k,$$

y, la otra igualdad (ahora sí es necesario comprobarla al no tener la propiedad conmutativa) sale de forma similar.

Queda, por tanto, ver que se verifican las propiedades asociativa y las propiedades distributivas del producto con respecto a la suma (son fáciles, aunque tediosas en cuanto a notación, y se dejan como **ejercicio**) y la existencia de inverso para cada cuaternión no nulo. Para ello, dado $w = a_1+b_1i+c_1j+d_1k$, consideramos su conjugado cuaterniónico $\overline{w}$. Es inmediato comprobar que $\overline{w_1 + w_2} = \overline{w_1} + \overline{w_2}$, $\forall\, w_1, w_2 \in \mathbb{H}$. Además, si $w_1 = a_1 + b_1i + c_1j + d_1k$ y $w_2 = a_2 + b_2i + c_2j + d_2k$ entonces:

$$\overline{w_1 \cdot w_2} = \overline{(a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) + (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)i+}$$

$$\overline{+(a_1c_2 + c_1a_2 - b_1d_2 + d_1b_2)j + (a_1d_2 + d_1a_2 - b_1c_2 + c_1b_2)k} =$$

$$= a_1a_2-b_1b_2-c_1c_2-d_1d_2-(a_1b_2+b_1a_2+c_1d_2-d_1c_2)i-(a_1c_2+c_1a_2-b_1d_2+d_1b_2)j-(a_1d_2+d_1a_2-b_1c_2+c_1b_2)k.$$

Por otro lado,

$$\overline{w_2} \cdot \overline{w_1} = (a_2 - b_2i - c_2j - d_2k) \cdot (a_1 - b_1i - c_1j - d_1k) =$$

$$= a_2a_1 - b_2b_1 - c_2c_1 - d_2d_1 + (-a_2b_1 - b_2a_2 + c_2d_1 - d_2c_1)i + (-a_2c_1 - c_2a_1 - b_2d_1 + d_2b_1)j+$$

$$+(-a_2d_1 - d_2a_1 - b_2c_1 + c_2b_1)k.$$

Luego ahora tenemos $\overline{w_1 \cdot w_2} = \overline{w_2} \cdot \overline{w_1}$. Si $w = a + bi + cj + dk \neq 0$, ó bien a ó b ó c ó d han de ser números reales no nulos. Si ahora hacemos

$$w \cdot \overline{w} = (a + bi + cj + dk) \cdot (a - bi - cj - dk) =$$

$$= (a^2 + b^2 + c^2 + d^2) + (-ab + ba - cd + dc)i + (-ac + ca - bd + db)j + (-ad + da + bc - cb)k =$$

$$= a^2 + b^2 + c^2 + d^2,$$

es un número real y si $w \neq 0$, entonces $w \cdot \overline{w} > 0$. Por tanto, si para cada $w \neq 0$ tomamos $w^{-1} = \frac{1}{w \cdot \overline{w}} \cdot \overline{w} = \frac{a}{a^2+b^2+c^2+d^2} - \frac{b}{a^2+b^2+c^2+d^2}i - \frac{c}{a^2+b^2+c^2+d^2}j - \frac{d}{a^2+b^2+c^2+d^2}k$, tendremos:

$$w \cdot w^{-1} = \left(\frac{a^2}{a^2 + b^2 + c^2 + d^2} + \frac{b^2}{a^2 + b^2 + c^2 + d^2} + \frac{c^2}{a^2 + b^2 + c^2 + d^2} + \frac{d^2}{a^2 + b^2 + c^2 + d^2}\right) +$$

$$+ \left(\frac{-ab}{a^2 + b^2 + c^2 + d^2} + \frac{ba}{a^2 + b^2 + c^2 + d^2} - \frac{cd}{a^2 + b^2 + c^2 + d^2} + \frac{dc}{a^2 + b^2 + c^2 + d^2}\right) i+$$

$$+ \left(-\frac{ac}{a^2 + b^2 + c^2 + d^2} + \frac{ca}{a^2 + b^2 + c^2 + d^2} + \frac{bd}{a^2 + b^2 + c^2 + d^2} - \frac{db}{a^2 + b^2 + c^2 + d^2}\right) j+$$

$$+ \left(-\frac{ad}{a^2 + b^2 + c^2 + d^2} + \frac{da}{a^2 + b^2 + c^2 + d^2} - \frac{bc}{a^2 + b^2 + c^2 + d^2} + \frac{cb}{a^2 + b^2 + c^2 + d^2}\right) k =$$

$$= \frac{a^2 + b^2 + c^2 + d^2}{a^2 + b^2 + c^2 + d^2} = 1.$$

Análogamente se obtiene que $w^{-1} \cdot w = 1$ y esto concluye la comprobación de que $(\mathbb{H}, +, \cdot)$ es un cuerpo no conmutativo.