Elementos de matemática discreta

Pablo Pallàs

22 de abril de 2023

Índice

1. Introducción a la lógica

2. Aritmética

2.1. Los números naturales

Para ir fabricando los números naturales sólo necesitamos disponer del primero, el 0 (siguiendo el convenio que se empleará en este texto). A continuación definiremos una aplicación que nos permitirá ir pasando al siguiente, y de ese a su siguiente y así sucesivamente.

Pero, ¿qué es ese siguiente?, ¿cómo lo definimos?, pues si tenemos un natural n definiremos su siguiente como $n+1$ y lo denotaremos por $s(n)$. Es decir, definiremos una aplicación tal que

$$\begin{array}{rccc} s\colon & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & n & \longmapsto & s(n) = n+1. \end{array}$$

y a $s(n)$ lo denominaremos *sucesor de* n. Inversamente, si tenemos un natural n tal que es el sucesor de otro natural k, $n = s(k)$, entonces a k lo denominaremos *predecesor de* n. Así, pasar de un número natural al siguiente es asociar cada n su

sucesor $s(n)$, es decir, aplicar la aplicación que acabamos de definir. Esta aplicación es claramente inyectiva ya que, dados dos naturales n, m, si $s(n) \neq s(m)$ entonces $n+1 \neq m+1$ y de aquí $n \neq m$. Decir que 0 es el primer número natural es decir que *no es el sucesor de ningún otro natural*, es decir, $0 \neq s(n)$ para cualquier $n \in \mathbb{N}$. Esto quiere decir que el 0 no está en el conjunto imagen de la aplicación s, $0 \notin Im\, s$ ó $0 \in \mathbb{N} \setminus s(\mathbb{N})$. También sabemos que que el principio de inducción tiene un enunciado conjuntista en términos de esta aplicación: dado $S \subseteq \mathbb{N}$ tal que $0 \in S$ y $s(n) \in S$ para cualquier $n \in S$, entonces necesariamente $S = \mathbb{N}$. Gracias a esto podemos llegar a los conocidos como ***axiomas de Peano***.

Estos axiomas surgen a finales del siglo XIX como respuesta a una crisis de la fundamentación matemática que se vivió en este siglo revolucionario para las matemáticas (crisis que por cierto se extendió también a las primeras décadas del siglo XX). El resultado fue la axiomatización de toda la aritmética, conocida desde tiempos de las sociedades antiguas, y su reconstrucción a partir de dichos axiomas, que se aplicaban sobre los números naturales.

Las propiedades que permiten describir axiomáticamente los números naturales son las que siguen:

Existen un conjunto $\mathbb{N}$ cuyos elementos se denominan ***números naturales***, que contienen un elemento distinguido 0, y una aplicación $s\colon \mathbb{N} \longrightarrow \mathbb{N}$ de modo que

1. s es inyectiva.
2. $0 \notin s(\mathbb{N})$.
3. Dado $S \subseteq \mathbb{N}$ con $0 \in S$ y $s(S) \subseteq S$, entonces $S = \mathbb{N}$ (por inducción).

Resulta bastante sorprendente que todas las propiedades usuales de los números naturales puedan deducirse de estas, tal y como demostró el matemático italiano Giuseppe Peano a finales del siglo XIX. En este texto se usará, tal y como se dijo antes, el convenio que si bien no empleó Peano en su primera formulación sí lo hizo a partir de 1895, esto es, partiendo de 0 como primer natural.

Axiomas de Peano. Existe un conjunto N, cuyos elementos se denominan números naturales, tal que

I. Para todo número natural n existe otro número natural, $s(n)$ que denominaremos *sucesor de* n.

II. Existe un número natural, que denotamos por 0, tal que $0 \neq s(n)$ para cualquier número natural n.

III. Para números naturales cualesquiera n y m, $s(n) = s(m)$ si y sólo si $n = m$.

IV. *Axioma de inducción matemática*: un conjunto de números naturales que contenga a 0 y que para cada n contenga su sucesor, $s(n)$, debe incluir todos los números naturales. Es decir, dado $S \subseteq \mathbb{N}$ tal que $0 \in S$ y $s(n) \in S$ para todo $n \in S$, entonces $S = \mathbb{N}$.

Así, es inmediato comprobar que la imagen de esta aplicación s es $\mathbb{N} \setminus 0$.

Ya hemos definido anteriormente lo que era el sucesor de un número natural, y lo habíamos expresado por $n+1$, para un n natural, y habíamos supuesto que $+$ era la suma habitual que todos conocemos desde niños. Sin embargo, esta suma no tiene por qué estar necesariamente definida sobre $\mathbb{N}$ inicialmente, definámosla:

Proposición 2.1 (***suma en*** $\mathbb{N}$)**.** *Definimos la suma de forma recurrente a partir de:*

a. $m + 0 = m$ *para cada* $m \in \mathbb{N}$.

b. $m + 1 = s(m)$

Como $m + n = s(m) + k$ *para cada* $m \in \mathbb{N}$*, si* $n = s(k)$.

Entonces, dados dos números naturales cualesquiera m *y* n*, su suma* $m + n$ *es un número natural perfectamente definido.*

Demostración: En efecto, n no puede ser 0 por la regla a, así que es el sucesor de algún natural k, así por la regla b $n = s(k) = k+1$, luego $m+n = m+1+k = s(m)+k$, con $n = s(k)$. Ahora, consideremos el siguiente conjunto

$$S = \{n \in \mathbb{N} : m + n \text{ está bien definido para cada } m \in \mathbb{N}\}.$$

Se trata de ver que $S = \mathbb{N}$. En primer lugar, $m + 0 = m$ está bien definido por a, luego $0 \in S$. Y si $k \in S$ entonces $m + k = s(m) + l$, con $k = s(l)$, está bien definido para todo $m \in \mathbb{N}$. Elegimos $m = k$ y así $m + k = s(k) + l$, con $k = s(l)$, está bien definido luego $s(k) \in S$. Por el principio de inducción, $S = \mathbb{N}$.

□

Esto es, hemos definido la suma de forma recurrente. El definir algunos conceptos de forma recurrente (iterando sobre sí mismo) aparecerá en más ocasiones a lo largo del texto, por lo que es importante. De hecho, sabemos que, dados dos naturales $m, n \in \mathbb{N}$, $m + n = s(m) + k$, con $n = s(k)$, y aplicando esto de nuevo tenemos que $s(m) + k = s(s(m)) + l$, con $k = s(l)$, y si aplicamos sucesivamente llegaremos a un número m' tal que será suma de una serie de sucesores de m y 0, ya que iremos calculando los predecesores de l hasta llegar a 0, que no tiene. Igualmente con el producto:

Proposición 2.2 (***producto en*** $\mathbb{N}$)**.** *Definimos el producto de la siguiente manera:*

1. $m \cdot 1 = m$ *para cada* $m \in \mathbb{N}$.
2. $m \cdot n = m \cdot k + m$ *para cada* $m \in \mathbb{N}$*, si* $n = s(k)$.

Entonces, dados dos números naturales cualesquiera m, n*,* $m \cdot n$ *es un número natural perfectamente definido y que denotaremos simplemente por* mn.

Así, tenemos las siguientes operaciones suma y producto sobre el producto cartesiano de $\mathbb{N}$:

$$\begin{array}{rccc} +: & \mathbb{N} \times \mathbb{N} & \longrightarrow & \mathbb{N} \\ & (m, n) & \longmapsto & m + n \end{array}$$

$$\begin{array}{rccc} +\colon & \mathbb{N}\times\mathbb{N} & \longrightarrow & \mathbb{N} \\ & (m,n) & \longmapsto & mn \end{array}$$

Propiedades de la suma y el producto en $\mathbb{N}$. Dados números naturales cualesquiera m, n, p se cumplen:

1. Propiedad asociativa de la suma: $(m+n)+p = m+(n+p)$.
2. Propiedad conmutativa de la suma: $m+n = n+m$.
3. Propiedad cancelativa de la suma: $m+n = m+p$ implica que $n = p$.
4. Propiedad asociativa del producto: $(mn)p = m(np)$.
5. Propiedad conmutativa del producto: $mn = nm$.
6. Existencia de elemento neutro (identidad) para la suma: $m+0 = m = 0+m$.
7. Existencia del elemento neutro (identidad) para el producto: $1 \cdot n = n \cdot 1 = n$.
8. Propiedad cancelativa del producto: $mn = mp$ implica $n = p$.
9. Propiedad distributiva del producto respecto de la suma: $m(n+p) = mn+mp$.

De estas propiedades podemos deducir que el conjunto de los números naturales dotado de la operación suma, $+$, que ya hemos visto que es una operación binaria interna y asociativa, un ***monoide*** con elemento neutro 0. Notar que si no hubieramos definido el 0 como natural, algunos autores lo hacen, entonces tendríamos que $\mathbb{N}$ sería un simple semigrupo (un conjunto dotado de una operación binaria asociativa).

Ahora, si queremos comparar el tamaño de dos números naturales cualesquiera se define en $\mathbb{N}$ una ordenación.

Definición 2.3. *Dados dos números naturales cualesquiera m, n, escribiremos $m \leq n$ y diremos que m es* ***menor o igual*** *que n, o lo que es lo mismo, que n es* ***mayor o igual*** *que m, que se escribe $n \geq m$, cuando $n = m$ ó $n = m+p$ para algún natural p.*

Igualmente, diremos que $m < n$ ó $n > m$ para expresar que m es estrictamente menor que n, es decir, que $m \leq n$ y $m \neq n$.

Esto que acabamos de definir se denomina ***relación de orden***. Veamos cuál sería una formalización más general para cualquier conjunto A:

Definición 2.4. *Dado A un conjunto y R una relación binaria definida en A, diremos que R es una relación de orden si es:*

1. ***Reflexiva****: todo elemento de A está relacionado consigo mismo, esto es, xRx para todo $x \in A$.*
2. ***Antisimétrica****: si dos elementos de A están relacionados entre sí, entonces son iguales, es decir, si xRy, yRx con $x, y \in A$ entonces $x = y$.*

3. ***Transitiva**: si un elemento de A está relacionado con otro y éste a su vez está relacionado con un tercero, entonces el primero está relacionado con el tercero. Es decir, si xRy, yRz, con $x, y, z \in A$, entonces xRz.*

*Diremos además que la relación es de **orden total** si y sólo si todos los elementos del conjunto están relacionados entre sí, es decir, si dados dos elementos x, y cualesquiera de A entonces xRy ó yRx.*

*Al par (A, R) lo denominaremos **conjunto ordenado**.*

Así, es claro que en el conjunto de los números naturales $\mathbb{N}$, tanto $\leq$ como $\geq$ definen una relación de orden total. No todas las relaciones definen un orden total, por ejemplo la inclusión ($\subseteq$) con los conjuntos: dados dos conjuntos A, B no tiene por qué tenerse que $A \subseteq B$ ó $B \subseteq A$.

Sin embargo, la propiedad más interesante e importante de la relación de orden en $\mathbb{N}$ no es que sea total sino que sea lo que conocemos como una ***buena ordenación***:

Proposición 2.5 (***Principio de buena ordenación***)**.** *Todo conjunto no vacío de números naturales posee un elemento mínimo, es decir, dado $S \subseteq N$ no vacío, existe un elemento m en S tal que $m \leq n$ para todo $n \in S$.*

Demostración: Mostraremos que el principio de inducción implica necesariamente este resultado. Supongamos que existe un subconjunto $M \subseteq \mathbb{N}$ que no tiene elemento mínimo. Veremos que M es el conjunto vacío, es decir, $M = \emptyset$. Sea

$$M' = \{n \in \mathbb{N} : \forall x \in M \; x \geq n\}.$$

Es decir, se tratará de probar que $M' = \mathbb{N}$. En efecto, $0 \in M'$ ya que para todo $x \in \mathbb{N}$ se tiene $x \geq 0$, en particular para todo $x \in M$.

Sea ahora $n \in M'$, es decir, $\forall x \in M$ se tiene que $x \geq n$. Pero n no puede estar en M ya que M no tiene elemento mínimo. Como para todo $x \in M$ se tiene que $x \geq n$ pero $n \notin M$, entonces ningún x podrá ser n y así $x > n$, pero esto quiere decir que $x \geq n + 1$. Así $n + 1 = s(n) \in M'$, luego por inducción tenemos que $M' = \mathbb{N}$ y así necesariamente $\mathbb{M} = \emptyset$.

□

De este resultado deducimos que el principio de inducción implica el principio de buena ordenación, de hecho son equivalentes bajo ciertas condiciones.

Observación 2.5.1. *Algunas propiedades:*

1. *Todos los números naturales son mayores o iguales que 0, es decir, el elemento mínimo de $\mathbb{N} = 0$.*

2. *Dados $m, n \in \mathbb{N}$, se tiene que $m > n$ si y sólo si existe $p \in \mathbb{N} \setminus 0$ tal que $m = n + p$. Lo abreviaremos diciendo que $m - n \in \mathbb{N}$.*

   Notar que esto es así ya que $m = n + p$ implica necesariamente que $m \neq n$. Esto se deduce del hecho de que $m \neq m + 1$ para todo $m \in \mathbb{N}$ (se puede comprobar fácilmente por inducción sobre m) e igualmente que $m \neq m + p$ para todo $m \in \mathbb{N}$ y $p \in \mathbb{N} \setminus 0$ (por inducción sobre p).

3. *Dados dos naturales m, n, no puede verificarse $n < m < n+1$. Es decir, entre dos números naturales consecutivos no hay ningún número natural.*

   Esto es así porque entonces, de acuerdo con el punto anterior, $m = n + p$, $n + 1 = m + l$, con $p, l \in \mathbb{N} \setminus 0$, es decir, $p, l \geq 1$. Así, tendríamos que $n + 1 = n + p + l$, luego $n + 1 \geq n + 2$, lo cuál es absurdo.

2.2. El anillo de los números enteros

Los números naturales se pueden sumar y multiplicar, tal y como lo hemos definido anteriormente, pero no siempre se pueden restar. Es decir, dados dos naturales n, m no siempre $m - n \in \mathbb{N}$, por ejemplo $2 - 5 \notin \mathbb{N}$, es decir, no existe un número natural x tal que $x + 5 = 2$. Para poder resolver ecuaciones tan sencillas como la anterior será necesario considerar, además de $\mathbb{N}$, los números negativos (y según hayamos definido el 0 como natural o no también). Los números que así obtenidos se denominan ***números enteros*** e incluyen los positivos, los negativos y el cero. En ocasiones, al conjunto de los números enteros positivos se les denotará por $\mathbb{N}^+$, y al conjunto de los números enteros positivos y el 0 como $\mathbb{N}_0$ (lo que según el convenio de este texto antes eran simplemente los números naturales).

Definición 2.6. *Diremos que un x es un **número entero** si $x \in \mathbb{N}$ ó si $x = -n$, con $n \in \mathbb{N}$.*

La idea de la construcción de estos nuevos números es pensar a cada entero como una diferencia de naturales, es decir, como $m - n$ siendo m, n dos naturales cualesquiera. Como en $\mathbb{N}$ no hemos definido la operación resta, pensaremos $m - n$ como un par ordenado $(m, n) \in \mathbb{N} \times \mathbb{N}$. Así, dados dos pares ordenados $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$, si pensamos el par (a, b) como $a - b$ y el par (c, d) como $c - d$, entonces si queremos que sean iguales haremos $a - b = c - d$. Pero como no hemos definido una resta en $\mathbb{N}$, expresaremos la anterior igualdad de la siguiente forma: $a + d = c + b$, empleando así sólo operaciones definidas en $\mathbb{N}$. Con esto como motivación podemos introducir la siguiente relación en $\mathbb{N} \times \mathbb{N}$:

$$(a, b) \sim (c, d) \Leftrightarrow a + d = c + b.$$

Proposición 2.7. *La relación anterior en $\mathbb{N} \times \mathbb{N}$ es una relación de equivalencia.*

Demostración: Veamos para ello que la relación cumple con las propiedades reflexiva, simétrica y transitiva.

Es reflexiva, ya que, dado un par ordenado $(a, b) \in \mathbb{N} \times \mathbb{N}$, $a + b = a + b$ claramente, luego $(a, b) \sim (a, b)$.

Es simétrica, ya que si tenemos dos pares ordenados $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$ tales que $(a, b) \sim (c, d)$ entonces $a + d = c + b$, y leyéndolo al revés tendremos que $c + b = a + d$ y así $(c, d) \sim (a, b)$.

Finalmente es transitiva. Dados tres pares ordenados $(a, b), (c, d), (e, f) \in \mathbb{N} \times \mathbb{N}$ tales que $(a, b) \sim (c, d)$ y $(c, d) \sim (e, f)$, entonces $a + d = c + b$ y $c + f = e + d$. Sumamos f en la primera igualdad y b en la segunda y tenemos $a + d + f = c + b + f$

y $c+f+b = e+d+b$, ahora por la conmutatividad de la suma llegamos a que $a+d+f = e+d+b$ y nuevamente por la conmutatividad y la propiedad cancelativa de la suma tenemos que $a+f = e+b$, es decir, $(a,b) \sim (e,f)$.

□

Como bien sabemos, una relación de equivalencia define unas clases, y si consideramos estas clases entonces llegaremos a un nuevo conjunto, el de los *números enteros*:

Definición 2.8. *Dada una relación de equivalencia sim tal que* $(a,b) \sim (c,d) \Leftrightarrow a+d = c+b$ *con* $a,b,c,d \in \mathbb{N}$*, entonces el conjunto cociente* $\mathbb{N}\times\mathbb{N}/\sim$ *lo denotaremos* $\mathbb{Z}$ *y a sus elementos, que son clases de equivalencia de pares ordenados* $(a,b) \in \mathbb{N}\times\mathbb{N}$*, los denominaremos* ***números enteros****.*

Es decir, hemos construido el conjunto de los números enteros $\mathbb{Z}$ como el conjunto cociente del producto cartesiano de $\mathbb{N}$ por la relación de equivalencia *sim* que hemos detallado anteriormente. A sus elementos, que ya sabemos que serán de la forma n ó $-n$ con un n natural, los denotaremos en ocasiones mediante $[a,b]$.

Veamos ahora cuál es su estructura algebraica, para ello primero tendremos que definir una serie de operaciones que podemos realizar sobre este conjunto que acabamos de definir y comprobar qué propiedades tienen:

En el conjunto cociente $\mathbb{Z} = \mathbb{N}\times\mathbb{N}/\sim$ se tienen operaciones de suma y producto de enteros, definidas como sigue: dadas dos clases $[a,b],[c,d] \in \mathbb{Z}$ escojemos respectivos representantes $(a,b) \in [a,b], (c,d) \in [c,d]$. Definamos las operaciones suma y producto.

Suma. Elegidos los representantes tenemos:

$$(a,b)+(c,d) = (a+c, b+d),$$

y tomamos la clase de equivalencia $[a+c, b+d] \in \mathbb{Z}$.

Producto. Elegidos los representantes tenemos:

$$(a,b)\cdot(c,d) = (ac+bd, ad+bc).$$

Para ver esto más claro la idea es pensar (a,b) y (c,d) como $a-b$ y $c-d$ respectivamente de tal forma que $(a-b)\cdot(c-d) = (ac+bd)-(ad+bc)$. Después, tomamos la clase de equivalencia $[ac+bd, ad+bc] \in \mathbb{Z}$. Será bastante usual omitir el $\cdot$ para indicar la operación.

Veamos ahora que estas operaciones están bien definidas, es decir, que da igual los representantes que elijamos de cada clase para tener una suma y un producto como los anteriores:

Proposición 2.9. *Si* $(a,b) \sim (a',b')$ *y* $(c,d) \sim (c',d')$*, entonces*

1. $(a+c, b+d) \sim (a'+c', b'+d')$.
2. $(ac+bd, ad+bc) \sim (a'c'+b'd', a'd'+b'c')$.

Demostración: Veámoslos por partes:

1. Por hipótesis $a + b' = a' + b$ y $c + d' = c' + d$. Entonces $(a + c) + (b' + d') = (a + b') + (c + d') = (a' + b) + (c' + d) = (a' + c') + (b + d)$, es decir, $(a + c, b + d) \sim (a' + c', b', d')$.

2. Nuevamente, por las hipótesis tenemos que $a+b' = a'+b$ y $c+d' = c'+d$, ahora mutiplicando la primera por d queda $ad + b'd = a'd + bd$ y si multiplicamos por c tenemos $ac + b'c = a'c + bc$. Multiplicando la segunda por a' tenemos $a'c + a'd' = a'c' + a'd$ y multiplicandola por b' tenemos $b'c + b'd' = b'c' + b'd$. Tenemos las cuatro igualdades siguientes:

$$\begin{aligned} bd + a'd &= ad + b'd \\ ac + b'c &= a'c + bc \\ a'c + a'd' &= a'c' + a'd \\ b'd + b'c' &= b'c + b'd' \end{aligned}$$

si las sumamos tenemos: $(ac + bd) + (a'd' + b'c') + (a'd + b'c + a'c + b'd) = (ad + bc) + (a'c' + b'd') + (b'd + a'c + a'd + b'c)$, y cancelando el tercer término tenemos que $(ac+bd)+(a'd'+b'c') = (a'c'+b'd')+(ad+bc)$, que es la igualdad que buscábamos.

□

Es decir, este resultado nos dice que las operaciones

$$\begin{array}{rccc} +: & \mathbb{Z} \times \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & ([a, b], [c, d]) & \longmapsto & [a + c, b + d] \end{array}$$

$$\begin{array}{rccc} \cdot: & \mathbb{Z} \times \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & ([a, b], [c, d]) & \longmapsto & [ac + bd, ad + bc] \end{array}$$

están bien definidas en $\mathbb{Z}$. Veamos ahora cuáles son sus propiedades para poder estudiar su estructura algebraica.

Lema 2.9.1. *Sean $a, b \in \mathbb{N}$. Entonces:*

1. $(a, a) \sim (b, b)$.
2. $(a + 1, a) \sim (b + 1, b)$.

Demostración:

1. $a + b = b + a$ por la conmutatividad de la suma.
2. $a + 1 + b = b + 1 + a$ por la asociatividad y la conmutatividad de la suma.

□

Teorema 2.10. *Las operaciones suma y producto de $\mathbb{Z}$ satisfacen las siguientes propiedades:*

1. *La suma es asociativa, es decir, para cualesquiera $[a, b], [c, d], [e, f] \in \mathbb{Z}$ tenemos que*
$$[a, b] + ([c, d] + [e, f]) = ([a, b] + [c, d]) + [e, f].$$

2. *La suma es conmutativa, es decir, para todo* $[a,b],[c,d] \in \mathbb{Z}$ *tenemos que*

$$[a,b]+[c,d]=[c,d]+[a,b].$$

3. *Existe un elemento neutro para la suma, llamado cero y denotado por* $0 \in \mathbb{Z}$ *tal que*

$$[a,b]+0=[a,b] \quad \forall [a,b] \in \mathbb{Z}.$$

4. *Cada elemento* $[a,b] \in \mathbb{Z}$ *tiene inverso aditivo, es decir, para todo* $[a,b] \in \mathbb{Z}$ *existe un* $[a',b'] \in \mathbb{Z}$ *tal que* $[a,b]+[a',b']=0$.

5. *El producto es asociativo, es decir, para cualesquiera* $[a,b],[c,d],[e,f] \in \mathbb{Z}$ *se tiene que*

$$[a,b]([c,d][e,f])=([a,b][c,d])[e,f].$$

6. *El producto es conmutativo, es decir, para todo* $[a,b],[c,d] \in \mathbb{Z}$ *se tiene que*

$$[a,b][c,d]=[c,d][a,b].$$

7. *Existe un elemento neutro para el producto, denominado uno y denotado* $1 \in \mathbb{Z}$ *tal que*

$$1 \cdot [a,b]=[a,b]\cdot=[a,b] \quad \forall [a,b] \in \mathbb{Z}.$$

8. *Se cumple la ley distributiva del producto respecto de la suma, es decir, para todo* $[a,b],[c,d],[e,f] \in \mathbb{Z}$ *se tiene*

$$[a,b]([c,d]+[e,f])=[a,b][c,d]+[a,b][e,f].$$

Demostración: Ya sabemos que $\mathbb{Z}$ es cerrado con respecto a la suma y el producto.

1. Para la asociatividad de la suma sean $[a,b],[c,d],[e,f] \in \mathbb{Z}$, entonces

$$[a,b]+([c,d]+[e,f])=[a,b]+[c+e,d+f]=[a+(c+e),b+(d+f)]=$$
$$[(a+c)+e,(b+d)+f]=[a+c,b+d]+[e,f]=([a,b]+[c,d])+[e,f].$$

2. Para la conmutatividad de la suma, sean $[a,b],[c,d] \in \mathbb{Z}$:

$$[a,b]+[c,d]=[a+c,b+d]=[c+a,d+b]=[c,d]+[a,b].$$

3. Para ver el neutro aditivo hay que tener en cuenta que un neutro aditivo de $\mathbb{Z}$ es de la forma $[s,s]$, con $s \in \mathbb{N}$, ya que para cualquier $[a,b] \in \mathbb{Z}$ se tiene

$$[a,b]+[s,s]=[a+s,b+s]=[a,b],$$

dónde la última igualdad es porque $(a+s,b+s) \sim (a,b)$. A la clase $[s,s]$ la denotamos por 0.

4. Para los inversos aditivos, el inverso aditivo (porque es único, aunque eso lo veremos más adelante) para un $[a,b] \in \mathbb{Z}$ es de la forma $[b,a]$ ya que

$$[a,b] + [b,a] = [a+b, b+a] = [a+b, a+b] = [s,s] = 0,$$

donde tenemos en cuenta que $(m,m) \sim (n,n)$ para cualesquiera naturales m, n. Denotaremos al inverso aditivo de $[a,b]$ por $-[a,b] = [b,a]$.

5. Para la asociatividad del producto, sean $[a,b], [c,d], [e,f] \in \mathbb{Z}$, entonces:

$$[a,b]([c,d][e,f]) = [a,b]([ce+df, cf+de]) = [a(ce+df)+b(cf+de), a(cf+de)+b(ce+df)] = [ace+adf+bcf+bde, acf+ade+bce+bdf] = [e(ac+bd)+f(ad+bc), e(ad+bc)+f(ac+bd)] = [ac+bd, ad+bc][e,f] = ([a,b][c,d])[e,f]$$

6. Para la conmutatividad del producto, sean $[a,b], [c,d] \in \mathbb{Z}$, entonces:

$$[a,b][c,d] = [ac+bd, ad+bc] = [ca+db, da+cb] = [ca+db, cb+da] = [c,d][a,b].$$

7. Para el elemento neutro del producto, el neutro multiplicativo de $\mathbb{Z}$ es la clase $[s+1, s]$ para cualquier $s \in \mathbb{N}$, ya que para cualquier $[a,b] \in \mathbb{Z}$ tenemos:

$$[a,b][s+1,s] = [a(s+1)+bs, as+b(s+1)] = [as+a+bs, as+bs+b] = [a,b],$$

donde sabemos que $(a,b) \sim (a+t, b+t)$ con $t \in \mathbb{N}$.

8. Para ver la propiedad distributiva del producto respecto de la suma, sean $[a,b], [c,d], [e,f] \in \mathbb{Z}$, entonces:

$$[a,b]([c,d]+[e,f]) = [a,b][c+e, d+f] = [a(c+e)+b(d+f), a(d+f)+b(c+e)] = [ac+ae+bd+bf, ad+af+bc+be] = [(ac+bd)+(ae+bf), (ad+bc)+(af+be)] = [ac+bd, ad+bc] + [ae+bf, af+be] = [a,b][c,d] + [a,b][e,f].$$

□

Es decir, vemos que las propiedades se cumplen para $\mathbb{Z}$ porque en esencia se cumplen para $\mathbb{N}$, así $\mathbb{Z}$ hereda de manera natural estas operaciones suma y producto. Pero ahora veremos que $\mathbb{Z}$ nos permite incorporar una ventaja fundamental con respecto a $\mathbb{N}$, y es que nos permitirá definir la operación opuesta, como hemos visto en cuanto a la existencia de elementos inversos aditivos, a la suma, la resta.

Al neutro aditivo de $\mathbb{Z}$ lo denotaremos por 0. Es el único elemento de $\mathbb{Z}$ que satisface que

$$a + 0 = a \quad \forall a \in \mathbb{Z}.$$

Además, este elemento es único, es decir, si $0'$ es otro elemento neutro entonces

$$a + 0 = a = a + 0',$$

y de aquí por la propiedad cancelativa de la suma $0 = 0'$. Al inverso aditivo de $a \in \mathbb{Z}$ lo denotaremos por $-a$. Este elemento es el único elemento de $\mathbb{Z}$ tal que

$$a + (-a) = 0 \quad \forall a \in \mathbb{Z}.$$

Es único, ya que si a' es otro inverso aditivo entonces

$$a + (-a) = 0 = a + a'$$

y de aquí por la propiedad cancelativa de la suma $-a = a'$. Por último, al neutro multiplicativo de $\mathbb{Z}$ lo denotaremos por 1 y es el único elemento de $\mathbb{Z}$ de que cumple

$$a \cdot 1 = a \quad \forall a \in \mathbb{Z},$$

ya que si $1'$ es otro elemento neutro multiplicativo, entonces $1 = 1 \cdot 1' = 1'$. Así, podemos llegar a dar una definición de lo que es $\mathbb{Z}$ desde el punto de vista algebraico:

Definición 2.11. *Un conjunto A con dos operaciones, suma $(+)$ y producto $(\cdot)$ bien definidas que satisfaga todas las propiedades del teorema anterior, a excepción de la conmutatividad del producto y la existencia del elemento neutro multiplicativo, se dice que es un* ***anillo****. Si el anillo $(A, +, \cdot)$ satisface la conmutatividad el producto diremos que es un* ***anillo conmutativo****. Si cumple la existencia del elemento neutro para el producto, 1, entonces diremos que es un* ***anillo unitario****.*

Con esto, podemos decir que $(\mathbb{Z}, +, \cdot)$ es un ***anillo conmutativo y unitario****. Lo denominaremos* ***anillo de los enteros****.*

Definición 2.12. *Si un anillo conmutativo y unitario cumple además la propiedad cancelativa para el producto, es decir, que $ab = ac$ implique que $b = c$ con $a, b, c \in \mathbb{Z}$, entonces diremos que es un* ***dominio de integridad****.*

A partir de ahora siempre trabajaremos con anillos conmutativos y unitarios.

Como todos los elementos de un anillo A tienen inverso aditivo, se puede definir una operación de ***resta*** en A: dados $a, b \in A$, entonces definiremos la resta como sigue:

$$a - b = a + (-b) \in A,$$

con $-b$ el inverso aditivo de b.

Además el anillo de los enteros cumple las siguientes propiedades aritméticas:

Proposición 2.13. *Dados $a, b \in \mathbb{Z}$. Entonces:*

1. $a \cdot 0 = 0$.
2. $a(-b) = (-a)b = -(ab)$.
3. $(-a)(-b) = ab$.
4. $(-1)a = -a$.

La relación de orden de $\mathbb{N}$ se puede extender también a $\mathbb{Z}$.

Definición 2.14. *Dados dos números enteros cualesquiera a, b, escribiremos $a \leq b$ y diremos que a es* ***menor o igual que*** *b (o que b es* ***mayor o igual que****, $b \geq a$) cuando $b = a + p$ para algún natural p.*

Igualmente escribiremos $a < b$ (ó $b > a$) para expresar que a es ***estrictamente menor*** *que b, es decir, que $b = a + p$, con p algún natural distinto de 0, es decir, con $p \in \mathbb{N}^+$.*

Podremos escribir

$$-\mathbb{N} = \{n \in \mathbb{Z} : n < 0\}.$$

Además, el orden en $\mathbb{Z}$ cumple las siguientes propiedades:

Proposición 2.15. *Dados a, b, p enteros cualesquiera, se tiene que:*

1. *$a \leq a$, $\forall a$ (propiedad reflexiva).*
2. *Si $a \leq b$ y $b \leq a$, entonces $a = b$ (propiedad antisimétrica).*
3. *Si $a \leq b$ y $b \leq p$, entonces $a \leq p$ (propiedad transitiva).*
4. *Siempre se tiene que $a \leq b$ ó $b \leq a$ (orden total).*

Sin embargo, no va a ser válido un principio de buena ordenación como ocurre en $\mathbb{N}$, ya que el anillo de los enteros $\mathbb{Z}$ no tiene un elemento mínimo, pues para cada $a \in \mathbb{Z}$ tenemos que $a - 1 < a$. Pero sí vamos a tener una propiedad análoga para ciertos subconjuntos:

Proposición 2.16 (***Principio de buena ordenación de los conjuntos minorados***)**.** *Todo conjunto no vacío de números enteros acotado inferiormente posee un elemento mínimo. Es decir, dado $S \subseteq \mathbb{Z}$ no vacío tal que para algún $k \in \mathbb{Z}$ se tiene $k \leq n$ para todo $n \in S$, existe un elemento m en S tal que $m \leq n$ para todo $n \in S$.*

Análogamente con el máximo:

Proposición 2.17 (***Principio del máximo***)**.** *Todo conjunto no vacío de números enteros acotado superiormente posee un elemento máximo. Es decir, dado $S \subseteq \mathbb{Z}$ no vacío tal que para algún $k \in \mathbb{Z}$ se tiene $k \geq n$ para todo $n \in S$, existe un elemento $m \in S$ tal que $m \geq n$ para todo $n \in S$.*

Sin embargo, en $\mathbb{Z}$ no se cumple el principio de inducción sino una propiedad similar, aunque más débil:

Proposición 2.18. *Un conjunto de números enteros que contenga un número k y que con cada n contenga a $n+1$, debe contener a todos los números enteros mayores o iguales que k. Es decir, dado $S \subseteq \mathbb{Z}$ tal que $k \in S$ y $n+1 \in S$ siempre que $n \in S$, se tiene $\{n \in \mathbb{Z} : k \leq n\} \subseteq S$.*

3. Combinatoria

4. Grafos

4.1. Generalidades

Definición 4.1. *Un **grafo no dirigido** es un par $G = (V, E)$, donde V es un conjunto finito, a cuyos elementos denominaremos **vértices** ó **nodos**, y E es un conjunto de pares no ordenados de vértices que denominaremos **ejes** ó **aristas**.*

Llamaremos ***orden*** *de un grafo y lo denotaremos por n al número de vértices,* $n = |V|$*, y* ***tamaño*** *del grafo G al número de ejes,* $m = |E|$*.*

Normalmente se usan los símbolos $v_1, \ldots, v_i, \ldots, v_n$ para denotar los vértices, y la notación (v_i, v_j) para denotar los ejes, pero también es equivalente usar $i, j, \ldots$ en lugar de $v_i, v_j, \ldots$ y la notación (i, j) en lugar de (v_i, v_j).

Notar que como hemos dicho que son pares no ordenados entonces el par (i, j) es el mismo par que (j, i). En ocasiones también usaremos $e_1, \ldots, e_m$ para los ejes, pero sólo cuando no nos interesen los vértices que forman ese par.

Definición 4.2. *Dado un eje* (i, j)*, diremos que dicho eje une i con j, y que éstos son sus* ***extremos****. También diremos que i y j son* ***adyacentes*** *ó* ***vecinos****, y que el eje* (i, j) *es* ***incidente*** *a i.*

Notar que cuando en un eje tengamos (i, i), con i un vértice, diremos que ese eje es un **bucle**.

Cuando en un grafo G permitimos que en el conjunto de ejes aparezcan pares repetidos diremos que G es un ***multigrafo no dirigido***.

Definición 4.3. *Un grafo no dirigido, sin bucles y sin pares repetidos es llamado* ***simple****. En este caso podemos ver cada eje de E como un subconjunto de V que consta de dos elementos.*

Aunque un grafo es una estructura abstracta, siempre se ha utilizado una representación visual de esta estructura cuando trabajamos con ellas. La representación más habitual es lo que se conoce como ***trazado de un grafo***. En esta representación cada vértice del grafo corresponde a un punto y cada eje a una línea que conecta los puntos correspondientes a sus extremos. Por ejemplo:

Definición 4.4. *El* ***grado*** $d(i)$ *de un vértice i es el número de ejes incidentes con él.*

Proposición 4.5. *En cualquier grafo no dirigido sin bucles el número de vértices de grado impar es par.*

Demostración: Como cada eje es incidente a exactamente dos vértices, la suma de los grados de todos los vértices, i, es dos veces el número de ejes, m, es decir

$$\sum_{i=1}^{n} d(i) = 2m.$$

Como la suma de los grados es un número par, tiene que haber un número par de sumandos con valor impar

□

Cuando dos o más grafos sean iguales entre sí para diferenciarlos simplemente le cambiaremos el nombre a sus nodos, usando por ejemplo números o letras. Esto sólo sirve para poder diferenciar entre ambos e identificarlos, pero en realidad la estructura subyacente es la misma: decimos entonces que los grafos son isomorfos.

Definición 4.6. *Un grafo $G = (V, E)$ es **isomorfo** al grafo $G' = (V', E')$ si existe una aplicación biyectiva φ de V a V' que preserva la adyacencia, es decir, tal que si $(i, j) \in E$ si y sólo si $(\varphi(i), \varepsilon(j)) \in E'$.*

4.2. Árboles

4.3. Grafos dirigidos