MÉTODOS MATEMÁTICOS DE LA FÍSICA I

Ignacio Sánchez Rodríguez

Curso 2006-07

TEMA PRELIMINAR

ÍNDICE

Date: Revisado el 3 de Octubre de 2006.

1. Lenguaje matemático

Definiciones y teoremas: La *definición* de un objeto nuevo es la expresión de lo que ese objeto es; dicha expresión emplea objetos previamente conocidos. Un *teorema* es la expresión de un resultado nuevo sobre objetos conocidos y su *demostración* es la prueba clara de la veracidad del resultado que enuncia el teorema; la demostración se obtiene a partir de otros enunciados verdaderos, previamente conocidos.

Los teoremas pueden ser llamados también *proposiciones* cuando son teoremas de menor importancia, reservando la palabra "teorema" para aquellos resultados nuevos que sean más relevantes. También se usan el término *lema*, para designar una proposición que se utiliza para la demostración de algún teorema posterior, y el término *corolario*, para designar una proposición que se prueba fácilmente a partir de un teorema anterior.

La igualdad: Una *igualdad* es un enunciado en el que se afirma que dos expresiones representan el mismo objeto. Si dos expresiones S y T representan el mismo objeto, podemos poner entre ellas el *signo de la igualdad*

$$S = T$$

y decimos que S es el *primer término* de la igualdad y T es el *segundo término* de la igualdad.

En el caso en que la igualdad sirva para definir lo que entendemos por S, decimos que es una *igualdad por definición* y, opcionalmente, podemos escribir

$$S := T$$

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

$$S \equiv T$$

Conjunción, disyunción y negación: Si p y q son dos enunciados, la *conjunción*

$$p \ \text{y} \ q$$

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

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

$$p \ \text{o} \ q$$

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

Si p es un enunciado, la *negación*

$$\text{no} \ p$$

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

Implicaciones: Dados dos enunciados p y q, se puede construir el enunciado "*p implica q*", que se denota como

$$p \Longrightarrow q$$

y que significa que si p es verdadero entonces q es verdadero (¡si p es falso, de este enunciado nada podemos deducir de q!). La verdad del enunciado "*p implica q*" nos dice que si q es falso necesariamente p también es falso. Por tanto, esta implicación es equivalente al enunciado

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

Dados dos enunciados p y q, se puede construir el enunciado "*p si y sólo si q*", que es la conjunción de los enunciados "p implica q" y "q implica p", y que se denota como

$$p \Longleftrightarrow q$$

y significa, simultáneamente, que si p es verdadero entonces q es verdadero y que si p es falso entonces q es falso. Equivalentemente, significa, simultáneamente, que si q es verdadero entonces p es verdadero y que si q es falso entonces p es falso. La expresión "$p \Leftrightarrow q$" también se puede leer como "p es *equivalente* a q" o "p es *necesario y suficiente* para q".

Cuantificadores: Los *cuantificadores* son ciertas expresiones relativas a la cantidad, representadas por un signo, que se utilizan frecuentemente para construir enunciados y que, en el lenguaje matemático, tienen un significado inequívoco. Principalmente son dos:

- El cuantificador "para todo" denotado con el signo $\forall$; por ejemplo, la expresión
$$\forall a$$
significa "para todo a", "para cualquier a" o "para cada a".
- El cuantificador "existe" denotado con el signo $\exists$; por ejemplo, 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:

$$\forall a, \exists b \qquad \text{leído "para cada } a\text{, existe } b\text{"}$$

que significa que para cada a que elija puedo encontrar un b (¡para diferentes elecciones de a los correspondientes b pueden ser diferentes!);

$\exists a, \forall b \dots$ leído "existe a tal que para todo $b \dots$"

que significa que puedo encontrar un a de tal manera que cualquiera que sea $b \dots$ (¡no es válido cambiar de a dependiendo de cual sea b; determinado quién sea 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. Sea p el enunciado "x es mayor que 0" y sea q el enunciado "y es mayor que 0". Dibuja en un plano de coordenadas XY, las regiones que corresponden a los enunciados "p y q", "p o q", y a las negaciones de ambos.
3. Si un teorema afirma: "p implica q", se puede demostrar probando: "(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*, $p \Leftrightarrow q$, hay que demostrar dos implicaciones: (i) $p \Rightarrow q$ y (ii) $q \Rightarrow p$. Probar así la siguiente proposiciön: 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 con sentido 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 de color blanco".

2. Conjuntos

Elementos y conjuntos: Las nociones de elemento y de conjunto no se definen, se apela a la intuición. Un conjunto es algo que tiene elementos y un elemento es algo que está en un conjunto. Una manera elemental de representar a un conjunto, que llamaremos *representación explícita* de un conjunto, es encerrando entre llaves los elementos que tiene; por ejemplo, $C = \{1,2,3\}$. Cuando un elemento a está en un conjunto C, decimos que a *pertenece* a C y se representa por

$$a \in C$$

Lo que sí se pide en matemáticas es que los conjuntos que consideremos estén "bien definidos", en el sentido de que de todo elemento podamos decir si pertenece o no pertenece al conjunto.

Se postula 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 $C \cup D$, definido por

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

Si C y D son dos conjuntos, se construye un nuevo conjunto llamado la *intersección* de C y D, denotado por $C \cap D$, 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 *disjumtos* si $C \cap D = \varnothing$.

Por último, llamamos la *diferencia* de C y D, y lo denotamos por $C-D$ o por $C\setminus D$, al conjunto definido por

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

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

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

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

$$\text{si} \quad a\in D \quad \text{entonces} \quad a\in C$$

Si D está incluido en C, 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:

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

que se leería 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 ":", cuyo significado es "que verifica que" o "tal que", a veces se escribe con el símbolo "/".

Si D es un subconjunto de C, decimos que el subconjunto $C\setminus D$ es el *complementario* de D (en C).

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

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

Por definición de subconjunto, todo conjunto es subconjunto de sí mismo; por tanto, $C \in \mathscr{P}(C)$. Por convenio, el conjunto vacío es subconjunto de cualquier conjunto; y por tanto, $\varnothing \in \mathscr{P}(C)$.

Ejercicios 2.

1. Dos conjuntos se dice que son iguales si tienen los mismos elementos. Para demostrar la igualdad entre dos conjuntos, $C = D$, hay que demostrar dos cosas: (i) $C \subset D$ y (ii) $D \subset C$.

   Sean los conjuntos

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

   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 $\bigcap_{i\in\mathbb{N}} C_i$.

Trata de dar las definiciones de la unión y de la intersección de todos los C_i; es decir completa estos dos enunciados:

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

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

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 $\mathscr{P}(C)$. Haz lo mismo para $\mathscr{P}(D)$, siendo $D = \{C\}$. Halla la unión y la intersección de los conjuntos $\mathscr{P}(C)$ y $\mathscr{P}(D)$.

6. Relee 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".

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 f. Una función 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.

Normalmente una función viene 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 hay que decir además cuál es el conjunto inicial y cuál es el conjunto final para tener bien definida la función!).

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

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

Composición de aplicaciones: Sean $f\colon C \to D$ y $g\colon D \to E$ 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 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:

$$\begin{tikzcd} C \arrow[r, "f"] \arrow[dr, "g\circ f"'] & D \arrow[d, "g"] \\ & E \end{tikzcd} \qquad \begin{tikzcd} a \arrow[r, mapsto, "f"] \arrow[dr, mapsto, "g\circ f"'] & f(a) \arrow[d, mapsto, "g"] \\ & g(f(a)) \end{tikzcd}$$

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 $f(C)$. Probar que la definición de que f es sobreyectiva es equivalente a decir que $f(C) = D$.

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 le llama *intervalo abierto* $]a,b[$ al subconjunto de $\mathbb{R}$ dado por $]a,b[:= \{x \in \mathbb{R} \colon a < x < b\}$.

   Sea f la aplicación del producto cartesiano $\mathbb{R} \times \mathbb{R} \equiv \mathbb{R}^2$ en $\mathbb{R}$, dada por

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

   Hallar 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 reales 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

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

   es biyectiva. Calcular la función inversa de f.

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

   $$f \colon \mathbb{R}^2 \to \mathbb{R} \qquad (x,y) \longmapsto 2x - 3y$$
   $$g \colon \mathbb{R} \to \mathbb{R}^2 \qquad x \longmapsto (2x^2, x + 3)$$

4. Relaciones

Relación en un conjunto: Una *relación* $\mathscr{R}$ 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 $\mathscr{R} \subset C \times C$ es una relación y si $(a,b) \in \mathscr{R}$, decimos que a está *$\mathscr{R}$–relacionado* con b, y escribimos $a\mathscr{R}b$.

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

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

Dado $a \in C$, el subconjunto de C formado por todos los elementos que están $\mathscr{R}$–relacionados con a se dice que es una *clase de equivalencia* por la relación de equivalencia $\mathscr{R}$, y que a es un *representante* de la clase. A una clase de equivalencia por $\mathscr{R}$, con representante a, la denotaremos por $[a]_{\mathscr{R}}$, o simplemente, si no hay posibilidad de error, por $[a]$.

El conjunto cuyos elementos son todas las clases de equivalencia es el llamado *conjunto cociente* respecto de $\mathscr{R}$, y se denota por $C/\mathscr{R}$, leído "C sobre $\mathscr{R}$" o "C cociente $\mathscr{R}$". Obviamente, $C/\mathscr{R}$ es un subconjunto de $\mathscr{P}(C)$. Y por las propiedades que tiene, este subconjunto se denomina una *partición* de C. Estas propiedades son:

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

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

Si $\mathscr{R}$ es una relación de equivalencia, $a\mathscr{R}b$ se suele escribir como $a \overset{\mathscr{R}}{\sim} b$, o simplemente, $a \sim b$.

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

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

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

Ejercicios 4.

1. Di cuáles de estos enunciados son verdaderos:

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

2. Sea $C = \{1,2,3,4,5,6\}$ y sea $\mathscr{R}$ una relación de equivalencia en C. Supongamos que sabemos que $1\mathscr{R}4,\ 2\mathscr{R}3,\ 2\mathscr{R}5,$ 1 no está $\mathscr{R}$–relacionado con 3, y 2 no está $\mathscr{R}$–relacionado con 6. Usa las propiedades que definen una relación de equivalencia para completar todas las $\mathscr{R}$–relaciones que se deducen de los datos ¿Está $\mathscr{R}$ unívocamente determinada? ¿Cuántos elementos tiene el conjunto cociente $C/\mathscr{R}$?
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 $\mathscr{H}$ un subconjunto de $\mathscr{P}(C)$. Decimos que $\mathscr{H}$ es una *partición* de C si se verifican:
   (a) La unión de todos los subconjuntos de C que son elementos de $\mathscr{H}$ es igual a C, esto es:

$$\bigcup_{A \in \mathscr{B}} A = C$$

   (b) Si $D, E \in \mathscr{B}$ y $D \neq E$, entonces $D \cap E = \varnothing$.

   Dada una partición $\mathscr{H}$ de C, definir una relación de equivalencia en C de tal forma que $\mathscr{H} = C/\mathscr{R}$ (¡Esto prueba que hay una correpondencia biyectiva entre las particiones de C y las relaciones de equivalencia en C!).
5. Definimos la relación $\leq$ en $\mathbb{N}$ como es usual: $\forall a, b \in \mathbb{N}$,

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

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

5. Estructuras algebraicas

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; esto 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 $a^\dagger \in C$, llamado *elemento simétrico de a*, tal que $a * a^\dagger = a^\dagger * a = e$.

Cuando el grupo además 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 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 $a \cdot b^{-1}$.
- *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 $a+(-b)$.

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

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, para cualesquiera $a,b,c \in C$ se verifica $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(III) La operación producto es *distributiva por la derecha* y *por la izquierda* respecto de la suma; esto es, para cualesquiera $a,b,c \in C$, se verifica:

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

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

Cuando el anillo verifica:

(IV) La operación producto tiene elemento unidad; esto es, $\exists 1 \in C$ tal que se verifica $a \cdot 1 = 1 \cdot a = a$, para cualquier $a \in C$.

entonces se dice que es un anillo *con unidad*.

Cuando el anillo verifica:

(v) El producto es conmutativo.

entonces se dice que es un anillo *conmutativo* o *abeliano*.

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 con unidad.

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

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

(¡el cero no tiene inverso!).

Cuando además el cuerpo verifica que:

(III) La operación producto es conmutativa.

entonces se dice que es un cuerpo *conmutativo* o *abeliano*.

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

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

Análogamente, 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*.

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.

Ejercicios 5.

1. De las propiedades enumeradas arriba que propiedades verifican las siguientes estructuras algebraicas:

$$(\mathbb{N},+) \qquad (\mathbb{N},\cdot) \qquad (\mathbb{Z},+) \qquad (\mathbb{Z},\cdot) \qquad (\mathbb{Z},+,\cdot) \qquad (\mathbb{R},+,\cdot)$$

2. Sobre el conjunto $C=\{0,1\}$ se definen las operaciones internas $+$ y $\cdot$, igual que la suma y el producto habituales de números, salvo que, por definición, decimos que $1+1=0$. Se puede comprobar que $(C,+,\cdot)$ es un cuerpo conmutativo ¿Cuál es el inverso de 1?, ¿y el opuesto de 1?

   Y si hubiéramos definido $1+1=1$ ¿sería $(C,+,\cdot)$ un cuerpo?

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. Probar que un homomorfismo f de $(\mathbb{Z},+)$ en $(\mathbb{Z},+)$ está determinado si sabemos el valor de $f(1)$.