Álgebra Lineal y Geometría I

Grado de Física – UGR

Curso 2019-20

TEMA 0

Ignacio Sánchez Rodríguez

TEMA 0

El lenguaje matemático

1. Definiciones y teoremas

Los enunciados: Una materia de matemáticas se organiza principalmente con definiciones y teoremas. La *definición* de un objeto es un enunciado que nos dice lo que ese objeto es, a partir de objetos previamente conocidos. Un *teorema* o *proposición* es el enunciado de un resultado nuevo sobre objetos ya definidos. La *demostración* de un teorema es la prueba clara de la veracidad de ese resultado; la demostración se obtiene a partir de otros enunciados verdaderos previamente conocidos.

La palabra "teorema" se suele reservar para las proposiciones más importantes. También se usan los términos *lema*, que designa una proposición que se utilizará en la demostración de alguna proposición posterior, y *corolario*, que designa una proposición cuya demostración es inmediata a partir de una proposición precedente.

La igualdad: Una *igualdad* es un enunciado en el que se afirma que dos expresiones diferentes definen o representan el mismo objeto matemático. Si tenemos dos expresiones, S y T, que representan el mismo objeto, decimos que S *es igual a* T y se escribe entre ellas el *signo de la igualdad*

$$S = T.$$

Diremos que S es el *primer término* de la igualdad y T es el *segundo término* de la igualdad. Si S no es igual a T escribimos: $S \neq T$.

En el caso en que la igualdad sea la definición de lo que el objeto S es, decimos que es una *igualdad por definición* y, opcionalmente, podemos escribir

$$S := T.$$

En el caso en que la igualdad sirva para indicar que S y T son dos notaciones equivalentes para representar al mismo objeto, decimos que es una *igualdad por notación* y, opcionalmente, podemos escribir

$$S \equiv T.$$

Conjunción, disyunción y negación: En general, los enunciados interesantes de las matemáticas son los que nos permiten saber de ellos si son verdaderos o falsos. Veamos algunas formas de construir nuevos enunciados.

Si p y q son dos enunciados, la *conjunción*

$$p \text{ y } q \quad \text{(a veces se escribe: } p \wedge q\text{)}$$

es un enunciado que es verdadero solamente si ambos son verdaderos.

Si p y q son dos enunciados, la *disyunción*

$$p \text{ o } q \quad \text{(a veces se escribe: } p \vee q\text{)}$$

es un enunciado que es verdadero si uno de ellos es verdadero o ambos son verdaderos.

Si p es un enunciado, la *negación*

$$\text{no } p \quad \text{(a veces se escribe: } \neg p\text{)}$$

es otro enunciado que es verdadero solamente si el enunciado p es falso.

Implicación: Dados los enunciados p y q, se puede construir el nuevo enunciado "p *implica* q", que se escribe:

$$p \implies q\,,$$

y que significa que "si p es verdadero entonces q es verdadero" (en cambio, si "$p \implies q$" es verdadero y p es falso entonces... ¡no podemos deducir que q sea verdadero o falso!).

La verdad del enunciado "*p implica q*" nos lleva a deducir que si q es falso entonces p también es falso. Por tanto, la implicación $p \implies q$ es equivalente al enunciado:

$$\text{no } q \implies \text{no } p$$

Dados los enunciados p y q, también se construye el enunciado "*p si y sólo si q*", que es la conjunción de los enunciados "p implica q" y "q implica p". Se le llama la *doble implicación* y se denota por:

$$p \iff q\,.$$

Significa, simultáneamente, que si p es verdadero entonces q es verdadero y que si q es verdadero entonces p es verdadero. La expresión "*p si y sólo si q*" también se puede leer como "p es *necesario y suficiente* para q".

Cuantificadores: Los *cuantificadores* son ciertas expresiones relativas a la cantidad. Vienen representados por un símbolo y se utilizan para construir nuevos enunciados. Principalmente son dos y, en el lenguaje matemático, su significado es inequívoco:

- El cuantificador "*para todo*", denotado con el símbolo $\forall$. La expresión:

  $$\forall\, a$$

  significa "para todo a", "para cualquier a" o "para cada a".
- El cuantificador "*existe*", denotado con el símbolo $\exists$. La expresión:

  $$\exists\, a$$

  significa "existe un a" o "existe al menos un a". A veces también se utiliza $\exists\,!\, a$ para expresar que "existe un a y es único".

Dos enunciados elementales formados con cuantificadores son los siguientes:

- "Para cada a, existe un b tal que se verifica... "; o escrito simbólicamente:

  $$\forall\, a, \exists\, b \textit{ tal que } \ldots$$

  Significa que, para cada a elegido, puedo encontrar un b verificando lo que se afirme a continuación (¡para diferentes elecciones de a los correspondientes b pueden ser diferentes!).

- "Existe a tal que para todo b se verifica... "; o escrito simbólicamente:

$$\exists\, a \ \textit{tal que}\ \forall\, b \ \ldots$$

Significa que puedo encontrar un a de tal manera que, cualquiera que sea b, se verifica lo que se afirme a continuación (¡no vale cambiar de a según sea el b! Encontrado el a, el enunciado que siga debe ser cierto para todo b).

Ejercicios 1.

1. (a) Considera los siguientes cuatro enunciados:
   1: p y $(q$ o $r)$ 2: p o $(q$ y $r)$ 3: $(p$ y $r)$ o $(q$ y $r)$ 4: $(p$ o $r)$ y $(q$ o $r)$
   ¿Cuáles son equivalentes?
   (b) Expresa la negación del enunciado "p y q" en términos de los enunciados "no p" y "no q". Lo mismo para la negación del enunciado "p o q".
2. Sean p el enunciado "x es mayor que 0" y q el enunciado "y es mayor que 0". Dibuja en el plano usual de coordenadas XY, las regiones que corresponden a los enunciados "p y q", "p o q" y a las negaciones de ambos.
3. Un teorema que afirma que "p implica q" se demuestra si se prueba que "(no q) implica (no p)". Demostrar así la proposición que dice: "Si un número natural es primo y mayor que 2 entonces es un número natural impar".
4. Para demostrar la *doble implicación*, $p \iff q$, hay que demostrar dos implicaciones: (i) $p \implies q$ y (ii) $q \implies p$. Probar así la siguiente proposición: Sea m un número natural. Se verifica que "m es par" si y sólo si "m^2 es par".
5. (a) Hacer una frase del lenguaje ordinario, con sentido, que contenga un enunciado del tipo "una cosa o la otra", y cuyo significado no sea "o una cosa o la otra, pero no las dos".
   (b) Escribe una frase que sea la negación del enunciado "En cualquier árbol de ese bosque, existe una rama que no tiene hojas". Igualmente, construir la negación de "En aquella isla existe un ave tal que todas sus plumas son blancas".

2. Conjuntos

Elementos y conjuntos: Las nociones de elemento y de conjunto no se definen; se apela a la intuición, entendiéndose que un conjunto es algo que tiene elementos y un elemento es algo que está en un conjunto. Lo que sí se pide en matemáticas es que cualquier conjunto que consideremos esté "bien definido"; esto quiere decir que, para cualquier objeto dado, podemos saber si es un elemento del conjunto considerado o no lo es.

Una manera elemental de representar un conjunto, que llamaremos *representación explícita* del conjunto, es encerrando entre llaves los elementos que tiene y separando éstos por comas; por ejemplo, $C = \{1, 2, 3\}$. Cuando un elemento b está en un conjunto C, decimos que b *pertenece* a C y se representa por

$$b \in C.$$

Se postula, por convenio, la existencia de un único conjunto, llamado *conjunto vacío* y denotado por $\varnothing$, caracterizado por no tener ningún elemento.

Si C y D son dos conjuntos, se construye un nuevo conjunto llamado la *unión* de C y D, denotado por

$$C \cup D,$$

que está definido por

$$a \in C \cup D \quad \text{si y sólo si} \quad a \in C \ \text{ o } \ a \in D.$$

También se construye un nuevo conjunto, llamado la *intersección* de C y D y denotado por

$$C \cap D,$$

que está definido por

$$a \in C \cap D \quad \text{si y sólo si} \quad a \in C \ \text{ y } \ a \in D.$$

Decimos que C y D son *disjuntos* si $C \cap D = \varnothing$.

Por último, llamamos la *diferencia* de C y D (o el *complementario* de D en C), y lo denotamos por

$$C - D \ \ (\text{o por } C \setminus D),$$

al conjunto definido por

$$a \in C - D \equiv C \setminus D \quad \text{si y sólo si} \quad a \in C \ \text{ y } \ a \notin D.$$

Conjunto producto: Dados dos elementos a y b, se define un nuevo objeto llamado el *par ordenado* (a, b) (¡no se debe confundir con el conjunto con dos elementos $\{a, b\}$!). Por definición, dos pares ordenados (a, b) y (a', b') son iguales si y sólo si $a = a'$ y $b = b'$.

Si C y D son dos conjuntos, se construye un nuevo conjunto llamado el *conjunto producto* o *producto cartesiano* de C y D, denotado por $C \times D$, cuyos elementos son pares ordenados, y está definido por

$$(a, b) \in C \times D \quad \text{si y sólo si} \quad a \in C \ \text{ y } \ b \in D.$$

NOTA: Cuando decimos "$a, b \in C$", se entiende "$a \in C$ y $b \in C$"; y no debemos suponer que a y b son dos elementos distintos, a no ser que se diga $a \neq b$.

Subconjuntos: Si C y D son dos conjuntos, decimos que D está *incluido* en C, denotado por $D \subset C$, cuando todos los elementos de D son elementos de C; esto es, D está incluido en C, si se verifica que:

$$\text{si} \quad a \in D \quad \text{entonces} \quad a \in C \qquad (a \in D \Longrightarrow a \in C)$$

En este caso, decimos que D es un *subconjunto* de C.

Una manera típica de definir un subconjunto es caracterizarlo por una propiedad que han de verificar sus elementos; por ejemplo, el conjunto P de los numeros pares es un subconjunto de los números naturales $\mathbb{N}$, y podemos escribir:

$$P = \{x \in \mathbb{N} : \tfrac{x}{2} \in \mathbb{N}\}$$

que se lee así: "P es el conjunto formado por los x pertenecientes a $\mathbb{N}$ que verifican que $\frac{x}{2}$ pertenece a $\mathbb{N}$". El símbolo "$:$" en la expresión anterior, cuyo significado es "que verifican que" o "tales que", a veces se escribe con el símbolo "$/$".

Partes de un conjunto: Si C es un conjunto, se construye un nuevo conjunto llamado *partes de* C, y denotado por $\mathcal{P}(C)$, que es aquel cuyos elementos son los posibles subconjuntos de C, es decir:

$$D \in \mathcal{P}(C) \quad \text{si y sólo si} \quad D \subset C$$

Por definición de subconjunto, todo conjunto es subconjunto de sí mismo; por tanto, $C \in \mathcal{P}(C)$. Por convenio, el conjunto vacío es subconjunto de cualquier conjunto; y por tanto, $\varnothing \in \mathcal{P}(C)$. También por convenio, un conjunto no puede ser elemento de sí mismo.

Ejercicios 2.

1. Dos conjuntos son iguales si tienen los mismos elementos. Para demostrar la igualdad entre conjuntos, $C = D$, hay que probar dos cosas: (i) $C \subset D$ y (ii) $D \subset C$. Ahora, en el producto cartesiano del conjunto de los números reales, $\mathbb{R}$, por sí mismo, $\mathbb{R}^2 \equiv \mathbb{R} \times \mathbb{R}$, consideremos los subconjuntos:

$$C = \{(x, y) \in \mathbb{R}^2 \colon xy = 0\}$$
$$D = \big(\{0\} \times \mathbb{R}\big) \cup \big(\mathbb{R} \times \{0\}\big)$$

   Probar que $C = D$.
2. Sean D y E dos subconjuntos de C. Probar que

$$C \setminus (D \cap E) = (C \setminus D) \cup (C \setminus E)$$
$$C \setminus (D \cup E) = (C \setminus D) \cap (C \setminus E)$$

3. Supongamos que, para cada $i \in \mathbb{N}$, tenemos un conjunto C_i. La unión de todos los C_i se denota por $\bigcup_{i\in\mathbb{N}} C_i$ y la intersección de todos los C_i se denota por $\bigcap_{i\in\mathbb{N}} C_i$. Ahora, trata de dar las definiciones de la unión y de la intersección de todos los C_i; es decir completa estos dos enunciados (usando cuantificadores):

$$a \in \bigcup_{i\in\mathbb{N}} C_i \qquad \text{si y sólo si} \quad \dots \dots \dots$$
$$a \in \bigcap_{i\in\mathbb{N}} C_i \qquad \text{si y sólo si} \quad \dots \dots \dots$$

4. Para cada $i \in \mathbb{N}$, sea $C_i = \{x \in \mathbb{R} \colon x \geq i\}$. Escribe qué conjuntos serían la unión y la intersección de todos los C_i; es decir completa los puntos suspensivos de estos

dos conjuntos:

$$\bigcup_{i\in\mathbb{N}} C_i = \{x \in \mathbb{R}\colon \dots \dots \dots\}$$

$$\bigcap_{i\in\mathbb{N}} C_i = \{x \in \mathbb{R}\colon \dots \dots \dots\}$$

(¡trata de hacerlo intuitivamente, aunque no hayas resuelto el ejercicio anterior!)

5. Sea $C = \{1\}$, el conjunto que sólo tiene el elemento 1. Escribe la representación explícita de $\mathcal{P}(C)$. Haz lo mismo para $\mathcal{P}(D)$, siendo $D = \{C\}$. Halla la unión y la intersección de los conjuntos $\mathcal{P}(C)$ y $\mathcal{P}(D)$.

6. Vuelve a leer el último párrafo de ésta sección: ¿Entiendes ese párrafo? Trata de expresar por escrito: (a) por qué se dice "Por definición de subconjunto, todo conjunto es subconjunto de sí mismo"; y (b) por qué crees que *no se dice*: "Por definición de subconjunto, el conjunto vacío es subconjunto de cualquier conjunto". Investiga en internet porqué no se admite que un conjunto pueda ser elemento de sí mismo.

3. Aplicaciones

Definición: Dados dos conjuntos C y D, una *aplicación* o *función*, f, de C en D es una manera de asignar a cada elemento a de C un único elemento de D, denotado por $f(a)$ y llamado la *imagen* de a (por la aplicación f).

Una aplicación se describe por el diagrama

$$f\colon C \longrightarrow D, \qquad a \longmapsto f(a)$$

Al conjunto C se le llama *conjunto inicial* o *dominio* de f y al conjunto D se le llama *conjunto final* o *codominio* de f.

Una aplicación suele venir descrita por una regla que nos dice cómo obtener la imagen de cualquier elemento del conjunto inicial; por ejemplo, $f(x) = x^2 - 3$ (¡pero, en matemáticas, siempre hay que fijar, además, cuál es el conjunto inicial y cuál es el conjunto final para tener bien definida la aplicación!).

De frecuente uso son las siguientes definiciones:

Aplicación inyectiva: Una aplicación $f\colon C \to D$ es *inyectiva* si ningún elemento de D es la imagen de dos elementos distintos de C, es decir,

$$\text{si } \ a, a' \in C \ \text{ y } \ f(a) = f(a') \ \text{ entonces } \ a = a'$$

Aplicación sobreyectiva: Una aplicación $f\colon C \to D$ es *sobreyectiva* si cada elemento de D es la imagen de algún elemento de C, es decir,

$$\forall\, b \in D, \ \text{ se verifica que } \ \exists\, a \in C \ \text{ tal que } \ f(a) = b$$

Aplicación biyectiva: Una aplicación $f\colon C \to D$ es *biyectiva* si es inyectiva y sobreyectiva.

Si $f\colon C \to D$ es una aplicación biyectiva entonces existe la llamada aplicación *inversa* de f de D en C, denotada por $f^{-1}\colon D \to C$, definida por

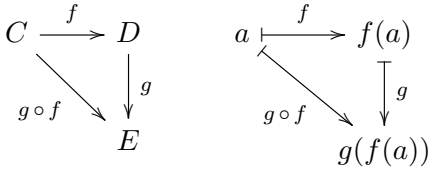
$$\text{si } \quad f(a) = b \ \text{ entonces } \quad f^{-1}(b) = a$$

Composición de aplicaciones: Sean $f\colon C \to D \quad$ y $\quad g\colon D \to E$ dos aplicaciones tales que el conjunto final de la primera coincide con el conjunto inicial de la segunda. Entonces podemos construir una nueva función de C en E, llamada la

composición de las aplicaciones f y g, que se denota por $g \circ f$ y se lee "f *compuesta de* g", y que está definida por

$$(g \circ f)(a) := g(f(a)), \quad \forall\, a \in C$$

La situación está reflejada en el siguiente diagrama:



Aplicación Identidad: Sea C un conjunto. Llamamos *aplicación identidad* de C a la aplicación $\mathrm{id}_C \colon C \to C$, definida por $\mathrm{id}_C(a) = a, \quad \forall\, a \in C$.

La siguiente proposición se puede usar para asegurar que una aplicación es biyectiva.

Proposición: Sea $f \colon C \to D$ una aplicación. Si existe otra aplicación $g \colon D \to C$ tal que $g \circ f = \mathrm{id}_C$ y $f \circ g = \mathrm{id}_D$ entonces f es biyectiva y $f^{-1} = g$.

Ejercicios 3.

1. Sean $f : C \to D$ una aplicación y $G \subset C$. Definimos la *imagen de* G por f, denotada por $f(G)$:

$$f(G) := \{y \in D \colon \exists\, x \in G \text{ tal que } f(x) = y\} = \{f(x) \colon x \in G\}$$

Llamamos *imagen de* f al subconjunto $f(C)$; se denota también por $\mathrm{im}\, f \equiv f(C)$. Probar que decir que f es sobreyectiva es equivalente a decir que $\mathrm{im}\, f = D$.

2. Sean $f : C \to D$ una aplicación y $H \subset D$. Definimos la *imagen inversa de* H por f, denotada por $f^{-1}(H)$ (¡no confundir con la aplicación inversa f^{-1} que se aplica a elementos de D, y que sólo existe si f es biyectiva!):

$$f^{-1}(H) := \{x \in C \colon f(x) \in H\}$$

Razonar si es verdadero o falso el siguiente enunciado:

Existe una aplicación $f : C \to D$ tal que $f^{-1}(D) \neq C$.

3. Dados $a, b \in \mathbb{R}$, con $a < b$, se llama *intervalo abierto*, $]a, b[$ —también denotado por (a, b)—, al subconjunto de $\mathbb{R}$ dado por $]a, b[:= \{x \in \mathbb{R} \colon a < x < b\}$. Ahora, si f es la aplicación del producto cartesiano $\mathbb{R} \times \mathbb{R} \equiv \mathbb{R}^2$ en $\mathbb{R}$, dada por

$$f \colon \mathbb{R}^2 \longrightarrow \mathbb{R}, \qquad f(x, y) = x + y\,,$$

hallad la imagen por la aplicación f del producto cartesiano de intervalos abiertos $]-1, 3[\ \times \ ]-2, 2[$. Hallar la imagen inversa por f de los números positivos.

4. Construir la negación de los enunciados que definen lo que es una aplicación inyectiva y lo que es una aplicación sobreyectiva.

5. Probar que la función

$$\begin{array}{rcl} f \colon \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & 3x + 4 \end{array}$$

es biyectiva. Calcular la función inversa de f.

6. Hallar $f \circ g$ y $g \circ f$ siendo

$$\begin{array}{ll} f \colon \mathbb{R}^2 \to \mathbb{R} & (x, y) \longmapsto 2x - 3y \\ g \colon \mathbb{R} \to \mathbb{R}^2 & x \longmapsto (2x^2, x + 3) \end{array}$$

4. Relaciones

Relación en un conjunto: Una *relación* $\mathcal{R}$ en un conjunto C se define como un subconjunto del conjunto producto $C \times C$, verificando ciertas propiedades que especifican el tipo de relación. Si $\mathcal{R} \subset C \times C$ es una relación y si $(a, b) \in \mathcal{R}$, decimos que a está $\mathcal{R}$*–relacionado* con b, y escribimos $a\mathcal{R}b$.

Relación de equivalencia: Una *relación de equivalencia* $\mathcal{R}$ en un conjunto C es una relación en C que verifica las propiedades siguientes:

1. Propiedad *reflexiva*: $\forall\, a \in C, \quad a\mathcal{R}a$.
2. Propiedad *simétrica*: Si $a, b \in C$ y $a\mathcal{R}b$ entonces $b\mathcal{R}a$.
3. Propiedad *transitiva*: Si $a, b, c \in C$, $a\mathcal{R}b$ y $b\mathcal{R}c$ entonces $a\mathcal{R}c$.

Dado $a \in C$, el subconjunto de C formado por todos los elementos que están $\mathcal{R}$–relacionados con a se dice que es una *clase de equivalencia* para la relación de equivalencia $\mathcal{R}$; en ese caso, se dice que a es un *representante* de esa clase de equivalencia. Una clase de equivalencia para $\mathcal{R}$, con representante a, la denotaremos por $[a]_{\mathcal{R}}$ o, simplemente, por $[a]$, si no hay confusión posible.

El conjunto cuyos elementos son las clases de equivalencia para $\mathcal{R}$ es el llamado *conjunto cociente* de $\mathcal{R}$, y se denota por $C/\mathcal{R}$, leído "C *sobre* $\mathcal{R}$" o "C *cociente* $\mathcal{R}$". Obviamente, $C/\mathcal{R}$ es un subconjunto de $\mathcal{P}(C)$ y tiene las siguientes propiedades:

(a) La unión de los subconjuntos de C que son elementos de $C/\mathcal{R}$ es igual a C.

(b) Si $D, E \in C/\mathcal{R}$ y $D \neq E$ entonces D y E son conjuntos disjuntos.

Un subconjunto $\mathcal{H}$ de $\mathcal{P}(C)$ que tiene estas dos propiedades: (1) la unión de elementos de $\mathcal{H}$ da C y (2) cada par de elementos distintos de $\mathcal{H}$ son disjuntos, se denomina una *partición* de C. Así, por (a) y (b), $C/\mathcal{R}$ es una partición de C.

Por ejemplo, los números pares e impares forman una partición del conjunto de los números enteros, $\mathbb{Z}$, con dos elementos; y puede obtenerse como conjunto cociente de la relación de equivalencia: "$a\mathcal{R}b$ si y sólo si $a - b$ es par".

Si $\mathcal{R}$ es una relación de equivalencia, se suele escribir $a\mathcal{R}b$ como $a \overset{\mathcal{R}}{\sim} b$, o simplemente, $a \sim b$; y el conjunto cociente por $C/\sim \equiv C/\mathcal{R}$.

Relación de orden: Una *relación de orden*, $\mathcal{R}$, en un conjunto C es una relación que verifica las propiedades siguientes:

1. Propiedad *reflexiva*: $\forall\, a \in C, \quad a\mathcal{R}a$.

2. Propiedad *antisimétrica*: Si $a, b \in C$, $a\mathcal{R}b$ y $b\mathcal{R}a$ entonces $a = b$.
3. Propiedad *transitiva*: Si $a, b, c \in C$, $a\mathcal{R}b$ y $b\mathcal{R}c$ entonces $a\mathcal{R}c$.

Una relación de orden, $\mathcal{R}$, en un conjunto C se dice que es una relación de orden *total* si además se verifica: $\forall\, a, b \in C, \quad a\mathcal{R}b$ o $b\mathcal{R}a$. Si $\mathcal{R}$ es una relación de orden total, $a\mathcal{R}b$ se suele escribir como $a \leq b$.

La usual relación "menor o igual" entre números es una relación de orden total en los conjuntos de números reales $\mathbb{R}$ (también en $\mathbb{N}$, $\mathbb{Z}$ o en los racionales, $\mathbb{Q}$).

Ejercicios 4.

1. Di cuáles de estos enunciados son verdaderos:

$$a \in [a] \subset C/\mathcal{R} \qquad a \in [a] \in C/\mathcal{R} \qquad a \in [a] \in C \qquad a \in [a] \subset C.$$

2. Sea $C = \{1, 2, 3, 4, 5, 6\}$ y sea $\mathcal{R}$ una relación de equivalencia en C. Supongamos que sabemos que $1\mathcal{R}4$, $2\mathcal{R}3$, $2\mathcal{R}5$, 1 no está $\mathcal{R}$–relacionado con 3, y 2 no está $\mathcal{R}$–relacionado con 6. Usa las propiedades que definen una relación de equivalencia para completar todas las $\mathcal{R}$–relaciones que se deducen de los datos ¿Está $\mathcal{R}$ unívocamente determinada? ¿Cuántos elementos tiene el conjunto cociente $C/\mathcal{R}$?

3. En $\mathbb{R}^2$ se define la siguiente relación de equivalencia

$$(x, y) \sim (x', y') \quad \Longleftrightarrow \quad x = x'$$

Determina qué tipo de subconjuntos de $\mathbb{R}^2$ son las clases de equivalencia pertenecientes a $\mathbb{R}^2/\sim$; por ejemplo, determina la clase $[(1, 2)]$ ¿Podrías establecer una biyección entre $\mathbb{R}$ y $\mathbb{R}^2/\sim$?

4. Sea C un conjunto y sea $\mathcal{H}$ un subconjunto de $\mathcal{P}(C)$. Decimos que $\mathcal{H}$ es una *partición* de C si se verifican las condiciones siguientes:
   (a) La unión de todos los subconjuntos de C que son elementos de $\mathcal{H}$ es igual a C; esto es:
   $$\bigcup_{A \in \mathcal{H}} A = C$$
   (b) Si $D, E \in \mathcal{H}$ y $D \neq E$, entonces $D \cap E = \varnothing$.

   Ahora, dada una partición $\mathcal{H}$ de C, definid una relación de equivalencia $\mathcal{R}$ en C de tal forma que $\mathcal{H} = C/\mathcal{R}$ (¡Probad que hay una correspondencia biyectiva entre las particiones de C y las relaciones de equivalencia en C!).

5. Definimos la relación $\leq$ en $\mathbb{N}$ como es usual; esto es: $\forall\, a, b \in \mathbb{N}$,

$$a \leq b \iff a \text{ es menor o igual que } b$$

   Probar que es una relación de orden total en $\mathbb{N}$.

6. Dado $p \in \mathbb{N}$, definimos en $\mathbb{Z}$ la relación $\sim_p$ de la siguiente forma: $\forall\, a, b \in \mathbb{Z}$,

$$a \sim_p b \iff \exists k \in \mathbb{Z} \text{ tal que } a - b = kp.$$

   Probar que es una relación de equivalencia en $\mathbb{Z}$. ¿Cuantos elementos tiene el conjunto cociente $\mathbb{Z}/\sim_p$ —frecuentemente denotado por $\mathbb{Z}_p$—?

5. Operaciones

Operación interna: Una *operación interna* o *ley de composición interna* en un conjunto C es una manera de asignar a cada dos elementos ordenados de C un elemento de C; es decir, una operación interna es una aplicación de $C \times C$ en C.

Para estas aplicaciones que son operaciones modificamos ligeramente la notación, denotando al elemento imagen del par ordenado (a, b) por $a * b$, donde "$*$" es el símbolo que representa a la operación. La situación se resume en el siguiente diagrama:

$$C \times C \xrightarrow{*} C \qquad (a, b) \longmapsto a * b$$

Cuando en un conjunto se definen una o varias operaciones, verificando ciertas propiedades, se dice que se ha dotado al conjunto de una *estructura algebraica*. Entre los tipos de estructuras algebraicas mas utilizados están las que siguen a continuación.

Estructura de grupo: Un *grupo* es un par $(C, *)$ donde C es un conjunto sobre el que hay definida una operación interna, $*$, que verifica las siguientes propiedades:

(I) La operación es *asociativa*; esto es, para cualesquiera $a, b, c \in C$ se verifica $(a * b) * c = a * (b * c)$.

(II) Existe un elemento especial, llamado *elemento neutro* y denotado por $e \in C$, de manera que, para cualquier $a \in C$, se verifica $a * e = e * a = a$.

(III) Para cada $a \in C$, existe un elemento $a' \in C$, llamado *elemento simétrico de* a, tal que $a * a' = a' * a = e$.

Cuando, además, el grupo verifica que:

(IV) La operación es *conmutativa*; esto es, para cualesquiera $a, b \in C$ se verifica $a * b = b * a$

entonces se dice que el grupo es *conmutativo* o *abeliano*.

Dos notaciones son frecuentemente utilizadas para grupos:

- *Notación aditiva*: A la operación " $*$ " se le denota por " $+$ " y se le llama *suma*; en lugar de $a * b$, escribiremos $a + b$ y lo leeremos "a más b" . Bajo esta notación: al elemento neutro se le suele llamar *cero* o *elemento nulo*, y se le denota por 0; y al elemento simétrico de a se le llama *opuesto* de a y se le denota por $-a$. También se puede escribir $a - b$ en vez de $a + (-b)$.

- *Notación multiplicativa*: A la operación " $*$ " se le denota por " $\cdot$ ", y se le llama *producto* o *multiplicación*; en lugar de $a * b$, escribiremos $a \cdot b$, o simplemente, si no hay posibilidad de error, yuxtaponiendo las letras ab, y lo leeremos "a por b". Bajo esta notación: al elemento neutro se le suele llamar *unidad*, y se le denota por 1; y al elemento simétrico de a se le llama *inverso* de a y se le denota por a^{-1}. También se puede escribir $\frac{a}{b}$ en lugar de $a \cdot b^{-1}$.

La notación aditiva se suele emplear únicamente en el caso de grupos conmutativos.

Algunos ejemplos de grupos: (a) La suma habitual de números es una operación interna para el conjunto de números naturales, $\mathbb{N}$, para los números enteros, $\mathbb{Z}$, para los números racionales, $\mathbb{Q}$, para los números reales, $\mathbb{R}$ y para los números complejos, $\mathbb{C}$. Son grupos conmutativos $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ y $(\mathbb{C}, +)$, pero $(\mathbb{N}, +)$ no es grupo.

(b) El producto habitual de números es una operación interna para $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$. Son grupos conmutativos $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$ y $(\mathbb{C} \setminus \{0\}, \cdot)$, pero si se añade el 0 no son grupos porque el cero no tiene inverso. En cambio, $(\mathbb{Z} \setminus \{0\}, \cdot)$ no es un grupo porque el inverso de un entero no es, en general, entero.

(c) También es grupo $(\{1, -1\}, \cdot)$. La llamada *tabla* de esta operación (¡tabla de multiplicar!) es:

$\cdot$	1	-1
1	1	-1
-1	-1	1

(d) A partir de la suma en $\mathbb{Z}$, se puede definir en el conjunto cociente $\mathbb{Z}/\sim_p$ — ver ejercicio 6 del apartado 4. Relaciones— una suma que es una operación interna. Resulta que $(\mathbb{Z}/\sim_p, +)$ es un grupo conmutativo. Lo denotaremos como suele hacerse por $\mathbb{Z}_p \equiv \mathbb{Z}/\sim_p$. Se los conoce como "*los enteros módulo p*".

(e) Sea A un conjunto y denotemos por $\mathcal{S}_A$ al conjunto de las funciones biyectivas de $A \to A$. Entonces $(\mathcal{S}_A, \circ)$ es un grupo con la operación composición de aplicaciones. Si el conjunto $A = \{1, 2, \cdots, n\}$ entonces denotamos $\mathcal{S}_n \equiv \mathcal{S}_A$ y se llama el n-ésimo *grupo simétrico* (o grupo de *permutaciones* de n elementos).

DEFINICIÓN. Dado un grupo $(C, *)$, un *subgrupo* de C es un subconjunto D de C tal que $(D, *)$ es un grupo; o, equivalentemente, si: (i) para todo pareja de elementos $a, b \in D$, se verifica que $a * b \in D$; (ii) el neutro $e \in D$; y (iii) para todo $a \in D$, el simétrico $a' \in D$.

Una condición necesaria y suficiente para que un subconjunto $D \subset C$ sea subgrupo de $(C, *)$ es que

(iv) $\forall\, a, b \in D$, se tiene que $a * b' \in D$, siendo b' el simétrico de b.

¡Probadlo! Es decir, probad que (i), (ii) y (iii) $\iff$ (iv). ¿Cómo se escribe (iv) en notación aditiva o multiplicativa?

Por ejemplo, $\mathbb{Z}$ es un subgrupo de $(\mathbb{R}, +)$. Otro ejemplo: dado $n \in \mathbb{N}$, el conjunto $n\mathbb{Z} := \{nk : k \in \mathbb{Z}\}$ de los *múltiplos* de n es un subgrupo de $(\mathbb{Z}, +)$.

DEFINICIÓN. Sean $(C, *)$ y $(D, \diamond)$ dos grupos. Decimos que una aplicación $f\colon C \to D$ es un *homomorfismo de grupos* si:

$$\forall\, a, b \in C, \quad \text{se verifica} \quad f(a * b) = f(a) \diamond f(b)$$

Por ejemplo, la aplicación $f\colon \mathbb{R} \to \mathbb{R} \setminus \{0\}$, dada por $f(x) = e^x$ es un homomorfismo de grupos de $(\mathbb{R}, +)$ en $(\mathbb{R} \setminus \{0\}, \cdot)$, ¿verdad?

Si f es un homomorfismo de grupos y además es una aplicación inyectiva, entonces decimos que f es un *monomorfismo* de grupos.

Si f es un homomorfismo de grupos y además es una aplicación sobreyectiva, entonces decimos que f es un *epimorfismo* de grupos.

Si f es un homomorfismo de grupos y además es una aplicación biyectiva, entonces decimos que f es un *isomorfismo* de grupos. Si existe un isomorfismo entre dos grupos diremos que ambos grupos son *isomorfos*.

Si f es un homomorfismo de un grupo en sí mismo, entonces decimos que f es un *endomorfismo* del grupo.

Si f es un isomorfismo de un grupo en sí mismo, entonces decimos que f es un *automorfismo* del grupo.

Algunos resultados: Veamos algunos pequeños "teoremas" sobre grupos, con sus demostraciones. Consideremos un grupo $(C, *)$:

1. El elemento neutro es único. En efecto, porque si e y $e_\circ$ son dos neutros, entonces $e = e * e_\circ = e_\circ$. La primera igualdad es porque $e_\circ$ es neutro "por la derecha" y la segunda igualdad es porque e es neutro "por la izquierda".
2. Cada elemento posee un único simétrico. En efecto, porque si a' y $a'_\circ$ son dos simétricos de a entonces $a' = a' * e = a' * (a * a'_\circ) = (a' * a) * a'_\circ = e * a'_\circ = a'_\circ$.

Sigamos, pero empleando la notación multiplicativa $(C, \cdot)$, que es la que más se utiliza para grupos en general —no forzosamente conmutativos—:

3. Se verifica que $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$, $\forall\, a, b \in C$. En efecto,

$$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = (a \cdot (b \cdot b^{-1})) \cdot a^{-1} = (a \cdot e) \cdot a^{-1} = a \cdot a^{-1} = e,$$
$$(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = b^{-1} \cdot ((a^{-1} \cdot a) \cdot b) = b^{-1} \cdot (e \cdot b) = b^{-1} \cdot b = e.$$

4. Si $\exists a \in C$ tal que $a \cdot b = a \cdot c$ entonces $b = c$. En efecto, para probarlo basta multiplicar por a^{-1} por la izquierda en ambos lados de la igualdad. Y también: si $\exists a \in C$ tal que $b \cdot a = c \cdot a$ entonces $b = c$. En efecto, basta multiplicar por a^{-1} por la derecha en ambos lados de la igualdad.

Estructura de anillo: Un *anillo* es una terna $(C, +, \cdot)$, donde C es un conjunto sobre el que hay definidas dos operaciones internas, $+$ y $\cdot$, que verifica las siguientes propiedades:

(I) $(C, +)$ es un grupo conmutativo.

(II) La operación producto es asociativa; esto es, si $a, b, c \in C$, entonces se verifica $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(III) La operación producto es *distributiva* respecto de la suma; esto es, si $a, b, c \in C$, se verifica:

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$
$$(b + c) \cdot a = (b \cdot a) + (c \cdot a)$$

Se dice que es un *anillo con unidad* cuando se verifica además:

(IV) La operación producto tiene elemento unidad; esto es, existe un elemento en C, distinto de 0, que denotamos por 1, tal que $a \cdot 1 = 1 \cdot a = a$, $\forall\, a \in C$.

Si el producto tiene la propiedad conmutativa entonces se dice que es un anillo *conmutativo* o *abeliano*.

NOTAS: Se verifica que $0 \cdot a = a \cdot 0 = 0,\ \forall\, a \in C$. En efecto: como $a + 0 = a$ y $a \cdot a + 0 = a \cdot a$, de la propiedad distributiva se sigue que

$$a \cdot a + 0 \cdot a = (a + 0) \cdot a = a \cdot a = a \cdot a + 0,$$

y aplicando la propiedad 4 de los resultados de grupos (en notación aditiva) se sigue $0 \cdot a = 0$ —análogamente se prueba la otra igualdad—.

Si en un anillo con unidad se admitiera la posibilidad de que $0 = 1$ el anillo solo tendría un elemento pues $1 \cdot a = a$ y $0 \cdot a = 0$ implicaría que $a = 0,\ \forall\, a \in C$. Este caso, que aquí hemos excluido, se dice que es un "anillo trivial".

Algunos ejemplos de anillos: (a) El conjunto de los números enteros con la suma y el producto, $(\mathbb{Z}, +, \cdot)$, tiene estructura de anillo conmutativo con unidad. También $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$ son anillos pero, como veremos en el siguiente apartado, el producto en estos conjuntos tiene una propiedad más.

(b) El conjunto de polinomios de una variable (o indeterminada) con coeficientes reales, denotado por $\mathcal{P}(\mathbb{R})$ o por $\mathbb{R}[x]$ (si llamamos x a la variable o indeterminada), dotado con las operaciones habituales de suma y producto de polinomios, es un anillo conmutativo con unidad.

(c) Sea A un conjunto dado. Si consideramos el conjunto de las funciones de A en $\mathbb{R}$, $\mathcal{F} = \{f / f\colon A \to \mathbb{R} \text{ es una función }\}$, con la suma de funciones $f + g$, definida por $(f + g)(x) := f(x) + g(x)$, y el producto de funciones fg, definido por $(fg)(x) := f(x)g(x)$, entonces $\mathcal{F}$ es un anillo conmutativo con unidad. Nótese que el elemento unidad es la función 1_A, definida por valer 1 constante, $1_A(x) = 1,\ \forall\, x \in A$.

(d) Sea $(C, +)$ un grupo conmutativo dado. Si en el conjunto $\operatorname{End} C$, de los endomorfismos del grupo C, consideramos las operaciones: suma $f + g$, definida —como en el ejemplo anterior— por $(f + g)(x) := f(x) + g(x)$, y composición de aplicaciones $f \circ g$, definida por $(f \circ g)(x) := f(g(x))$, entonces $(\operatorname{End} C, +, \circ)$ es un anillo con unidad, que en general no es conmutativo.

(e) En el grupo $(\mathbb{Z}_p, +)$ —ver el ejemplo (d) de grupos— se define un producto a partir de la multiplicación de números enteros. Resulta que $(\mathbb{Z}_p, +, \cdot)$ es un anillo conmutativo con unidad.

Estructura de cuerpo: Un *cuerpo* es una terna $(C, +, \cdot)$, donde C es un conjunto, sobre el que hay definidas dos operaciones internas, que verifica las siguientes propiedades:

(I) $(C, +, \cdot)$ es un anillo conmutativo con unidad.

(II) Todo elemento de C, distinto de 0, tiene inverso; esto es,

$$\forall\, a \in C \setminus \{0\},\ \exists\, a^{-1} \in C \ \text{ tal que } \ a \cdot a^{-1} = a^{-1} \cdot a = 1.$$

En otras palabras, un cuerpo es un anillo $(C, +, \cdot)$ tal que $(C \setminus \{0\}, \cdot)$ es un grupo abeliano.

NOTA: ¡El cero no tiene inverso! Si existiera $0^{-1} \in C$ tal que $0 \cdot 0^{-1} = 1$, como $0 \cdot a = 0,\ \forall\, a \in C$, tomando $a = 0^{-1}$ concluiríamos que $0 = 1$, y este caso está excluido de la definición de cuerpo —ver Notas a la definición de anillo—.

Como ejemplos de cuerpos tenemos $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$ con las operaciones habituales de suma y producto, no así los números enteros pues les falla la propiedad de los elementos inversos. En este curso nos interesan los cuerpos de números reales y de números complejos —conviene que repaséis las operaciones elementales en $\mathbb{C}$; por ejemplo en `https://www.superprof.es/apuntes/escolar/matematicas/aritmetica/complejos/` —.

Análogamente a la definición de homomorfismo de grupos, se puede definir lo que es un homomorfismo de anillos o de cuerpos, pero no lo usaremos en este curso. En general, se puede definir la noción de homomorfismo para cualquier tipo de estructura algebraica. Volveremos a ello cuando introduzcamos la estructura algebraica de *espacio vectorial*.

EJERCICIOS 5.

1. Construye la tabla de la suma para los grupos $(\mathbb{Z}_2, +)$ y $(\mathbb{Z}_3, +)$ e identifica quién es el opuesto de cada elemento —ver ej. (d) de grupos—.
2. Demuestra que $(\mathcal{S}_A, \circ)$ es un grupo —ver ej. (e) de grupos—.
3. Consideramos $(\mathbb{Z}, +)$ el grupo aditivo de los números enteros. Probar que la aplicación $f : \mathbb{Z} \to \mathbb{Z}, \quad f(k) = 7k$, es un homomorfismo de grupos, y además es monomorfismo pero no epimorfismo. ¿Son homomorfismos las aplicaciones g y h de $(\mathbb{Z}, +)$ en $(\mathbb{Z}, +)$ dadas por $g(k) = 4k + 3$ y $h(k) = k^2$?

4. Prueba que un endomorfismo f de $(\mathbb{Z}, +)$ está determinado si sabemos el valor de $f(1)$.
5. Sobre el conjunto $C = \{0, 1\}$ se definen las operaciones $+$ y $\cdot$ como la suma y el producto habituales de números, salvo que, por definición, decimos que $1 + 1 := 0$. Comprobar que $(C, +, \cdot)$ es un cuerpo conmutativo. ¿Cuál es el inverso de 1? ¿Y el opuesto de 1? Si hubiéramos definido $1 + 1 := 1$, ¿sería $(C, +, \cdot)$ un cuerpo?