# Capítulo 5

# Los números naturales y los números enteros

---

Hemos supuesto a lo largo del texto que el lector conoce, al menos intuitivamente, los números naturales, enteros, racionales y reales. Conoce como se suman, se multiplican e incluso sabe reconocer cuando un número es mayor que otro.

En este capítulo, vamos a fundamentar todas estas propiedades sobre los números naturales y enteros. Es decir, el objeto del capítulo es justificar resultados familiares y conocidos. En los ejemplos 2.5 y 3.8 hemos introducido los conjuntos de números naturales, $\mathbb{N}$, y enteros, $\mathbb{Z}$. El primer conjunto se ha introducido mediante los axiomas de Peano, mientras que los números enteros se han construido, partiendo de los números naturales, como conjunto cociente de una determinada relación de equivalencia. Para facilitar la lectura del capítulo repetiremos estas construcciones.

La idea básica de los números naturales es que sirven para contar los elementos de los conjuntos finitos y que dos conjuntos tienen el mismo número de elementos cuando existe una biyección entre ellos. Retomaremos pues el concepto de cardinal, introducido en la sección 3.4, centrándonos en los cardinales finitos y en los cardinales numerables, ambos conceptos íntimamente relacionados con la noción de número natural.

Los números naturales no forman un grupo respecto de la suma. La ecuación $b+x=a$ no tiene solución en $\mathbb{N}$ si $a<b$. Construimos el conjunto de los números enteros $\mathbb{Z}$ donde esta ecuación tendrá siempre solución. Este conjunto será una extensión del conjunto de los números naturales, en el sentido de que identificaremos $\mathbb{N}$ con un subconjunto de $\mathbb{Z}$, conservando las operaciones y el orden.

Estudiaremos los conceptos de máximo común divisor y mínimo común múltiplo vía los ideales de $\mathbb{Z}$, que aportan un método sencillo y natural para introducirlos.

## 5.1. Los números naturales

Intuitivamente se conocen los números naturales como los números que utilizamos para contar:

$$\mathbb{N} = \{0, 1, 2, 3, 4 \ldots\}$$

El cero, a veces, se excluye del conjunto de los números naturales. Nosotros utilizaremos la notación:

$$\mathbb{N}^* = \{1, 2, 3, 4 \ldots\}$$

Introducimos los números naturales mediante los axiomas de Peano que informalmente son los siguientes:

$A_1$. El elemento 0 es un número natural.

$A_2$. Todo número natural $n$ tiene un único elemento sucesor que es también un número natural.

$A_3$. 0 no es el sucesor de ningún número natural.

$A_4$. Dos números naturales cuyos sucesores son iguales, son iguales.

$A_5$. Si un conjunto de números naturales contiene al 0 y a los sucesores de cada uno de sus elementos entonces contiene a todos los números naturales.

El segundo axioma asegura que todo número natural tiene un sucesor mientras que el cuarto asegura que si dos números naturales son distintos, sus respectivos sucesores son distintos. Esto se traduce en la existencia de una aplicación $s\colon \mathbb{N} \longrightarrow \mathbb{N}$ (la aplicación que a cada número natural le hace corresponder su sucesor o siguiente) y que esta aplicación es inyectiva. El tercer axioma asegura que $0 \notin \mathrm{Im}(s)$ y el quinto axioma permite asegurar que el número 0 es el único elemento sin antecesor pues en caso contrario, existe $a \in \mathbb{N}$, $a \notin \mathrm{Im}(s)$ y $a \neq 0$. En este caso, el conjunto $A = \mathbb{N}\backslash\{a\}$, es un conjunto de naturales que satisface las hipótesis del quinto axioma y por tanto $\mathbb{N} \subset A$, lo cual es una contradicción. En resumen:

- Todo número natural $n \neq 0$ es el sucesor de algún número natural.

Los axiomas de Peano permiten también ver que los elementos que se van generando son distintos. En concreto:

- Para todo $n \in \mathbb{N}$, $n \neq s(n)$.

En efecto, si $A = \{n \in \mathbb{N} \mid n \neq s(n)\}$, entonces $0 \in A$ pues 0 no es el sucesor de ningún número natural y por tanto $0 \neq s(0)$. Supongamos que $n \in A$. Si $s(n) \notin A$ entonces $s(n) = s(s(n))$ y por el cuarto axioma se cumple $n = s(n)$, es decir, $n \notin A$ que es una contradicción. Por el quinto axioma se obtiene que $A = \mathbb{N}$.
Como ya habíamos observado en el ejemplo 2.5 los cinco axiomas de Peano permiten pensar en $\mathbb{N}$ como en el conjunto:

$$\mathbb{N} = \Big\{0, s(0), s\big(s(0)\big), s\Big(s\big(s(0)\big)\Big), \ldots\Big\}$$

De esta manera, cero, uno, dos, tres, etc., son las denominaciones de cero, sucesor de cero, sucesor del sucesor de cero, sucesor del sucesor del sucesor de cero, etc., y $0, 1, 2, 3$, etc., son las notaciones utilizadas para $0, s(0), s\big(s(0)\big), s\Big(s\big(s(0)\big)\Big)$, etc.

## Suma en $\mathbb{N}$

La suma de números naturales se define por recurrencia utilizando el axioma $A_5$.

**Definición 5.1** Se define por recurrencia sobre $n$ la suma $m+n$ mediante:

1. $m + 0 = m$ para todo $m \in \mathbb{N}$.
2. $m + s(n) = s(m + n)$ para todo $m, n \in \mathbb{N}$.

**Observaciones:**

1. De la definición anterior se obtiene que $m + 1 = s(m)$ para todo $m \in \mathbb{N}$ pues

$$m + 1 = m + s(0) = s(m + 0) = s(m)$$

2. También se cumple que $1 + m = s(m)$ para todo $m \in \mathbb{N}$ pues procediendo por inducción sobre $m$ se tiene:

   i) La propiedad es cierta para $m = 0$ pues $1 + 0 = 1 = s(0)$.

   ii) Supongamos que la propiedad es cierta para $m$, esto es, $1 + m = s(m)$ y veamos que es cierta para $s(m)$, esto es, $1 + s(m) = s\big(s(m)\big)$. En efecto:

$$\begin{aligned} 1 + s(m) &= s(1 + m) && \text{por definición de suma,} \\ &= s\big(s(m)\big) && \text{por la hipótesis de inducción.} \end{aligned}$$

   A partir de ahora utilizaremos indistintamente $s(m)$ o $m + 1$.

3. Dados $m, n \in \mathbb{N}$, si $m + n = 0$ entonces $m = n = 0$.
   En efecto, si $n \neq 0$ entonces existe $r \in \mathbb{N}$ tal que $n = s(r)$ y por tanto $0 = m + n = m + s(r) = s(m + r)$ en contradicción con el axioma $A_3$. En consecuencia $n = 0$ y por tanto $m = 0$.

Las propiedades básicas de esta operación están resumidas en la siguiente proposición:

**Proposición 5.2** La suma de números naturales es una operación interna en $\mathbb{N}$ que satisface, cualesquiera que sean $m, n$ y $p \in \mathbb{N}$, las siguientes propiedades:

1. *Existencia del elemento neutro:* $m + 0 = 0 + m = m$
2. *Asociativa:* $(m + n) + p = m + (n + p)$
3. *Conmutativa:* $m + n = n + m$
4. *Cancelativa:* Si $m + p = n + p$, entonces $m = n$.

**Demostración:** Las cuatro propiedades se demuestran por inducción.
1. Sólo hay que demostrar que $0 + m = m$ para todo $m \in \mathbb{N}$ pues la otra igualdad se deduce de la propia definición de la operación $+$. Por inducción sobre $m$ se tiene:

i) La propiedad es cierta para $m = 0$ pues $0 + 0 = 0$.

ii) Supongamos que la propiedad es cierta para $m$, esto es, $0 + m = m$ y veamos que es cierta para $s(m)$, esto es, $0 + s(m) = s(m)$. En efecto:

$$\begin{aligned} 0 + s(m) &= s(0 + m) && \text{por definición de suma,} \\ &= s(m) && \text{por la hipótesis de inducción.} \end{aligned}$$

2. Se procede por inducción sobre $p$.

i) La propiedad es cierta para $p = 0$ pues $(m + n) + 0 = m + n = m + (n + 0)$.

ii) Supongamos que la propiedad es cierta para $p$, esto es, $(m+n)+p = m+(n+p)$ y veamos que es cierta para $s(p)$, esto es, $(m + n) + s(p) = m + (n + s(p))$. En efecto:

$$\begin{aligned} (m + n) + s(p) &= s((m + n) + p) && \text{por definición de suma,} \\ &= s(m + (n + p)) && \text{por la hipótesis de inducción,} \\ &= m + s(n + p) && \text{por definición de suma,} \\ &= m + (n + s(p)) && \text{por definición de suma.} \end{aligned}$$

3. Procedemos por inducción sobre $n$.

i) La propiedad es cierta para $n = 0$, esto es, $m + 0 = 0 + m$. (Se deduce de la propiedad 1.)

ii) Supongamos que la propiedad es cierta para $n$, esto es, $m + n = n + m$ y veamos que es cierta para $s(n)$, esto es, $m + s(n) = s(n) + m$. En efecto

$$\begin{aligned} m + s(n) &= s(m + n) && \text{por definición de suma,} \\ &= s(n + m) && \text{por la hipótesis de inducción,} \\ &= n + s(m) && \text{por definición de suma,} \\ &= n + (1 + m) && \text{pues } 1 + m = s(m) \text{ por la observación 2,} \\ &= (n + 1) + m && \text{por la propiedad asociativa,} \\ &= s(n) + m && \text{pues } n + 1 = s(n) \text{ por la observación 1.} \end{aligned}$$

4. Procedemos por inducción sobre $p$.

i) La propiedad es cierta para $p = 0$ pues si $m + 0 = n + 0$, claramente se deduce que $m = n$.

ii) Supongamos que la propiedad es cierta para $p$, esto es, de $m + p = n + p$ se deduce que $m = n$. Veamos que de $m + s(p) = n + s(p)$, también se deduce que $m = n$. En efecto:

$$\begin{aligned} \text{Si} \quad m + s(p) &= n + s(p)\,, \\ \text{entonces} \quad s(m + p) &= s(n + p) \quad \text{por definición de suma,} \\ \text{y en consecuencia,} \quad m + p &= n + p \quad \text{pues } s \text{ es inyectiva.} \\ \text{Y por la hipótesis de inducción} \quad m &= n\,. \end{aligned}$$

□

## Producto en $\mathbb{N}$

El producto de números naturales se define por recurrencia utilizando el axioma $A_5$.

**Definición 5.3** Se define por recurrencia sobre $n$ el producto, que designaremos por $m \cdot n$ o $mn$, de los números naturales $m$ y $n$ mediante:

1. $m \cdot 0 = 0$ para todo $m \in \mathbb{N}$.
2. $m \cdot s(n) = (m \cdot n) + m$ para todo $m, n \in \mathbb{N}$.

**Observaciones:**

1. Nótese que el apartado 2 en la definición anterior se escribe también como:

$$m(n+1) = (mn) + m \quad \text{para todo} \quad m, n \in \mathbb{N}$$

2. Se obtiene que $0 \cdot m = 0$ para todo $m \in \mathbb{N}$ pues procediendo por inducción sobre $m$ se tiene:

   *a*) La propiedad es cierta para $m = 0$ pues $0 \cdot 0 = 0$.

   *b*) Supongamos que la propiedad es cierta para $m$, esto es, $0 \cdot m = 0$ y veamos que es cierta para $s(m)$, esto es, $0 \cdot s(m) = 0$. En efecto:

$$\begin{aligned} 0 \cdot s(m) &= (0 \cdot m) + 0 && \text{por definición de producto,} \\ &= 0 && \text{por la hipótesis de inducción.} \end{aligned}$$

   En otras palabras, 0 es absorbente para el producto.

3. De la definición anterior se obtiene que $m \cdot 1 = m$ para todo $m \in \mathbb{N}$ pues

$$m \cdot 1 = m \cdot s(0) = (m \cdot 0) + m = 0 + m = m$$

Resumimos las propiedades básicas del producto en la siguiente proposición:

**Proposición 5.4** El producto de números naturales es una operación interna en $\mathbb{N}$ que satisface, cualesquiera que sean $m, n$ y $p \in \mathbb{N}$, las siguientes propiedades:

1. *Existencia del elemento neutro:* $m \cdot 1 = 1 \cdot m = m$
2. *Distributiva:* $m(n+p) = mn + mp$ y $(n+p)m = nm + pm$
3. *Asociativa:* $(mn)p = m(np)$
4. *Conmutativa:* $mn = nm$
5. *Cancelativa:* Si $mp = np$ y $p \neq 0$, entonces $m = n$.

**Demostración:** Las cinco propiedades se demuestran por inducción y son análogas a las demostraciones de las propiedades de la suma. Demostraremos la primera, la segunda y la última.
1. Sólo hay que demostrar que $1 \cdot m = m$ para todo $m \in \mathbb{N}$ pues la otra igualdad es la observación 3 de la definición 5.3. Procedemos por inducción sobre $m$.

i) La propiedad es cierta para $m = 0$ pues $1 \cdot 0 = 0$.

ii) Supongamos que la propiedad es cierta para $m$, esto es, $1 \cdot m = m$ y veamos que es cierta para $s(m)$, esto es, $1 \cdot s(m) = s(m)$. En efecto:

$$\begin{aligned} 1 \cdot s(m) &= (1 \cdot m) + 1 && \text{por definición de producto,} \\ &= m + 1 = s(m) && \text{por la hipótesis de inducción.} \end{aligned}$$

En otras palabras, 1 es el elemento neutro del producto.

2. Se procede por inducción sobre $p$. Sólo demostraremos la primera propiedad distributiva.

i) La propiedad es cierta para $p = 0$ pues $m(n + 0) = mn = mn + 0 = mn + m0$.

ii) Supongamos que la propiedad es cierta para $p$, esto es, $m(n + p) = mn + mp$ y veamos que es cierta para $s(p)$, esto es, $m(n + s(p)) = mn + ms(p)$. En efecto:

$$\begin{aligned} m(n + s(p)) &= m \cdot s(n + p) && \text{por definición de suma,} \\ &= m(n + p) + m && \text{por definición de producto,} \\ &= mn + mp + m && \text{por la hipótesis de inducción,} \\ &= mn + (mp + m) = mn + m \cdot s(p) && \text{por definición de producto.} \end{aligned}$$

3. Se demuestra por inducción sobre $p$.
4. Se demuestra por inducción sobre $n$.
5. Procedemos por inducción sobre $n$.

i) La propiedad es cierta para $n = 0$. Hay que demostrar que si $mp = 0 \cdot p = 0$ y $p \neq 0$, entonces $m = 0$. Si $p \neq 0$ entonces existe $q \in \mathbb{N}$ tales que $s(q) = p$. De $mp = 0$, sustituyendo se obtiene que $ms(q) = 0$, esto es, $mq + m = 0$. De la observación 3 de la definición 5.1 se deduce que $m = 0$.

ii) Supongamos que la propiedad es cierta para $n$, esto es, que para todo $m, p \in \mathbb{N}$ de $mp = np$ y $p \neq 0$ se deduce que $m = n$. Veamos que de $mp = s(n) \cdot p$, también se deduce que $m = s(n)$. En efecto:

Observemos en primer lugar que $m \neq 0$ pues si $m = 0$, entonces $s(n) \cdot p = mp = 0$ y por tanto, de i) se deduce que $s(n) = 0$, lo que contradice el axioma $A_3$. En consecuencia $m = s(r) = r + 1$ para un cierto $r \in \mathbb{N}$.

Sustituyendo en la igualdad $mp = s(n) \cdot p$ se obtiene $(r + 1)p = (n + 1)p$, esto es $rp + p = np + p$. Por la propiedad cancelativa de la suma se obtiene que $rp = np$ y por la hipótesis de inducción se deduce que $r = n$. En consecuencia $s(r) = s(n)$, es decir, $m = s(n)$.

□

**Observación:** De las propiedades cancelativa y conmutativa del producto se deduce que si $m, p \in \mathbb{N}$ y $mp = 0$, entonces $m = 0$ o $p = 0$.

Una vez definido el producto se define la potenciación de números naturales en forma recurrente por:

**Definición 5.5** Se define la potencia $n$-ésima de $a$, $a^n$, mediante

1. $0^n = 0$ para todo $n \in \mathbb{N}^*$.
2. $a^0 = 1$ para todo $a \in \mathbb{N}^*$.
3. $a^{n+1} = a^n \cdot a$ para todo $a \in \mathbb{N}^*$ y $n \in \mathbb{N}$.

**Observaciones** 1)Si $n \in \mathbb{N}^*$ es fácil ver que $a^n = \overbrace{a \cdot a \cdot \cdots \cdot a}^{n \text{ veces}}$.
2) Hemos dejado sin definir el valor de $0^0$ pues no hay un tratamiento único al respecto y depende del contexto en el que se maneje.
En muchos contextos, donde no intervienen argumentos de continuidad, interpretar $0^0$ como 1 simplifica fórmulas y elimina a veces el tener que estudiar el caso 0 como caso especial. Es habitual por tanto usar la convención $0^0 = 1$, en teoría de conjuntos o en álgebra. Por ejemplo, en la teoría de polinomios o series de potencias las notaciones se simplifican notablemente si una constante $a$ se escribe como $ax^0$ para un $x$ arbitrario. Por ejemplo, la expresión del binomio de Newton $(1+x)^n = \sum_{i=0}^{n} \binom{n}{i} x^i$ no es válida para $x = 0$ salvo que $0^0$ se sustituya por 1. O la regla de derivación de $x^n$, $(x^n)' = nx^{n-1}$, no es válida para $n = 1$ y $x = 0$ salvo que a $0^0$ se le dé el valor 1.
Por otro lado $0^0$ debe fijarse como una indeterminación cuando se obtiene como expresión algebraica en el cálculo de límites: cuando $f$ y $g \in \mathcal{F}(\mathbb{R}, \mathbb{R})$ con $f(x) > 0$ y $\lim_{x \to a} f(x) = \lim_{x \to a} g(x) = 0$ , el límite de la función $f(x)^{g(x)}$ cuando $x$ tiende a $a$ es indeterminado, en el sentido de que, dependiendo de las funciones $f$ y $g$, el resultado puede ser cualquier número mayor o igual a 0, $+\infty$, o incluso el límite puede no existir.

De la propia definición se obtienen por inducción las siguientes propiedades de las potencias:

Para todo $(a, m, n) \in \mathbb{N}^* \times \mathbb{N} \times \mathbb{N}$, $\boxed{a^m \cdot a^n = a^{m+n}}$

Para todo $(a, m, n) \in \mathbb{N}^* \times \mathbb{N} \times \mathbb{N}$, $\boxed{\left(a^n\right)^m = a^{nm}}$

Para todo $(a, b, n) \in \mathbb{N}^* \times \mathbb{N}^* \times \mathbb{N}$, $\boxed{a^n b^n = (ab)^n}$

## Ordenación de los números naturales

**Definición 5.6** Dados $m, n \in \mathbb{N}$ se define la relación *menor o igual*, $\leqslant$, mediante:

$$m \leqslant n \quad \text{si} \quad \text{existe} \quad p \in \mathbb{N} \text{ tal que } m + p = n$$

Si $m \leqslant n$ se dice que $m$ es menor o igual que $n$.

Si $m \leqslant n$ y $m \neq n$ se dice que $m$ es estrictamente menor que $n$ y se escribe $m < n$. Observemos que dados dos elementos $m$, $n \in \mathbb{N}$ se tiene:

$$m < n \quad \text{si y sólo si} \quad \text{existe} \quad p \in \mathbb{N}^* \text{ tal que } m + p = n$$

Además se obtiene la siguiente relación: $\boxed{m < n \quad \text{si y sólo si} \quad m + 1 \leqslant n}$

En efecto, si $m < n$ entonces existe $p \in \mathbb{N}$ tal que $m + p = n$. Además $p \neq 0$ pues si $p = 0$ entonces $n = m$. Luego $p$ es el sucesor de algún número natural $r$. En consecuencia, $m + r + 1 = n$, esto es, $(m + 1) + r = n$. Por tanto $m + 1 \leqslant n$. El recíproco es inmediato pues $m < m + 1$.

Las relaciones *mayor o igual*, $\geqslant$, y *estrictamente mayor*, $>$, se definen mediante:

$n \geqslant m$, respectivamente $n > m$, si y sólo si $m \leqslant n$, respectivamente $m < n$.

**Proposición 5.7** La relación $\leqslant$ es una relación de orden total en $\mathbb{N}$, compatible con la suma y producto de números naturales, es decir para todo $m, n, p \in \mathbb{N}$ se tiene:

$$\text{si} \quad m \leqslant n \quad \text{entonces} \quad m + p \leqslant n + p \quad \text{y} \quad mp \leqslant np$$

**Demostración:** Veamos primero que la relación $\leqslant$ es una relación de orden.
Es reflexiva pues $n + 0 = n$ para todo $n \in \mathbb{N}$.
Es antisimétrica: Si $n \leqslant m$ y $m \leqslant n$ entonces existen $p, q \in \mathbb{N}$ tales que $n + p = m$ y $m + q = n$. Al sustituir $n$ en la primera igualdad se obtiene $(m + q) + p = m$,

esto es, $m + (q + p) = m + 0$ y por la propiedad cancelativa de la suma se obtiene que $q + p = 0$. De la observación 3 de la definición 5.1 se deduce que $p = 0$. En consecuencia $n = m$.
Es transitiva: Si $n \leqslant m$ y $m \leqslant r$ entonces existen $p, q \in \mathbb{N}$ tales que $n + p = m$ y $m + q = r$. Al sustituir $m$ en la segunda igualdad se obtiene $(n + p) + q = r$, esto es, $n + (p + q) = r$. En consecuencia, $n \leqslant r$.
El orden $\leqslant$ es total: Hay que ver que para todo $m, n \in \mathbb{N}$ se verifica que $m \leqslant n$ o $n \leqslant m$. Lo demostramos por inducción sobre $n$ para cualquier $m \in \mathbb{N}$.

i) La propiedad es cierta para $n = 0$ pues de $0 + m = m$ se deduce que $0 \leqslant m$.

ii) Supongamos que la propiedad es cierta para $n$, esto es, que para todo $m, n \in \mathbb{N}$ $m \leqslant n$ o $n \leqslant m$. Veamos que la propiedad es cierta para $s(n) = n + 1$, esto es, $m \leqslant n + 1$ o $n + 1 \leqslant m$.

   En efecto, si $m \leqslant n$, como $n \leqslant n + 1$, de la propiedad transitiva se tiene $m \leqslant n + 1$.

   Si $n \leqslant m$, entonces $n = m$ o $n < m$. En el primer caso $n = m$, aplicando el caso anterior o directamente, se obtiene que $m \leqslant n + 1$. Si $n < m$, entonces $n + 1 \leqslant m$.

Finalmente el orden es compatible con las operaciones. En efecto, sean $m, n, p \in \mathbb{N}$ y supongamos que $m \leqslant n$. Sea $q \in \mathbb{N}$ tal que $m + q = n$. Entonces, por un lado, $m + q + p = n + p$, esto es, $(m + p) + q = n + p$ y por tanto $m + p \leqslant n + p$. Por otro lado, $(m + q)p = np$, es decir, $mp + qp = np$ y en consecuencia $mp \leq np$.

□

Observemos que de la definición de orden que hemos dado se deduce que $\mathbb{N}$ no tiene máximo.
Finalmente estudiamos tres propiedades del orden definido en $\mathbb{N}$. Son propiedades específicas del orden de $\mathbb{N}$ que no serán ciertas ni en $\mathbb{Q}$ ni en $\mathbb{R}$ con el orden usual. La primera de ellas es la existencia de intervalos abiertos de $\mathbb{N}$ con extremos distintos que no tienen elementos. En concreto:

El intervalo abierto $(n, n + 1)_{\mathbb{N}}$ es vacío, para todo $n \in \mathbb{N}$.

**Demostración:** Recordemos que $(n, n+1)_{\mathbb{N}} = \{p \in \mathbb{N} \mid n < p < n+1\}$. Razonamos por reducción al absurdo. Sea $p \in \mathbb{N}$ tal que $n < p < n + 1$. De $n < p$ se obtiene que $n + 1 \leqslant p$ y por tanto, $n + 1 \leq p < n + 1$ que es una contradicción. □

El conjunto $\mathbb{N}$ con la relación $\leqslant$ es un conjunto bien ordenado.

**Demostración:** Tenemos que demostrar que todo subconjunto de $\mathbb{N}$, no vacío, tiene mínimo. Por reducción al absurdo, supongamos que existe $A \subset \mathbb{N}$ sin elemento mínimo. Veamos que $A = \emptyset$. Sea $U$ el conjunto de cotas inferiores de $A$:

$$U = \{n \in \mathbb{N} \mid n \leqslant a, \text{ para todo } \ a \in A\}$$

Se tiene:
1. $U \cap A = \emptyset$, pues si existiera $n \in U \cap A$, entonces $n$ sería una cota inferior de $A$ y al mismo tiempo un elemento de $A$, por tanto sería un mínimo de $A$.
2. $U = \mathbb{N}$. En efecto, se procede por inducción:

i) $0 \in U$ pues $0 \leqslant m$ para todo $m \in \mathbb{N}$, y en particular, para todo $m \in A$.

ii) Supongamos que $n \in U$ y veamos que $n + 1 \in U$. En efecto, si $n \in U$ entonces $n \leqslant a$ para todo $a \in A$. Además, como $n \notin A$ se puede asegurar que $n < a$ para todo $a \in A$. Por tanto, para todo $a \in A$ se verifica que $n + 1 \leqslant a$ y en consecuencia, $n + 1 \in U$.

□

En $\mathbb{N}$, todo subconjunto no vacío y acotado superiormente, tiene máximo.

**Demostración:** Basta observar que si $\emptyset \neq A \subset \mathbb{N}$ está acotado superiormente entonces el conjunto $U$ de las cotas superiores de $A$ es un conjunto no vacío y por tanto tiene mínimo $m = \text{mín}(U)$. Veamos que $m \in A$. Razonando por reducción al absurdo, si $m \notin A$, como $m$ es cota superior de $A$, tendríamos que $a < m$ para todo $a \in A$. Podemos deducir dos cosas:

i) $a + 1 \leqslant m$ para todo $a \in A$ y ii) $m \neq 0$ pues $A \neq \emptyset$.

De ii) se deduce que existe un número natural $n$ tal que $m = n + 1$.
Al sustituir en i) se obtiene $a + 1 \leqslant n + 1$. Es decir, para todo $a \in A$ existe $p \in \mathbb{N}$ tal que $(a + 1) + p = n + 1$. De las propiedades asociativa, conmutativa y cancelativa de la suma se obtiene que $a + p = n$ y por tanto, $a \leqslant n$ para todo $a \in A$. Por consiguiente $n$ es una cota superior de $A$. Pero $n < n + 1 = m$, y por tanto $m$ no es el mínimo de las cotas superiores de $A$ que es una contradicción. Así pues $m \in A$ y por tanto $m$ es el máximo de $A$.

□

## 5.2. Conjuntos finitos

En la sección 3.4 hemos definido el concepto de cardinal mediante la relación de equipotencia entre conjuntos; dos conjuntos son equipotentes si son biyectivos. El conjunto vacío y los conjuntos equipotentes con los intervalos cerrados $[1,n]_{\mathbb{N}}$ de $\mathbb{N}$, con $n \neq 0$, son los conjuntos finitos y para ellos se definió el cardinal mediante $\text{card}(\emptyset) = 0$ y $\text{card}(A) = n$ si $A$ es biyectivo con $[1,n]_{\mathbb{N}}$. Demostraremos la consistencia de esta definición estudiando previamente los subconjuntos finitos de $\mathbb{N}$.

**Definición 5.8** Un conjunto $A$ es **finito** si es vacío o si existe una biyección de $A$ sobre un intervalo cerrado $[1,n]_{\mathbb{N}}$ con $n \neq 0$. En caso contrario, se dice que el conjunto $A$ es **infinito**.

Estudiemos algunas propiedades de los intervalos cerrados $[1,n]_{\mathbb{N}}$ de $\mathbb{N}$.

- Si $n$ y $m \in \mathbb{N}^*$ y existe una aplicación $f\colon [1,n]_{\mathbb{N}} \longrightarrow [1,m]_{\mathbb{N}}$ inyectiva, entonces $n \leqslant m$.

**Demostración:** Procedemos por inducción sobre $n$. Para $n = 1$ la propiedad es evidente pues $m \geq 1$. Supongamos la propiedad cierta para $n$ y vemos que también se verifica para $n+1$. Sea $f\colon [1,n+1]_{\mathbb{N}} \longrightarrow [1,m]_{\mathbb{N}}$ inyectiva, y sean $p = f(n+1)$ y $M = [1,m]_{\mathbb{N}} \setminus \{p\}$. Como $m \neq 0$ entonces $m = r+1$ con $r \in \mathbb{N}$. Sea $g\colon [1,n]_{\mathbb{N}} \longrightarrow M$ la restricción de $f$ a $[1,n]_{\mathbb{N}}$, es decir la aplicación que coincide con $f$ en $[1,n]_{\mathbb{N}}$. La aplicación $g$ es también inyectiva. Sea la aplicación $h\colon M \longrightarrow [1,r]_{\mathbb{N}}$ definida de la manera siguiente:

$$h(x) = \begin{cases} x & \text{si} \quad 1 \leqslant x < p \\ a(x) & \text{si} \quad p < x \leqslant m \end{cases}$$

siendo $a(x)$ el predecesor de $x$, es decir, $a(x) + 1 = x$ que está definido ya que $x \neq 0$ pues $p < x$.

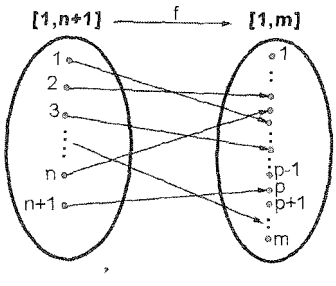



Figura 5.1: Representación de $f$

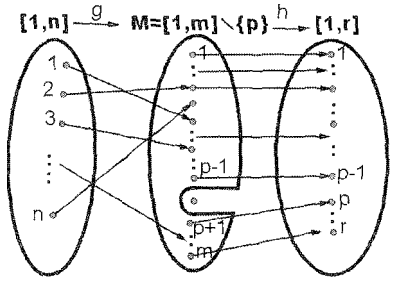



Figura 5.2: Representaciones de $h$ y $g$

La aplicación $h$ es claramente biyectiva. En consecuencia, $h \circ g\colon [1,n]_{\mathbb{N}} \longrightarrow [1,r]_{\mathbb{N}}$ es una aplicación inyectiva. Por la hipótesis de inducción $n \leqslant r$ y en consecuencia $n+1 \leqslant r+1 = m$.

□

Teniendo en cuenta que toda aplicación biyectiva y su inversa son inyectivas se obtiene el siguiente resultado.

- Si $n$ y $m \in \mathbb{N}^*$ y existe una biyección de $[1,n]_{\mathbb{N}}$ a $[1,m]_{\mathbb{N}}$, entonces $n = m$.

La siguiente proposición es consecuencia inmediata de esta propiedad y da consistencia a la definición de cardinal finito.

**Proposición 5.9** Sea $A$ un conjunto finito no vacío. Existe un único número natural $n$, no nulo, tal que $A$ y $[1,n]_{\mathbb{N}}$ son equipotentes.
Se dice entonces que $\text{card}(A) = n$.

El estudio de los subconjuntos finitos de $\mathbb{N}$ permite conocer mejor los conjuntos finitos.

- Si $n \in \mathbb{N}^*$ entonces toda aplicación inyectiva, $f\colon [1,n]_{\mathbb{N}} \longrightarrow [1,n]_{\mathbb{N}}$, es biyectiva.

**Demostración:** Procedemos por inducción sobre $n$. Para $n = 1$, sólo existe una aplicación de $[1,1]_{\mathbb{N}} = \{1\}$ en $[1,1]_{\mathbb{N}} = \{1\}$ y es biyectiva.
Supongamos que toda aplicación inyectiva, $h\colon [1,n]_{\mathbb{N}} \longrightarrow [1,n]_{\mathbb{N}}$, es biyectiva y sea $f\colon [1,n+1]_{\mathbb{N}} \longrightarrow [1,n+1]_{\mathbb{N}}$ una aplicación inyectiva. Procediendo exactamente igual que en la demostración anterior sean $p = f(n+1)$ y $M = [1,n+1]_{\mathbb{N}} \setminus \{p\}$. Sea $g\colon [1,n]_{\mathbb{N}} \longrightarrow M$ la restricción de $f$ a $[1,n]_{\mathbb{N}}$, es decir la aplicación que coincide con $f$ en $[1,n]_{\mathbb{N}}$. La aplicación $g$ es también inyectiva. Sea la aplicación $h\colon M \longrightarrow [1,n]_{\mathbb{N}}$ definida de la manera siguiente:

$$h(x) = \begin{cases} x & \text{si} \quad 1 \leqslant x < p \\ a(x) & \text{si} \quad p < x \leqslant m \end{cases}$$

siendo $a(x)$ el predecesor de $x$, es decir, $a(x)+1 = x$. El predecesor de $x$ está definido ya que $x \neq 0$ pues $p < x$. La aplicación $h$ es biyectiva. En consecuencia, la aplicación $h \circ g\colon [1,n]_{\mathbb{N}} \longrightarrow [1,n]_{\mathbb{N}}$ es inyectiva. Por la hipótesis de inducción, $h \circ g$ es biyectiva y como $g = h^{-1} \circ (h \circ g)$ resulta que $g$ es biyectiva. De la propia construcción de $g$, se deduce que $f$ es biyectiva.

□

La siguiente proposición caracteriza los subconjuntos finitos de $\mathbb{N}$.

**Proposición 5.10** Sea $A$ un subconjunto no vacío de $\mathbb{N}$. $A$ es un conjunto finito si y sólo si $A$ es un conjunto acotado superiormente.

**Demostración:** Supongamos que $A$ es un conjunto finito no vacío y sean $n = \text{card}(A)$ y $f$ una biyección de $[1,n]_{\mathbb{N}}$ sobre $A$. Demostraremos que $A$ es un conjunto acotado superiormente procediendo por inducción sobre $n$.

i) Si $n = 1$, entonces $A = \{f(1)\}$ está acotado superiormente por todos los números naturales superiores a $f(1)$.

ii) Supongamos que todo conjunto de cardinal $n$ es un conjunto acotado superiormente y supongamos que $\text{card}(A) = n+1$. Sea $f$ una biyección de $[1,n+1]_{\mathbb{N}}$ sobre $A$. Por la hipótesis de inducción $f([1,n]_{\mathbb{N}})$ está acotado superiormente y sea $S$ una cota superior de $f([1,n]_{\mathbb{N}})$. Si $p = \text{máx}(S, f(n+1))$, que existe pues la relación de orden en $\mathbb{N}$ es total, $p$ es una cota superior de $A$.

Recíprocamente, supongamos que $A$ es un conjunto acotado superiormente no vacío. Sabemos que $A$ tiene elemento máximo $m$. Para ver que $A$ es un conjunto finito procedemos por inducción sobre $m$.

i) Para $m = 0$ es cierto, ya que entonces, $A = \{0\}$, que es un conjunto finito pues es biyectivo con $[1,1]_{\mathbb{N}}$.

ii) Supongamos que todo conjunto cuyo máximo es menor o igual a $m$ es un conjunto finito, sea $A$ tal que $\text{máx}(A) = m+1$ y sea $B = A \setminus \{m+1\}$. En consecuencia, $\text{máx}(B) \leqslant m$ y por la hipótesis de inducción, $B$ es un conjunto finito y existe por tanto una biyección $g$ de $B$ sobre $[1,p]_{\mathbb{N}}$ para un cierto $p \in \mathbb{N}^*$. La extensión $f$ de $g$ a $A$ definida por $f(m+1) = p+1$ y que coincide con $g$ sobre $B$ es una biyección de $A$ sobre $[1,p+1]_{\mathbb{N}}$. Por tanto, $A$ es un conjunto finito.

□

Como corolario de esta última propiedad se obtienen fácilmente las siguientes propiedades:

- $\mathbb{N}$ es un conjunto infinito.
- Todo subconjunto de un subconjunto finito de $\mathbb{N}$ es finito.
- La unión de dos subconjuntos finitos de $\mathbb{N}$ es finito.
- El complementario de un subconjunto finito de $\mathbb{N}$ es un conjunto infinito.

Las propiedades estudiadas sobre las partes finitas de $\mathbb{N}$ se trasladan fácilmente al estudio de los conjuntos finitos.

**Proposición 5.11 Subconjuntos de un conjunto finito**
Sea $A$ un subconjunto de un conjunto finito $B$ tal que $A \neq B$. Entonces $A$ es un conjunto finito y $\text{card}(A) < \text{card}(B)$.

**Demostración:** Si $A = \emptyset$, el resultado es obvio. Si $A \neq \emptyset$, sean $n = \text{card}(B)$ y $f$ una biyección de $B$ sobre $[1,n]_{\mathbb{N}}$. El conjunto $f(A)$ es un subconjunto de $[1,n]_{\mathbb{N}}$ y es por tanto finito. Sea $g\colon A \longrightarrow f(A)$ la aplicación que coincide con $f$ en $A$ (restricción de $f$ a $A$). La aplicación $g$ es también biyectiva y por tanto $A$ es equipotente a $f(A)$. Sea $p = \text{card}(A) = \text{card}(f(A))$ y sea $h$ una biyección de $[1,p]_{\mathbb{N}}$ en $A$ y sea $i$ la inclusión natural de $A$ a $B$ definida por $i(a) = a$ para todo $a \in A$ que es inyectiva. La aplicación $j = f \circ i \circ h$,

$$[1,p]_{\mathbb{N}} \xrightarrow{h} A \xrightarrow{i} B \xrightarrow{f} [1,n]_{\mathbb{N}}$$

es inyectiva y por tanto $p \leqslant n$, esto es, $\text{card}(A) \leqslant \text{card}(B)$. Si fuera $\text{card}(A) = \text{card}(B)$ entonces la aplicación $j$ sería biyectiva y por tanto $i = f^{-1} \circ j \circ h^{-1}$ sería biyectiva y en particular $A = i(A) = B$ que contradice la hipótesis $A \neq B$. □

**Proposición 5.12** Sean $A$ un conjunto finito y $f$ una aplicación de $A$ en un conjunto cualquiera $B$. Entonces $f(A)$ es un conjunto finito y

$$\text{card}\big(f(A)\big) \leqslant \text{card}(A)$$

Además, se tiene la igualdad $\text{card}\big(f(A)\big) = \text{card}(A)$ si y sólo si $f$ es una aplicación inyectiva.

**Demostración:** Sea para todo $y \in f(A)$ el conjunto $A_y = \{x \in A \mid f(x) = y\}$ que es un subconjunto de $A$ no vacío. Tomamos un elemento fijo en cada $A_y$, que designamos por $h(y)$. Claramente, se tiene $f(h(y)) = y$. Sea el conjunto:

$$C = \{h(y) \mid y \in f(A)\} \subset A$$

$C$ es un conjunto finito pues $C$ es un subconjunto del conjunto finito $A$. Además $\text{card}(C) \leqslant \text{card}(A)$. Veamos que $C$ y $f(A)$ son equipotentes. Sea $g$ la restricción de $f$ al conjunto $C$. Esto es, $g$ es la aplicación definida por:

$$g\colon C \longrightarrow f(A) \text{ tal que } g(c) = f(c) \text{ para todo } c \in C$$

La aplicación $g$ es inyectiva pues si $c \neq c'$, existen $y, y' \in f(A)$ tales que $y \neq y'$, $c = h(y)$ y $c' = h(y')$. Pero $y = f(c) = g(c)$ e $y' = f(c') = g(c')$ y por tanto $g(c) \neq g(c')$.
Por construcción, la aplicación $g$ es claramente sobreyectiva.
En consecuencia, $\text{card}\big(f(A)\big) = \text{card}(C) \leqslant \text{card}(A)$.
Si $\text{card}\big(f(A)\big) = \text{card}(A)$ entonces $\text{card}(C) = \text{card}(A)$ y por tanto $C = A$. En consecuencia, $f$ y $g$ coinciden sobre $A$ y $f$ es inyectiva sobre $A$. Recíprocamente, si $f$ es inyectiva sobre $A$, entonces $A$ y $f(A)$ son biyectivos y por tanto, $\text{card}\big(f(A)\big) = \text{card}(A)$.

□

**Proposición 5.13** Si $f$ es una aplicación sobreyectiva de un conjunto finito $A$ en un conjunto $B$, entonces:

$$\text{card}(B) \leqslant \text{card}(A)$$

Además, se tiene la igualdad $\text{card}(B) = \text{card}(A)$ si y sólo si $f$ es una aplicación biyectiva.

**Demostración:** Si $f$ es sobreyectiva entonces $f(A) = B$ y se aplica la propiedad anterior.

□

El siguiente teorema es consecuencia inmediata de las dos últimas proposiciones.

**Teorema 5.14** Sean $A$ y $B$ dos conjuntos finitos de igual cardinal y sea una aplicación $f\colon A \longrightarrow B$. Son equivalentes:

(i) $f$ es inyectiva.
(ii) $f$ es sobreyectiva.
(iii) $f$ es biyectiva.

**Observación:** Este teorema es falso si los conjuntos $A$ y $B$ no son conjuntos finitos. Por ejemplo, las aplicaciones $f$ y $g$ de $\mathbb{N}$ en $\mathbb{N}$ tales que $f(n) = n+1$ y $g(n) = 2n$ son dos aplicaciones inyectivas, que no son sobreyectivas pues $f\big(\mathbb{N}\big) = \mathbb{N}^*$ y $g\big(\mathbb{N}\big) = 2\mathbb{N}$ siendo $2\mathbb{N}$ el conjunto de los números naturales pares. La aplicación $h$ de $\mathbb{R}$ en $\mathbb{R}$ tal que $h(x) = x^3 - x$ es una aplicación sobreyectiva que no es inyectiva.

**Proposición 5.15** Sean $A$ y $B$ dos conjuntos finitos disjuntos. Entonces, $A \cup B$ es un conjunto finito y

$$\text{card}(A \cup B) = \text{card}(A) + \text{card}(B)$$

**Demostración:** Supongamos que $A \neq \emptyset$ y $B \neq \emptyset$ pues en caso contrario la fórmula es trivial. Sean $n = \text{card(A)}$ y $f$ una biyección de $A$ sobre $[1, n]_{\mathbb{N}}$ y sean $m = \text{card}(B)$ y $g$ una biyección de $B$ sobre $[1, m]_{\mathbb{N}}$. Se define la aplicación $h$ de $A \cup B$ en $[1, n+m]_{\mathbb{N}}$ tal que

$$h(x) = \begin{cases} f(x) & \text{si } x \in A \\ n + g(x) & \text{si } x \in B \end{cases}$$

Se comprueba fácilmente que $h$ es biyectiva y por tanto $\text{card}(A \cup B) = n + m$

□

**Proposición 5.16** Sean $A$ y $B$ dos conjuntos finitos. Entonces, $A \cup B$ y $A \cap B$ son conjuntos finitos y

$$\text{card}(A \cup B) + \text{card}(A \cap B) = \text{card}(A) + \text{card}(B)$$

**Demostración:** $A \cap B$ y $B \setminus A$ son conjuntos finitos pues son subconjuntos de $B$.

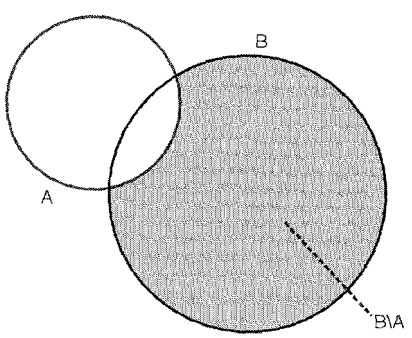



Figura 5.3: $A \cup B = A \cup (B \setminus A)$

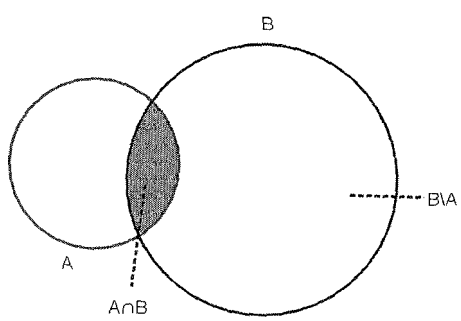



Figura 5.4: $B = (B \setminus A) \cup (A \cap B)$

Además $A \cup B = A \cup (B \setminus A)$ y $A \cap (B \setminus A) = \emptyset$. En consecuencia, $A \cup B$ es un conjunto finito y

$$\text{card}(A \cup B) = \text{card}(A) + \text{card}(B \setminus A)$$

Teniendo en cuenta que $B = (B \setminus A) \cup (A \cap B)$ y que $(B \setminus A) \cap (A \cap B) = \emptyset$ resulta que

$$\text{card}(B \setminus A) + \text{card}(A \cap B) = \text{card}(B)$$

Sumando ambas igualdades entre cardinales se obtiene

$$\text{card}(A \cup B) + \text{card}(B \setminus A) + \text{card}(A \cap B) = \text{card}(A) + \text{card}(B \setminus A) + \text{card}(B)$$

y de la propiedad cancelativa de la suma en $\mathbb{N}$ se obtiene finalmente:

$$\text{card}(A \cup B) + \text{card}(A \cap B) = \text{card}(A) + \text{card}(B)$$

□

**Proposición 5.17** Sean $A$ y $B$ dos conjuntos finitos. Entonces, $A \times B$ es un conjunto finito y

$$\text{card}(A \times B) = \text{card}(A) \cdot \text{card}(B)$$

**Demostración:** Supongamos que $A \neq \emptyset$ y $B \neq \emptyset$ pues en caso contrario la fórmula es trivial. Procedemos por *inducción sobre el cardinal de* $B$.

i) Si $\text{card}(B) = 1$ entonces $B = \{b\}$ y $A \times B = A \times \{b\}$ que es equipotente con el conjunto $A$.

ii) Supuesto que $\text{card}(A \times B') = \text{card}(A) \cdot \text{card}(B')$ para todo conjunto $B'$ tal que $\text{card}(B') = n$, sean $B$ tal que $\text{card}(B) = n + 1$ y $b \in B$. Consideramos el conjunto $B' = B \setminus \{b\}$. Como $A \times B = A \times (B' \cup \{b\}) = (A \times B') \cup (A \times \{b\})$, con $(A \times B') \cap (A \times \{b\}) = \emptyset$, por la proposición anterior y la hipótesis de inducción se obtiene:

$$\begin{aligned} \text{card}(A \times B) &= \text{card}(A \times B') + \text{card}(A \times \{b\}) \\ &= \text{card}(A) \cdot n + \text{card}(A) = \text{card}(A) \cdot (n + 1) \\ &= \text{card}(A) \cdot \text{card}(B) \end{aligned}$$

□

**Proposición 5.18** Sean $A$ y $B$ dos conjuntos finitos. Supongamos que $a = \text{card}(A) \neq 0$ y $b = \text{card}(B) \neq 0$. Entonces, el número de aplicaciones de $A$ en $B$ es $b^a$. Es decir:

$$\text{card}\left(\mathcal{F}(A,B)\right) = \text{card}\left(B^A\right) = b^a$$

**Demostración:** Se procede por inducción sobre $a$.

i) Para $a = 1$, dado que una aplicación de $A$ a $B$ está determinada por la imagen del único elemento de $A$, existen tantas aplicaciones como elementos hay en $B$, esto es $\text{card}\left(B^A\right) = b$.

ii) Supongamos que $\text{card}\left(B^A\right) = b^a$ si $\text{card}(A) = a$ y sea $A' = A \cup \{q\}$ con $q \notin A$. Así pues $\text{card}(A') = a + 1$. Veamos que $\text{card}\left(B^{A'}\right) = b^{a+1}$. En efecto, dada una aplicación de $A$ en $B$, ésta se puede extender a una aplicación de $A'$ a $B$ dando la imagen del elemento $q$. Como hay $b$ valores posibles para la imagen del elemento $q$, por cada aplicación de $A$ a $B$ obtenemos $b$ aplicaciones distintas de $A'$ a $B$. Dos extensiones a $A'$ de dos aplicaciones distintas de $A$ a $B$ son obviamente distintas. Además, cualquier aplicación de $A'$ a $B$ es una extensión de una aplicación de $A$ a $B$. Por tanto:

$$\text{card}\left(B^{A'}\right) = b \cdot \text{card}\left(B^A\right) = b \cdot b^a = b^{a+1}$$

□

**Observación:** La fórmula anterior sigue siendo cierta si $a = 0$ o $b = 0$, pero no simultáneamente nulos. Si $B = \emptyset$ y $A \neq \emptyset$ entonces $\mathcal{F}(A,\emptyset) = \emptyset$ y en consecuencia, $\text{card}\left(\mathcal{F}(A,\emptyset)\right) = 0 = 0^a$ si $a \neq 0$. Si $A = \emptyset$, entonces el conjunto $\emptyset$ es el único subconjunto del producto cartesiano $A \times B = \emptyset$, y además es una aplicación de $A$ a $B$ que se denomina aplicación vacía. En consecuencia, $\text{card}\left(\mathcal{F}(\emptyset,B)\right) = 1$.

**Ejercicio 5.19** ¿Cuántas apuestas sencillas distintas (resultados 1, $X$ y 2 en catorce encuentros de fútbol) se pueden hacer en una quiniela?
**Solución:** Basta observar que existe una biyección entre el conjunto de apuestas y el conjunto de aplicaciones del conjunto $A = \{1,2,3,\ldots,14\}$ en el conjunto $B = \{1,X,2\}$. Por tanto el número de apuestas posibles es $3^{14}$. □

**Proposición 5.20** Sea $A$ un conjunto finito. Entonces, el número de subconjuntos de $A$ es $2^{\text{card}(A)}$, es decir:

$$\text{card}\left(\mathcal{P}(A)\right) = 2^{\text{card}(A)}$$

**Demostración:** Basta observar que existe una aplicación biyectiva entre el conjunto $\mathcal{P}(A)$ de las partes del conjunto $A$ y el conjunto $\mathcal{F}(A, \{0,1\})$ de las aplicaciones de $A$ en $\{0,1\}$ que asocia a todo subconjunto $B$ de $A$ la función característica $\chi_B : A \longrightarrow \{0,1\}$ tal que $\chi_B(x) = \begin{cases} 1 & \text{si } x \in B \\ 0 & \text{si } x \in A \setminus B \end{cases}$

En consecuencia, $\text{card}\left(\mathcal{P}(A)\right) = \text{card}\left(\mathcal{F}(A,\{0,1\})\right) = 2^{\text{card}(A)}$.

□

Sean $A$ y $B$ dos conjuntos. Designamos por $\mathcal{B}(A,B)$ al conjunto de aplicaciones biyectivas de $A$ en $B$ y por $\mathcal{I}(A,B)$ al conjunto de aplicaciones inyectivas de $A$ en $B$. Si $A$ y $B$ son conjuntos finitos entonces $\mathcal{B}(A,B)$ y $\mathcal{I}(A,B)$ también lo son pues ambos son subconjuntos del conjunto finito $\mathcal{F}(A,B)$.

**Proposición 5.21** Sean $A$ y $B$ dos conjuntos finitos cuyos cardinales son $\text{card}(A) = n \neq 0$ y $\text{card}(B) = m \neq 0$ con $n \leqslant m$. Entonces el número de aplicaciones inyectivas de $A$ en $B$ es

$$\text{card}\left(\mathcal{I}(A,B)\right) = m(m-1)\cdots(m-n+1)$$

es decir, es el producto de $n$ enteros consecutivos siendo $m$ el mayor de ellos.

**Demostración:** Procedemos por inducción sobre $n$.

i) Si $n = 1$, toda aplicación de $A$ a $B$ es inyectiva y por tanto hay $m^1 = m$ aplicaciones inyectivas.

ii) Supongamos cierto para $n < m$, esto es, se verifica que $\text{card}\left(\mathcal{I}(A,B)\right) = m(m-1)\cdots(m-n+1)$. Veámoslo para $n+1$. Sea $A' = A \cup \{c\}$ con $c \notin A$ y por tanto, $\text{card}(A') = n+1$. Veamos que $\text{card}\left(\mathcal{I}(A',B)\right) = m(m-1)\cdots(m-n)$. En efecto, una aplicación inyectiva de $A$ a $B$ se puede extender a una aplicación de $A'$ a $B$ dando la imagen del elemento $c$. Como hay $n$ elementos de $B$ que ya son la imagen de algún elemento de $A$, hay $m-n$ valores posibles para la imagen del elemento $c$ y en consecuencia, por cada aplicación inyectiva de $A$ a

$B$ obtenemos $m-n$ aplicaciones inyectivas distintas de $A'$ a $B$. Dos extensiones a $A'$ de dos aplicaciones distintas de $A$ a $B$ son obviamente distintas. Además, cualquier aplicación inyectiva de $A'$ a $B$ es una extensión de una aplicación inyectiva de $A$ a $B$. Por tanto:

$$\begin{aligned} \text{card}\left(\mathcal{I}(A', B)\right) &= (m-n) \cdot \text{card}\left(\mathcal{I}(A, B)\right) \\ &= (m-n) \cdot m(m-1)\cdots(m-n+1) \\ &= m(m-1)\cdots(m-n) \end{aligned}$$

□

**Observación:** El número $m(m-1)\cdots(m-n+1)$ se denota por $V_{m,n}$ y se lee como **variaciones de $m$ sobre $n$**. Es fácil comprobar que:

$$V_{m,n} = m(m-1)\cdots(m-n+1) = \frac{m!}{(m-n)!}$$

Cuando $\text{card}(A) = \text{card}(B)$ sabemos que toda aplicación inyectiva es biyectiva. Como consecuencia inmediata se obtiene la siguiente proposición:

**Proposición 5.22** Sean $A$ y $B$ dos conjuntos finitos tales que $\text{card}(A) = \text{card}(B) = n$ . Entonces el número de aplicaciones biyectivas de $A$ sobre $B$ es:

$$\text{card}\left(\mathcal{B}(A, B)\right) = n!$$

Finalmente indicamos el número de subconjuntos de $n$ elementos que se pueden extraer de un conjunto de $m$ elementos. Hágase la demostración a modo de ejercicio.

**Proposición 5.23** Sea $A$ un conjunto finito tal que $\text{card}(A) = m$. Sea $0 \leqslant n \leqslant m$. El número de subconjuntos de $A$ que poseen exactamente $n$ elementos es:

$$\binom{m}{n}$$

**Observación:** El número $\binom{m}{n}$, que se lee **m sobre n**, se denomina **coeficiente**

**binomial** o **número combinatorio**. Se denota también por $C_{m,n}$ y se lee **combinaciones de m sobre n**.

**Ejemplo 5.24** Interpretación teórica de la fórmula $\binom{m}{n} = \binom{m}{m-n}$ si $0 \leqslant n \leqslant m$.

La fórmula anterior es evidente si se utiliza la expresión $\binom{m}{n} = \dfrac{m!}{n!(m-n)!}$.

Conceptualmente es también sencilla de establecer: la aplicación $f\colon \mathcal{P}(A) \longrightarrow \mathcal{P}(A)$ tal que $f(B) = \complement B = A \setminus B$ es una biyección. En particular, establece una biyección entre el conjunto de subconjuntos de $n$ elementos con el conjunto de subconjuntos de $m - n$ elementos.

**Ejercicio 5.25** ¿Cuántas diagonales tiene un polígono convexo de $n$ lados?
**Solución:** Cada dos vértices no consecutivos del polígono obtenemos una diagonal. Con dos vértices consecutivos se obtiene un lado del polígono. Tenemos $n$ vértices posibles. En consecuencia, el número de subconjuntos de 2 elementos que se pueden extraer del conjunto de los $n$ vértices es la suma del número $x$ de diagonales más el número $n$ de lados. Luego $x = \binom{n}{2} - n$. □

## 5.3. Conjuntos infinitos

Hemos clasificado los conjuntos en dos tipos: conjuntos finitos y conjuntos infinitos. Ya sabemos que existen conjuntos infinitos. Por ejemplo, $\mathbb{N}$ y cualquier subconjunto no acotado de $\mathbb{N}$ es un conjunto infinito. En conjuntos finitos el concepto de cardinal de un conjunto está intuitivamente asociado al número de elementos del conjunto, de manera que un subconjunto de un conjunto finito y el propio conjunto no son nunca biyectivos salvo que sean iguales (véase la proposición 5.11). Esta propiedad deja de ser cierta en los conjuntos infinitos. Así, si consideramos en $\mathbb{N}$ el conjunto $A$ de los elementos que son cuadrado de algún número natural, $A = \{0, 1, 4, 9, 16, \dots\}$, se tiene que $\operatorname{card}(A) = \operatorname{card}(\mathbb{N})$, pues la aplicación $f$ de $\mathbb{N}$ en $A$ definida por $f(n) = n^2$ es biyectiva. Es decir, que expresiones tales como "menos elementos", "más elementos", o "tantos elementos como" no pueden aplicarse de igual manera en los conjuntos finitos como en los conjuntos infinitos. De hecho si $X$ es un conjunto finito, $\operatorname{card}(X)$ se denomina también número de elementos de $X$, mientras que si $X$ es un conjunto infinito, $\operatorname{card}(X)$ se denomina número transfinito.
La primera pregunta que cabe hacerse sobre los conjuntos infinitos es si tienen todos el mismo cardinal. ¿O existen distintos cardinales infinitos? Cantor probó que existen distintos cardinales infinitos y en particular demostró que los conjuntos $\mathbb{R}$ y $\mathbb{N}$ no son equipotentes. El siguiente teorema establece la existencia de conjuntos infinitos

no biyectivos.

**Teorema 5.26** Sea $A$ un conjunto cualquiera. Entonces el conjunto $\mathcal{P}(A)$ de los subconjuntos de $A$ y el conjunto $A$ no son equipotentes.

**Demostración:** Observemos que ya sabemos que el teorema es cierto si $A$ es un conjunto finito pues $\text{card}\left(\mathcal{P}(A)\right) = 2^{\text{card}(A)} \neq \text{card}(A)$. Veamos que el teorema es cierto para cualquier conjunto $A$. Por reducción al absurdo, supongamos que los conjuntos $A$ y $\mathcal{P}(A)$ son equipotentes. En consecuencia existe una aplicación biyectiva $h\colon A \longrightarrow \mathcal{P}(A)$. Observemos que para todo $x \in A$, $h(x)$ es un subconjunto de $A$. Tiene por tanto sentido definir el conjunto $F = \{x \in A \mid x \notin h(x)\}$. En consecuencia:

$$x \in F \quad \text{si y sólo si} \quad x \notin h(x) \tag{5.1}$$

Por otro lado, como $h$ es una aplicación biyectiva de $A$ en $\mathcal{P}(A)$ y $F \in \mathcal{P}(A)$, existe un único $a \in A$ tal que $F = h(a)$. Nos planteamos la pregunta de si $a \in F$.
Si $a \in F$, de (5.1) se deduce que $a \notin h(a)$, y como $h(a) = F$, resulta que $a \notin F$.
Análogamente, si $a \notin F$, de (5.1) se deduce que $a \in h(a)$, y como $h(a) = F$, resulta que $a \in F$.
En ambos casos se llega a una contradicción. Luego no existe una biyección entre un conjunto y el conjunto de las partes de este conjunto.

□

**Definición 5.27** Un conjunto $A$ se denomina **numerable** si es equipotente con el conjunto $\mathbb{N}$.

El cardinal de cualquier conjunto numerable se denota por $\aleph_0$, que se lee *alef sub cero*. Son numerables los conjuntos $\mathbb{N}$, el conjunto de los números naturales pares, $2\mathbb{N}$, el conjunto $A$ de los elementos que son cuadrado de algún número natural, $A = \{0, 1, 4, 9, 16, \dots\}$ y $\mathbb{N}^*$. Cualquier conjunto numerable, al ser equipotente con $\mathbb{N}$, puede ponerse en la forma $\{x_n \mid n \in \mathbb{N}\}$ donde la aplicación biyectiva $f\colon \mathbb{N} \longrightarrow A$ viene definida por $f(n) = x_n$. Además como $f$ es inyectiva resulta que $x_n \neq x_m$ si $n \neq m$.
El teorema 5.26 asegura la existencia de conjuntos no numerables. Por ejemplo, $\mathcal{P}(\mathbb{N})$ no es un conjunto numerable. Incluso, se puede intuir una jerarquía infinita de conjuntos infinitos, $\mathbb{N}, \mathcal{P}(\mathbb{N}), \mathcal{P}\big(\mathcal{P}(\mathbb{N})\big), \mathcal{P}\Big(\mathcal{P}\big(\mathcal{P}(\mathbb{N})\big)\Big), \dots$

**Ejemplo 5.28** El conjunto $\{0,1\}^{\mathbb{N}}$ de las aplicaciones de $\mathbb{N}$ en $\{0,1\}$ no es numerable. Basta observar que existe una biyección entre $\mathcal{P}(\mathbb{N})$ y $\{0,1\}^{\mathbb{N}}$: la que a

todo subconjunto $A$ de $\mathbb{N}$ le asocia la función caraterística $\chi_A\colon \mathbb{N} \longrightarrow \{0,1\}$ definida por: $\chi_A(x) = \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{si } x \in \mathbb{N} \setminus A \end{cases}$

**Observación:** Algunos autores extienden la definición de conjunto numerable para incluir también a los conjuntos finitos. En ese caso se refieren a los conjuntos que aquí hemos denominado numerables como conjuntos infinitos numerables.

Como el prototipo de los conjuntos numerables es el conjunto de los números naturales, estudiamos algunas propiedades de $\mathbb{N}$ referentes a cardinalidad. Hemos visto varios ejemplos de subconjuntos de $\mathbb{N}$ que son equipotentes a $\mathbb{N}$. ¿Existe algún subconjunto infinito de $\mathbb{N}$ que no sea equipotente a $\mathbb{N}$? La respuesta es negativa:

**Proposición 5.29** Sea $A$ un subconjunto de $\mathbb{N}$. Entonces $A$ es un conjunto finito o $A$ es un conjunto numerable.

**Demostración:** Es suficiente demostrar que si $A$ es un conjunto infinito, entonces $A$ es un conjunto numerable. Definimos por inducción la aplicación $f\colon \mathbb{N} \longrightarrow A$, teniendo en cuenta que $\mathbb{N}$ es un conjunto bien ordenado y por tanto, todo subconjunto no vacío posee mínimo.

i) $f(0) = \text{mín}(A)$.

ii) Supongamos que tenemos definido $f(0), f(1), \ldots, f(n)$ entonces se define

$$f(n+1) = \text{mín}\left(A \setminus \{f(0), f(1), \ldots, f(n)\}\right)$$

La aplicación $f$ es inyectiva pues si $n < m$ entonces $f(m) \notin \{f(0), f(1), \ldots, f(n)\}$ y por tanto $f(m) \neq f(n)$.

La aplicación $f$ es sobreyectiva. Sea $a \in A$ arbitrario, veamos que existe $m \in \mathbb{N}$ tal que $f(m) = a$. En efecto, sea el subconjunto $M$ de $\mathbb{N}$ definido por:

$$M = \{\, n \in \mathbb{N} \mid a \leqslant f(n) \,\}$$

$M \neq \emptyset$ pues si fuera $M = \emptyset$, entonces $f(\mathbb{N}) \subset [0, a)$ y en consecuencia $f(\mathbb{N})$ sería un conjunto finito y $f$ no sería inyectiva. Sea $m = \text{mín}\, M$. De $m \in M$ se deduce que $a \leqslant f(m)$. Veamos que $a = f(m)$. Por reducción al absurdo, supongamos que $a \neq f(m)$. Entonces $a < f(m)$ y, como $f(m)$ era el mínimo de $A \setminus \{f(0), f(1), \ldots, f(m')\}$ siendo $m'$ tal que $m' + 1 = m$, resulta que $a \in \{f(0), f(1), \ldots, f(m')\}$. Es decir, existe $i < m$ tal que $a = f(i)$. En consecuencia $i \in M$ y $m$ no sería el mínimo de $M$. Por tanto, $a = f(m)$ y en consecuencia $f$ es sobreyectiva.

□

**Proposición 5.30** El conjunto $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ es numerable.

**Demostración:** La aplicación $f\colon \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ definida por $f(n,m) = 2^n 3^m$ para todo $n, m$ es inyectiva. En efecto, si $2^n 3^m = 2^{n'} 3^{m'}$ supongamos que $n \leqslant n'$, pues el caso $n' \leqslant n$ es análogo. Sea entonces $p \in \mathbb{N}$ tal que $n' = n + p$. Sustituyendo en la igualdad se obtiene,

$$\begin{aligned} 2^n 3^m &= 2^{n+p} 3^{m'} \\ 2^n 3^m &= 2^n 2^p 3^{m'} \text{ y por la propiedad cancelativa del producto,} \\ 3^m &= 2^p 3^{m'} \end{aligned}$$

Se deduce que $p = 0$ pues si $p \neq 0$ entonces $3^m$ sería un número par. Por tanto, $n = n'$ y $3^m = 3^{m'}$. De nuevo, suponemos $m \leqslant m'$, siendo el caso $m' \leqslant m$ análogo. Sea pues $q \in \mathbb{N}$ tal que $m' = m + q$. De $3^m = 3^{m'}$ se obtiene que $3^m = 3^m 3^q$ y por tanto, $3^q = 1$ y en consecuencia, $q = 0$. Es decir, $m = m'$. Por tanto $f$ es inyectiva. Como consecuencia de ser $f$ inyectiva, se obtiene que

$$\operatorname{card}\big(f(\mathbb{N} \times \mathbb{N})\big) = \operatorname{card}(\mathbb{N} \times \mathbb{N})$$

y como $f(\mathbb{N} \times \mathbb{N})$ es un subconjunto de $\mathbb{N}$ que es claramente infinito, de la proposición 5.29 se deduce que $f(\mathbb{N} \times \mathbb{N})$ es un conjunto numerable. Por tanto, $\mathbb{N} \times \mathbb{N}$ es un conjunto numerable.

□

**Ejemplo 5.31** De entre las posibles biyecciones que existen entre $\mathbb{N} \times \mathbb{N}$ y $\mathbb{N}$ vamos a exponer la que se utiliza en el método diagonal de Cantor.
Disponemos los elementos de $\mathbb{N} \times \mathbb{N}$ en un gráfico cartesiano y sea el conjunto:

$$A_k = \{(x,y) \in \mathbb{N} \times \mathbb{N} \mid x + y = k\}$$

$A_k$ es el conjunto de los puntos que están situados en la diagonal que parte de $(k,0)$ y llega al punto $(0,k)$. La biyección $f$ iría asignando los valores $f(0,0) = 0$, $f(1,0) = 1$ y $f(0,1) = 2$, $f(2,0) = 3$, $f(1,1) = 4$ y $f(0,2) = 5$, etc., veáse la figura 5.5. Se obtiene la biyección dada por:

$$f(n,m) = \frac{(n+m)(n+m+1)}{2} + m$$

□

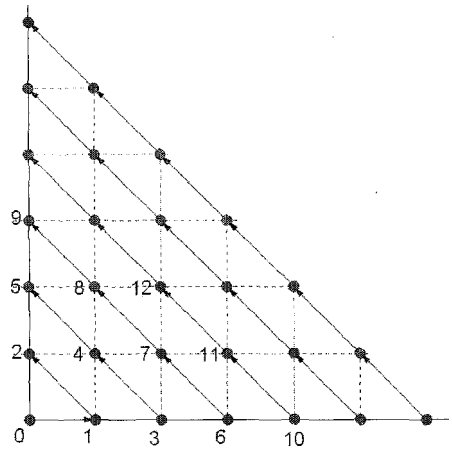



Figura 5.5: $\mathbb{N} \times \mathbb{N}$ es numerable

**Proposición 5.32** Se satisfacen las siguientes propiedades:

i) Todo subconjunto de un conjunto numerable es finito o numerable.

ii) El producto de conjuntos numerables es numerable.

iii) La unión de dos conjuntos numerables es numerable.

iv) La unión numerable de conjuntos numerables es numerable.

**Demostración:** Las propiedades i) y ii) se obtienen como consecuencias de las dos últimas proposiciones.
iii) Sean $A$ y $B$ dos conjuntos numerables.
Caso 1. Supongamos que $A \cap B = \emptyset$ y sean $f\colon \mathbb{N} \longrightarrow A$ y $g\colon \mathbb{N} \longrightarrow B$ dos aplicaciones biyectivas. La aplicación $h\colon \mathbb{N} \longrightarrow A \cup B$ tal que

$$\begin{cases} h(2n) & = f(n) \in A \\ h(2n+1) & = g(n) \in B \end{cases}$$

es biyectiva y por tanto $A \cup B$ es numerable.
Caso 2. Supongamos ahora que $A \cap B \neq \emptyset$. Como $A \cup B = A \cup (B \setminus A)$ y $A \cap (B \setminus A) = \emptyset$, distinguimos dos posibles situaciones:

a) Si $B \setminus A$ es numerable, aplicamos el caso 1 a $A$ y $(B \setminus A)$ y se obtiene que $A \cup B = A \cup (B \setminus A)$ es numerable.

b) Si $B \setminus A$ es finito, sea $p = \text{card}(B \setminus A) \in \mathbb{N}$. Si $p = 0$ entonces $B \setminus A = \emptyset$ y $A \cup B = A$ es numerable. Si $p \neq 0$, sea $p' \in \mathbb{N}$ tal que $p' + 1 = p$. Claramente los intervalos de $\mathbb{N}$, $[0, p']$ y $[1, p]$ son biyectivos. Sean $f\colon \mathbb{N} \longrightarrow A$ y $g\colon [0, p'] \longrightarrow (B \setminus A)$ dos aplicaciones biyectivas, que existen pues $A$ es numerable y $p = \text{card}(B \setminus A)$. La aplicación $h\colon \mathbb{N} \longrightarrow A \cup (B \setminus A)$ tal que

$$\begin{cases} h(n) = g(n) \in B \setminus A & \text{si } n \in [0, p'] \\ h(p + k) = f(k) \in A & \text{si } k \in \mathbb{N} \end{cases}$$

es biyectiva y en consecuencia $A \cup B = A \cup (B \setminus A)$ es numerable.
**Nota:** Hemos demostrado que la unión de un conjunto numerable y de un conjunto finito es numerable.

iv) Veamos en primer lugar que la unión numerable de conjuntos finitos o numerables disjuntos dos a dos es numerable. Supongamos pues que para todo $n \in \mathbb{N}$, $A_n \neq \emptyset$ es un conjunto finito o numerable tal que $A_n \cap A_m = \emptyset$ si $n \neq m$. Veamos que $\bigcup_{n \in \mathbb{N}} A_n$ es numerable. En efecto, si cada $A_n \neq \emptyset$ es un conjunto finito o numerable entonces, para cada $n$ existe una aplicación inyectiva $f_n\colon A_n \longrightarrow \mathbb{N}$. Además, se puede suponer sin pérdida de generalidad, que $1 \in f(A_n)$ para todo $n \in \mathbb{N}$ pues si $A_n$ es numerable, se puede tomar $f_n$ biyectiva, mientras que si $A_n \neq \emptyset$ es finito, se toma $f_n = i_n \circ g_n$ siendo $g_n\colon A_n \longrightarrow [1, \text{card}(A_n)]$ biyectiva e $i_n\colon [1, n] \longrightarrow \mathbb{N}$ la inmersión natural. Se define $h\colon \bigcup_{n \in \mathbb{N}} A_n \longrightarrow \mathbb{N}^2$ de la manera siguiente: si $a \in \bigcup_{n \in \mathbb{N}} A_n$, sea

$$h(a) = (n, f_n(a))$$

siendo $n$ el único $n \in \mathbb{N}$ tal que $a \in A_n$. La aplicación $h$ así definida es inyectiva puesto que si $h(a) = h(a')$, entonces $(n, f_n(a)) = (n', f_{n'}(a'))$, siendo $n$ y $n'$ tales que $a \in A_n$ y $a' \in A_{n'}$. En consecuencia $n = n'$ y $f_n(a) = f_{n'}(a')$, de donde $f_n(a) = f_n(a')$, y como $f_n$ es inyectiva, $a = a'$.
Como consecuencia de ser $h$ inyectiva, se obtiene que

$$\text{card}\left(h\left(\bigcup_{n \in \mathbb{N}} A_n\right)\right) = \text{card}\left(\bigcup_{n \in \mathbb{N}} A_n\right)$$

y como $h\left(\bigcup_{n \in \mathbb{N}} A_n\right)$ es un subconjunto de $\mathbb{N}^2$, se tiene que $h\left(\bigcup_{n \in \mathbb{N}} A_n\right)$ es un conjunto finito o numerable. Como además, $(n, 1) \in h\left(\bigcup_{n \in \mathbb{N}} A_n\right)$ para todo $n \in \mathbb{N}$ resulta que $h\left(\bigcup_{n \in \mathbb{N}} A_n\right)$ es un conjunto numerable y por tanto también lo es $\bigcup_{n \in \mathbb{N}} A_n$.
En el caso general, si para todo $n \in \mathbb{N}$, $A_n \neq \emptyset$ es un conjunto numerable, tomamos $B_0 = A_0$, $B_1 = A_1 \setminus A_0$, $B_2 = A_2 \setminus (A_0 \cup A_1)$, ..., $B_{n+1} = A_{n+1} \setminus (A_0 \cup A_1 \cdots \cup A_n)$. Obtenemos una familia numerable $B_n$ de conjuntos disjuntos dos a dos y tales que $\bigcup_{n \in \mathbb{N}} A_n = \bigcup_{n \in \mathbb{N}} B_n$. Sea $I = \{n \in \mathbb{N} \mid B_n \neq \emptyset\}$. $I$ es no vacío pues $0 \in I$. Si $I$ no es un conjunto finito, entonces estamos en el supuesto inicial de una unión numerable

de conjuntos no vacíos disjuntos dos a dos y finitos o numerables. Por tanto, $\bigcup_{n\in\mathbb{N}} A_n$ es numerable. Si $I$ es un conjunto finito, estamos en el supuesto de una unión finita de conjuntos finitos o numerables siendo uno de ellos, $B_0$, numerable. Aplicando iii) o la nota de la demostración de iii), se obtiene que $\bigcup_{n\in\mathbb{N}} A_n$ es numerable.

□

**Ejemplo 5.33** Los conjuntos $\mathbb{Z}$ y $\mathbb{Q}$ son numerables. En efecto, $\mathbb{Z}$ es unión de dos conjuntos numerables, $\mathbb{Z}_+ = \{x \in \mathbb{Z} \mid x \geqslant 0\}$ y $\mathbb{Z}_- = \{x \in \mathbb{Z} \mid x \leqslant 0\}$. $\mathbb{Q}_+ = \{x \in \mathbb{Q} \mid x \geqslant 0\}$ es numerable pues la aplicación $f : \mathbb{Q}_+ \longrightarrow \mathbb{N}^2$ definida por $f(x) = (p, q)$, siendo $\frac{p}{q}$ la expresión de $x$ como fracción irreducible, es una aplicación inyectiva. Por tanto, $\mathbb{Q}_+$ es equipotente con un subconjunto de $\mathbb{N}^2$, y en consecuencia es finito o numerable. Como $\mathbb{N} \subset \mathbb{Q}_+$, se obtiene que $\mathbb{Q}_+$ es numerable. La deducción de la numerabilidad de $\mathbb{Q}$ es inmediata.
Veremos en el siguiente capítulo que $\mathbb{R}$ no es numerable.

**Ejemplo 5.34** Para todo $n \in \mathbb{N}$ se define el conjunto de partes de $n$ elementos de $\mathbb{N}$,

$$\mathcal{P}_n(\mathbb{N}) = \{A \subset \mathbb{N} \mid \text{card}(A) = n\}$$

y el conjunto de las partes finitas de $\mathbb{N}$,

$$\mathcal{P}_F(\mathbb{N}) = \{A \subset \mathbb{N} \mid A \text{ es un conjunto finito}\}$$

Si $n \neq 0$, el conjunto $\mathcal{P}_n(\mathbb{N})$ es numerable.
En efecto, consideremos la aplicación $f\colon \mathcal{P}_n(\mathbb{N}) \longrightarrow \mathbb{N}^n$ tal que para todo $A \in \mathcal{P}_n(\mathbb{N})$ se define $f(A) = (a_1, a_2, \ldots, a_n)$ siendo $a_1 < a_2 < \cdots < a_n$ y $A = \{a_1, a_2, \ldots, a_n\}$. Claramente $f$ es inyectiva luego $\text{card}\,(\mathcal{P}_n(\mathbb{N})) = \text{card}\,(f\,(\mathcal{P}_n(\mathbb{N})))$. Como $f\,(\mathcal{P}_n(\mathbb{N}))$ es un subconjunto del conjunto numerable $\mathbb{N}^n$, se tiene que $\mathcal{P}_n(\mathbb{N})$ es finito o numerable y claramente es numerable (hállese una aplicación inyectiva de $\mathbb{N}$ en $\mathcal{P}_n(\mathbb{N})$).

El conjunto $\mathcal{P}_F(\mathbb{N})$ es numerable.
En efecto, basta observar que $\mathcal{P}_F(\mathbb{N}) = \bigcup_{n\in\mathbb{N}} \mathcal{P}_n(\mathbb{N})$.

## 5.4. Los números enteros

Queremos construir una ampliación del conjunto $\mathbb{N}$ donde la ecuación $b + x = a$ tenga siempre solución. El par $(a, b) \in \mathbb{N}^2$, supuesto que $b \leqslant a$, determina un único $x \in \mathbb{N}$ tal que $b + x = a$. Inversamente, existen infinidad de pares que determinan el mismo número $x$. Por ejemplo, todos los pares de la forma $(a + n, b + n)$ con $n \in \mathbb{N}$. En general, si los pares $(a, b)$ y $(a', b')$ determinan el mismo número natural $x$, se

verifica entonces: $\begin{cases} b+x &= a \\ a' &= b'+x \end{cases}$

Sumando ambas igualdades resulta que $a'+b+x = a+b'+x$. De la propiedad cancelativa de la suma en $\mathbb{N}$ se deduce que $a'+b = a+b'$. Esto lleva a definir la siguiente relación:

**Definición 5.35** En $\mathbb{N}\times\mathbb{N}$ se define la relación de equivalencia $\mathcal{E}$:

$$(a,b)\ \mathcal{E}\ (a',b') \quad \text{si y sólo si} \quad a+b' = a'+b$$

Toda clase de equivalencia es por definición un **número entero** y el conjunto de las clases de equivalencia o conjunto cociente $(\mathbb{N}\times\mathbb{N})/\ \mathcal{E}$ es el conjunto de los números enteros y se denota $\mathbb{Z}$.

Si se representa gráficamente sobre un plano, la clase de equivalencia $[(a,b)]$ del par $(a,b)$ es el conjunto de puntos de coordenadas naturales que están situados sobre la recta que pasa por el punto $(a,b)$ y que es paralela a la diagonal del primer cuadrante (véase la figura 5.6).

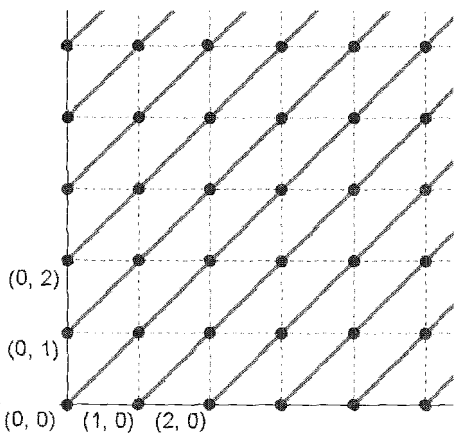



Figura 5.6: Clases de equivalencia en $\mathbb{N}\times\mathbb{N}$

Compruébese que efectivamente $\mathcal{E}$ es una relación de equivalencia sobre $\mathbb{N}\times\mathbb{N}$.
Sea $\alpha = [(a,b)] \in \mathbb{Z}$. Existe un par $(m,n)$ representante de $\alpha$ donde al menos una de las dos componentes es nula. En efecto:

Si $b \leqslant a$, existe $m \in \mathbb{N}$ tal que $b+m = a$, y por tanto $\alpha = [(m,0)]$.
Si $a < b$, existe $n \in \mathbb{N}$ tal que $a+n = b$ y por tanto $\alpha = [(0,n)]$.

Estos pares, con al menos una de las dos componentes nula, se denominan **representantes canónicos del número entero** $\alpha$.

## Operaciones en $\mathbb{Z}$

**Definición 5.36** Sean $\alpha, \beta \in \mathbb{Z}$ y sean $(a,b),(c,d) \in \mathbb{N} \times \mathbb{N}$ sendos representantes. Se definen la suma $\alpha + \beta$ y el producto $\alpha\beta$ como números enteros cuyos representantes vienen dados por:

$$\alpha + \beta = [(a+c, b+d)] \quad \text{y} \quad \alpha\beta = [(ac+bd, bc+ad)]$$

Veamos en primer lugar que las operaciones están bien definidas, o en otras palabras, que el resultado es independiente de los representantes elegidos.
Supongamos que $(a,b)\ \mathcal{E}\ (a',b')$ y que $(c,d)\ \mathcal{E}\ (c',d')$. Hay que ver que:

$$(a+c, b+d)\ \mathcal{E}\ (a'+c', b'+d') \quad \text{y} \quad (ac+bd, bc+ad)\ \mathcal{E}\ (a'c'+b'd', b'c'+a'd')$$

En efecto, si $(a,b)\ \mathcal{E}\ (a',b')$ y $(c,d)\ \mathcal{E}\ (c',d')$ entonces $a+b' = a'+b$ y $c+d' = c'+d$. Sumando ambas igualdades y utilizando las propiedades asociativa y conmutativa de la suma en $\mathbb{N}$ se obtiene $(a+c)+(b'+d') = (a'+c')+(b+d)$, esto es, $(a+c, b+d)\ \mathcal{E}\ (a'+c', b'+d')$. Luego, la definición de la suma es consistente.

Para ver que $(ac+bd, bc+ad)\ \mathcal{E}\ (a'c'+b'd', b'c'+a'd')$, se demuestra en dos pasos:

i) $(ac+bd, bc+ad)\ \mathcal{E}\ (a'c+b'd, b'c+a'd)$ pues de $a+b' = a'+b$ se deduce multiplicando por $c$ y $d$ que $(a+b')c = (a'+b)c$ y $(a'+b)d = (a+b')d$. Sumando ambas igualdades y operando utilizando las propiedades de la suma en $\mathbb{N}$ se obtiene que $(ac+bd)+(b'c+a'd) = (bc+ad)+(a'c+b'd)$, esto es, $(ac+bd, bc+ad)\ \mathcal{E}\ (a'c+b'd, b'c+a'd)$.

ii) $(a'c+b'd, b'c+a'd)\ \mathcal{E}\ (a'c'+b'd', b'c'+a'd')$: se demuestra de manera análoga.

Como consecuencia de la propiedad transitiva de la relación $\mathcal{E}$ y de i) y ii), se deduce que $(ac+bd, bc+ad)\ \mathcal{E}\ (a'c'+b'd', b'c'+a'd')$. Luego la definición del producto es consistente.

**Ejemplo 5.37** Como consecuencia de la definición de las operaciones en $\mathbb{Z}$ cuando se toman representantes canónicos se tiene:

$$[(m,0)]+[(m',0)] = [(m+m',0)] \quad \text{y} \quad [(m,0)]\cdot[(m',0)] = [(mm',0)]$$
$$[(0,n)]+[(0,n')] = [(0,n+n')] \quad \text{y} \quad [(0,n)]\cdot[(0,n')] = [(nn',0)]$$
$$[(m,0)]+[(0,n)] = [(m,n)] \quad \text{y} \quad [(m,0)]\cdot[(0,n)] = [(0,mn)]$$

En el conjunto $\mathbb{Z}$, la suma satisface las siguientes propiedades:

1. Es conmutativa.
2. Es asociativa.
3. El elemento $[(0,0)]$, denotado por 0, es el elemento neutro de la suma.
4. Todo número entero tiene elemento opuesto.

En otras palabras $(\mathbb{Z}, +)$ es un grupo conmutativo:
El opuesto del elemento $\alpha = [(a,b)]$ es el elemento $[(b,a)]$ (y que como viene siendo habitual denotamos por $-\alpha = -[(a,b)] = [(b,a)]$). En particular, cuando se toman representantes canónicos se obtiene que $-[(m,0)] = [(0,m)]$. Las propiedades asociativa y conmutativa,

$$(\alpha+\beta)+\gamma = \alpha+(\beta+\gamma) \quad \text{y} \quad \alpha+\beta = \beta+\alpha$$

de la suma se demuestran viendo en cada caso que los números enteros de cada miembro de la igualdad tienen un representante común.

En el conjunto $\mathbb{Z}$, el producto satisface las siguientes propiedades:

1. Es conmutativo.
2. Es asociativo.
3. El elemento $[(1,0)]$, denotado por 1, es el elemento neutro del producto.

También en este caso, las propiedades asociativa y conmutativa,

$$(\alpha\beta)\gamma = \alpha(\beta\gamma) \quad \text{y} \quad \alpha\beta = \beta\alpha$$

del producto se demuestran viendo en cada caso que los números enteros de cada miembro de la igualdad tienen un representante común.

Finalmente, se demuestra de manera análoga que en $\mathbb{Z}$, el producto es distributivo respecto de la suma, es decir,

4. Para todo $\alpha, \beta, \gamma \in \mathbb{Z}$, se tiene: $\alpha(\beta+\gamma) = \alpha\beta + \alpha\gamma$

Todas las propiedades enunciadas para los números enteros se resumen en el siguiente teorema:

**Teorema 5.38** $(\mathbb{Z}, +, \cdot)$ es un anillo conmutativo unitario.

De entre las propiedades que se derivan de la estructura de anillo destacamos las siguientes:

$$\alpha \cdot 0 = 0 \cdot \alpha = 0 \text{ para todo } \alpha \in \mathbb{Z}$$

En $\mathbb{Z}$ no hay divisores de cero. Es decir:

> Si $\alpha, \beta \in \mathbb{Z}$ y $\alpha\beta = 0$ entonces $\alpha = 0$ o $\beta = 0$

En efecto, utilizando representantes canónicos de $\alpha$ y $\beta$ se puede asegurar, véase el ejemplo 5.37, que $\alpha\beta$ es de la forma $\alpha\beta = [(mn, 0)]$ o $\alpha\beta = [(0, mn)]$, siendo $m, n \in \mathbb{N}$. En consecuencia si $\alpha\beta = 0$ entonces $mn = 0$. Utilizando la observación que se deduce de la proposición 5.4, se obtiene $m = 0$ o $n = 0$. Esto es, $\alpha = 0$ o $\beta = 0$.

## Orden en $\mathbb{Z}$

Se definen en $\mathbb{Z}$ dos subconjuntos, el subconjunto $\mathbb{Z}_+$ de los números enteros positivos y el subconjunto $\mathbb{Z}_-$ de los números enteros negativos:

$$\mathbb{Z}_+ = \{[(m, 0)] \in \mathbb{Z} \mid m \in \mathbb{N}\} \quad \text{y} \quad \mathbb{Z}_- = \{[(0, n)] \in \mathbb{Z} \mid n \in \mathbb{N}\}$$

Se comprueba fácilmente que $[(a, b)] \in \mathbb{Z}_+$ si $a \geqslant b$ mientras que $[(a, b)] \in \mathbb{Z}_-$ si $a \leqslant b$. Además:

$$\mathbb{Z}_+ \cup \mathbb{Z}_- = \mathbb{Z} \quad \text{y} \quad \mathbb{Z}_+ \cap \mathbb{Z}_- = \{0\}$$

Del ejemplo 5.37 se deduce fácilmente:

- Si $\alpha, \beta \in \mathbb{Z}_+$, entonces $\alpha + \beta \in \mathbb{Z}_+$ y $\alpha\beta \in \mathbb{Z}_+$.

**Definición 5.39** Dados $\alpha, \beta \in \mathbb{Z}$, se define la relación:

$$\alpha \leqslant \beta \quad \text{si y sólo si} \quad \beta - \alpha \in \mathbb{Z}_+$$

La relación $\leqslant$ es una relación de orden total en $\mathbb{Z}$:
Es reflexiva pues $\alpha - \alpha = 0 \in \mathbb{Z}_+$.
Es antisimétrica pues si $\alpha \leqslant \beta$ y $\beta \leqslant \alpha$ entonces $\beta - \alpha \in \mathbb{Z}_+ \cap \mathbb{Z}_- = \{0\}$, es decir, $\alpha = \beta$.
Es transitiva pues si $\alpha \leqslant \beta$ y $\beta \leqslant \gamma$ entonces $\beta - \alpha \in \mathbb{Z}_+$ y $\gamma - \beta \in \mathbb{Z}_+$. En consecuencia $(\beta - \alpha) + (\gamma - \beta) = \gamma - \alpha \in \mathbb{Z}_+$ y $\alpha \leqslant \gamma$.
El orden es total pues $\mathbb{Z}_+ \cup \mathbb{Z}_- = \mathbb{Z}$.
Además el orden es compatible con la suma pues si $\alpha, \beta, \gamma \in \mathbb{Z}$, como $(\gamma + \beta) - (\gamma + \alpha) = \beta - \alpha$, resulta que $\alpha \leqslant \beta$ si y sólo si $\gamma + \alpha \leqslant \gamma + \beta$.
Por tanto se concluye:

**Teorema 5.40** $(\mathbb{Z}, +, \cdot, \leqslant)$ es un anillo totalmente ordenado.

Como en todo anillo totalmente ordenado, se define en $(\mathbb{Z}, +, \cdot, \leqslant)$ el **valor absoluto** de $\alpha \in \mathbb{Z}$ mediante

$$|\alpha| = \begin{cases} \alpha & \text{si} \quad 0 \leqslant \alpha \\ -\alpha & \text{si} \quad \alpha < 0 \end{cases}$$

donde $-\alpha$ es el elemento opuesto de $\alpha$ y el símbolo $<$ en $\alpha < 0$ indica que $\alpha \leqslant 0$ y $\alpha \neq 0$. Obsérvese que $\big|\,[(m,0)]\,\big| = [(m,0)]$ mientras que $\big|\,[(0,n)]\,\big| = [(n,0)]$.
Se satisfacen todas las propiedades de anillo estudiadas en el capítulo 4 y en particular, las propiedades de la proposición 4.37. En concreto:

- Si $\alpha \leqslant \beta$ y $\alpha' \leqslant \beta'$ entonces $\alpha + \alpha' \leqslant \beta + \beta'$.
- Si $\alpha \leqslant \beta$ entonces $-\beta \leqslant -\alpha$.
- Si $\alpha \leqslant \beta$ y $0 \leqslant \gamma$ entonces $\alpha\gamma \leqslant \beta\gamma$.
- Si $\alpha \leqslant \beta$ y $\gamma \leqslant 0$ entonces $\beta\gamma \leqslant \alpha\gamma$.
- Para todo $\alpha \in \mathbb{Z}$, $\alpha^2 \geqslant 0$.
- $|\alpha| \geqslant 0$ para todo $\alpha \in \mathbb{Z}$ y $|\alpha| = 0$ si y sólo si $\alpha = 0$.
- $|\alpha\beta| = |\alpha|\,|\beta|$ para todo $\alpha, \beta \in \mathbb{Z}$.
- $|\alpha + \beta| \leqslant |\alpha| + |\beta|$ para todo $\alpha, \beta \in \mathbb{Z}$.

## Identificación de $\mathbb{N}$ con $\mathbb{Z}_+$

Veamos que el conjunto de los números enteros constituye una ampliación del conjunto de los números naturales. Cuando decimos que $\mathbb{Z}$ es una extensión de $\mathbb{N}$, queremos decir que $\mathbb{Z}$ contiene un subconjunto ordenado isomorfo al conjunto ordenado de los números naturales, es decir, que existe una aplicación inyectiva $f : \mathbb{N} \longrightarrow \mathbb{Z}$ tal que para todo $n, n' \in \mathbb{N}$ se tiene:

1. $f(n + n') = f(n) + f(n')$
2. $f(n \cdot n') = f(n) \cdot f(n')$
3. Si $n \leqslant n'$ entonces $f(n) \leqslant f(n')$

Claramente, la aplicación

$$\begin{aligned} f: \ \mathbb{N} &\longrightarrow \mathbb{Z} \\ n &\longmapsto f(n) = [(n,0)] \end{aligned}$$

es un isomorfismo entre $\mathbb{N}$ y el subconjunto $\mathbb{Z}_+$ de $\mathbb{Z}$. Identificaremos por tanto todo elemento de $\mathbb{Z}_+$ con un elemento de $\mathbb{N}$. Así, escribiremos $n$ en lugar de $[(n,0)]$. En particular, el elemento nulo $[(0,0)]$ y el elemento unidad $[(1,0)]$, que usualmente se escriben como 0 y 1 por ser los elementos neutros de la suma y del producto en un anillo, también se escriben como 0 y 1 por la identificación anterior.
Mediante esta identificación, para todo $n \in \mathbb{N}$ se tiene:

$$-n = -[(n,0)] = [(0,n)]$$

La inclusión $\mathbb{N} \subset \mathbb{Z}$ expresa la identificación de $\mathbb{N}$ con $\mathbb{Z}_+ \subset \mathbb{Z}$ y aun siendo un abuso de lenguaje, se suele escribir habitualmente.

En la figura 5.7, hemos representado las clases de equivalencia en $\mathbb{N} \times \mathbb{N}$. Sobre el eje de abscisas se encuentran todos los puntos de la forma $(n,0)$ con $n \in \mathbb{N}$ representantes canónicos del número entero $n = [(n,0)]$ y tomaremos esos puntos como representación de los números $n = [(n,0)]$. Dado el número entero $[(0,n)] = -n$, consideramos la recta $r$ donde se encuentran todos sus representantes. Esta recta $r$ corta al eje de ordenadas en el punto $(0,n)$ y corta también al eje de abscisas. El punto de intersección de la recta $r$ con el eje de abscisas será la representación geométrica del número entero $-n$. De esta manera todos los números enteros están representados por un punto del eje de abscisas.

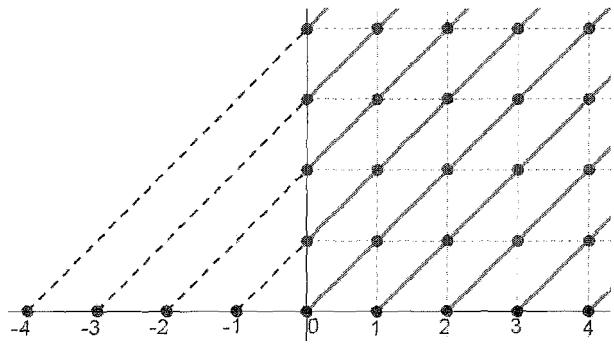



Figura 5.7: Representación lineal de $\mathbb{Z}$

Como consecuencia del isomorfismo que conserva el orden entre $\mathbb{N}$ y $\mathbb{Z}_+$, ciertas propiedades de $\mathbb{N}$ se amplían al conjunto $\mathbb{Z}$.

**Proposición 5.41**

1. Todo subconjunto de $\mathbb{Z}$ no vacío y acotado superiormente tiene máximo.
2. Todo subconjunto de $\mathbb{Z}$ no vacío y acotado inferiormente tiene mínimo.

**Demostración:** Demostramos sólo la primera parte, siendo análoga la demostración de la segunda parte. Sea $A$ un subconjunto no vacío de $\mathbb{Z}$ acotado superiormente.
Si $A \cap \mathbb{Z}_+ \neq \emptyset$, el conjunto $A \cap \mathbb{Z}_+$ considerado como subconjunto de $\mathbb{N}$ está acotado superiormente y tiene máximo que es también máximo de $A$.
Si $A \cap \mathbb{Z}_+ = \emptyset$, entonces el conjunto $-A = \{-a \mid a \in A\} \subset \mathbb{Z}_+$ y por la buena ordenación de $\mathbb{N}$, el conjunto $-A$ tiene mínimo $n$ en $\mathbb{N}$. Por tanto $-n$ es el máximo de $A$ en $\mathbb{Z}$.

□

**Proposición 5.42 Propiedad arquimediana de $\mathbb{Z}$**

Dados $\alpha, \beta \in \mathbb{Z}$ con $\alpha > 0$, existe $n \in \mathbb{N}$ tal que $n\alpha > \beta$.

**Demostración:** Si $\beta < 0$, la propiedad es cierta tomando $n = 0$, pues $0\alpha = 0 > \beta$.
Si $\beta \geqslant 0$ y $\alpha > \beta$, la propiedad es cierta tomando $n = 1$.
Si $\beta \geqslant 0$ y $\alpha \leqslant \beta$, consideremos el conjunto $A = \{k\alpha \mid k\alpha \leqslant \beta \text{ con } k \in \mathbb{N}\}$. El conjunto $A$ es no vacío pues $\alpha \in A$ y está acotado superiormente. Tiene por tanto elemento máximo $m\alpha$. En consecuencia, $(m+1)\alpha \notin A$, es decir, $(m+1)\alpha > \beta$. Tomando $n = m + 1$, se verifica la propiedad.

□

## 5.5. Máximo común divisor y mínimo común múltiplo

Muchas propiedades del conjunto de los números enteros se apoyan en lo que se denomina **división entera** también llamada **división euclídea**. La división entera es la división entre números enteros, con resto, que se estudia en Primaria.

**Teorema 5.43 División entera**
Sean $a$ y $b \in \mathbb{Z}$ tales que $b > 0$. Existen $q$ y $r \in \mathbb{Z}$ únicos tales que:

$$a = qb + r \quad \text{y} \quad 0 \leqslant r < b$$

Los números $q$ y $r$ se denominan respectivamente **cociente** y **resto** de la división entera de $a$ entre $b$.

**Demostracion:** Sea el conjunto $A = \{nb \mid nb \leqslant a \text{ con } n \in \mathbb{Z}\}$ que está acotado superiormente. Tiene por tanto elemento máximo $qb$ con $q \in \mathbb{Z}$ y además $(q+1)b \notin A$, es decir, $qb \leqslant a$ y $(q+1)b > a$. En consecuencia, tomando $r = a - qb$ se verifica que $0 \leqslant r < b$. La unicidad de $q$ y $r$ se demuestra viendo que si fuera

$$a = qb + r = q'b + r' \quad \text{con} \quad 0 \leqslant r < b \quad \text{y} \quad 0 \leqslant r' < b$$

entonces $b(q - q') = r' - r$ y $-b < r' - r < b$. Es decir, $r' - r$ es múltiplo de $b$ y $-b < r' - r < b$. En consecuencia $r' - r = 0$ que a su vez implica que $b(q - q') = 0$ y como $b \neq 0$, resulta que $q - q' = 0$. □

**Observación:** La definición anterior se extiende sin ninguna dificultad al caso $b \in \mathbb{Z}$ con $b \neq 0$. En ese caso los números $q$ y $r \in \mathbb{Z}$ cumplen:

$$a = qb + r \quad \text{y} \quad 0 \leqslant r < |b|$$

Cuando $a$ o $b$ son negativos es práctico hacer la división entera con los valores absolutos y adaptar el resultado al caso pedido. Por ejemplo,
i) Si $a = 14$ y $b = 3$, el cociente es 4 y el resto es 2 pues $14 = 4 \cdot 3 + 2$.
ii) Si $a = 14$ y $b = -3$, el cociente es $-4$ y el resto es 2 pues $14 = (-4) \cdot (-3) + 2$.
iii) Si $a = -14$ y $b = 3$, se tiene $-14 = (-4) \cdot 3 - 2$ pero $-2$ no es una cantidad positiva. Hay que sumarle el divisor, que a su vez se resta: $-14 = (-4) \cdot 3 - 3 - 2 + 3 = (-5) \cdot 3 + 1$. Luego el cociente es $-5$ y el resto es 1.
iv) Si $a = -14$ y $b = -3$ , el cociente es 5 y el resto es 1 pues en la expresión anterior $-14 = (-5) \cdot 3 + 1$ basta escribirla como $-14 = 5 \cdot (-3) + 1$.

**Ejercicio 5.44** Una consecuencia de la división entera es que permite caracterizar a todos los subgrupos de $\mathbb{Z}$. Demuestre los siguientes resultados:

1. Todo ideal de $\mathbb{Z}$ es un ideal principal. Véase la definición 4.29.
2. Sea $(G, +)$ un subgrupo de $(\mathbb{Z}, +)$, entonces existe $n \in \mathbb{N}$ tal que $G = n\mathbb{Z} = \{kn \mid k \in \mathbb{Z}\}$.

**Solución:** 1.- Sea $I$ un ideal de $\mathbb{Z}$. Hay que probar que existe $n \in \mathbb{Z}$ tal que $I = (n) = n\mathbb{Z} = \{kn \mid k \in \mathbb{Z}\}$. Comprobaremos además que se puede tomar $n \in \mathbb{N}$.

Si $I = \{0\}$ entonces $I = 0\mathbb{Z}$ y el resultado estaría probado.
Si $I \neq \{0\}$, sea $A = \{a \in I \mid a > 0\} \subset \mathbb{Z}_+$. $A$ es un conjunto no vacío que tiene mínimo $n \in \mathbb{N}^*$. Veamos que $I = (n)$. En efecto sea $a \in I$. Efectuamos la división entera de $a$ entre $n$:

$$a = qn + r \quad \text{y} \quad 0 \leqslant r < n$$

Luego, $r = a - qn$ y como $a, n \in I$ e $I$ es un ideal, resulta que $r \in I$. Pero, al ser $n$ el mínimo elemento de $I$ estrictamente positivo y $0 \leqslant r < n$, necesariamente se tiene que $r = 0$. En consecuencia, $a = qn$.
2. Demostraremos que todo subgrupo $G$ de $\mathbb{Z}$ es un ideal de $\mathbb{Z}$ y entonces aplicando la primera parte se obtiene 2.
Atendiendo a la definición 4.27 de ideal sólo tenemos que probar que si $a \in G$ y $p \in \mathbb{Z}$, entonces $pa \in G$. Además teniendo en cuenta que $(-p)a = -(pa)$, véase la proposición 4.21, y que $G$ es un subgrupo, bastará probarlo para todo $p \in \mathbb{N}$. Procedemos por inducción sobre $p$.

i) Si $p = 0$ entonces $0 \cdot a = 0 \in G$.

ii) Supongamos que $pa \in G$. Teniendo en cuenta que $(p+1)a = pa + a$, $a$ y $pa$ son elementos de $G$, y la suma es interna en $G$, resulta que $(p+1)a \in G$. □

Consideremos la relación *divide* en $\mathbb{Z}$, $b$ divide a $a$, definida por:

$$b \mid a \quad \text{si y sólo si} \quad \text{existe } q \in \mathbb{Z} \text{ tal que } a = qb$$

La relación anterior se expresa también diciendo que $b$ es un **divisor** de $a$, $a$ es **divisible** por $b$ o $a$ es un **múltiplo** de $b$.
No es una relación de orden pues no satisface la propiedad antisimétrica ya que $a \mid -a$ y $-a \mid a$ y sin embargo $a \neq -a$ si $a \neq 0$. En cambio, sí es una relación de orden cuando nos restringimos al conjunto $\mathbb{N}^*$, es decir suponemos en la definición anterior que $a, b$ y $q \in \mathbb{N}^*$.
Observe que se satisfacen las siguientes propiedades:

- 0 es divisible por cualquier número entero.
- 1 y $-1$ son divisores de cualquier número entero.
- $b \mid a$ si y sólo si $a \in b\mathbb{Z}$.
- $b \mid a$ si y sólo si $a\mathbb{Z} \subset b\mathbb{Z}$.

Con el objetivo de buscar el mínimo común múltiplo de dos números enteros, nos podemos limitar al caso $a$ y $b \in \mathbb{N}^*$ pues por un lado el único múltiplo de 0 es el mismo, y por otro lado cualquier múltiplo de $a$ es también múltiplo de $-a$.

**Teorema 5.45** Sean $a$ y $b \in \mathbb{N}^*$. Se tiene:

1. Existe un único $m \in \mathbb{N}^*$ tal que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.
2. Además, $m$ es un múltiplo común de $a$ y $b$ y si $n \in \mathbb{Z}$ es un múltiplo común de $a$ y $b$, entonces $n$ es múltiplo de $m$.

**Demostración:** 1. La demostración se deduce del hecho de ser la intersección, $a\mathbb{Z} \cap b\mathbb{Z}$, de dos ideales de $\mathbb{Z}$ un ideal de $\mathbb{Z}$. Recordemos que todos los ideales de $\mathbb{Z}$ son de la forma $m\mathbb{Z}$ con $m \in \mathbb{N}$, véase el ejercicio 5.44. Además, $a\mathbb{Z} \cap b\mathbb{Z} \neq \{0\}$ pues contiene al producto $ab \neq 0$. Por tanto, $m \neq 0$. La unicidad se deduce de que si $m$ y $m' \in \mathbb{N}$ son tales que $m\mathbb{Z} = m'\mathbb{Z}$, entonces $m \mid m'$ y $m' \mid m$ y por tanto $m = m'$.
2. Como $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$, se tiene que $m \in a\mathbb{Z}$ y $m \in b\mathbb{Z}$ y en consecuencia, $m$ es múltiplo de $a$ y de $b$. Supongamos que $n \in \mathbb{Z}$ es un múltiplo común de $a$ y $b$, entonces $n \in a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$ y por tanto $n$ es un múltiplo de $m$.

□

Del teorema anterior se deduce que $m$ es el **mínimo común múltiplo** de $a$ y $b$, y se designa por $\text{mcm}(a, b)$, $\text{MCM}(a, b)$ o $\text{m.c.m.}(a, b)$.

**Teorema 5.46** Sean $a$ y $b \in \mathbb{N}^*$. Se tiene:

1. Existe un único $d \in \mathbb{N}^*$ tal que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.
2. Además, $d$ es un divisor común de $a$ y $b$ y si $n \in \mathbb{Z}$ es un divisor común de $a$ y $b$, entonces $n$ es un divisor de $d$.

**Demostración:** 1. La demostración se deduce del hecho de ser la suma, $a\mathbb{Z} + b\mathbb{Z}$, de dos ideales de $\mathbb{Z}$ un ideal de $\mathbb{Z}$, que será por tanto principal. Sea pues $d \in \mathbb{N}^*$ tal que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. La unicidad se deduce como en el teorema anterior.
2. Como $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, se tiene que:

$$d\mathbb{Z} = \{am + bn \mid m, n \in \mathbb{Z}\}$$

En particular para $m = 1$ y $n = 0$, se obtiene que $a \in d\mathbb{Z}$ mientras que si $m = 0$ y $n = 1$ se obtiene $b \in d\mathbb{Z}$. En consecuencia, $d$ es divisor de $a$ y de $b$. Además como $d \in a\mathbb{Z} + b\mathbb{Z}$, existen $u$ y $v \in \mathbb{Z}$ tales que $d = au + bv$. Supongamos que $n \in \mathbb{Z}$ es un divisor común de $a$ y $b$, entonces $a \in n\mathbb{Z}$ y $b \in n\mathbb{Z}$. Por tanto, $d = au + bv \in n\mathbb{Z}$, es decir $n$ es un divisor de $d$.

□

Del teorema anterior se deduce que $d$ es el **máximo común divisor** de $a$ y $b$, y se designa por $\text{mcd}(a,b)$, $\text{MCD}(a,b)$ o $\text{m.c.d.}(a,b)$.

En la demostración del teorema anterior, hemos establecido la igualdad que se conoce bajo el nombre de **Identidad de Bézout**:

> Sean $a$ y $b \in \mathbb{N}^*$ y $d = \text{mcd}(a,b)$, entonces existen $u$ y $v \in \mathbb{Z}$ tales que:
>
> $$d = au + bv$$
>
> Además, $d$ es el mínimo número de $\mathbb{N}^*$ que se puede expresar en la forma $am + bn$ siendo $m$ y $n \in \mathbb{Z}$.

**Ejercicio 5.47** Sean $a, b$ y $d \in \mathbb{N}^*$. Demuestre que $d = \text{mcd}(a,b)$ si y sólo si existen $a'$ y $b' \in \mathbb{N}^*$ tales que $a = da'$ y $b = db'$ y $\text{mcd}(a',b') = 1$.
**Solución:** En efecto, supongamos que $d = \text{mcd}(a,b)$. Como $d$ es divisor de $a$ y $b$, existen $a'$ y $b' \in \mathbb{N}^*$ tales que $a = da'$ y $b = db'$. Si $d' = \text{mcd}(a',b')$, entonces $d'$ es divisor de $a'$ y $b'$ y por tanto existen $a''$ y $b'' \in \mathbb{N}^*$ tales que $a' = d'a''$ y $b' = d'b''$. En consecuencia, $a = (dd')a''$ y $b = (dd')b''$, es decir, $dd'$ es un divisor común de $a$ y $b$. Por tanto $dd'$ es un divisor de $d$ y en consecuencia $d' = 1$. En consecuencia:

$$\mathbb{Z} = a'\mathbb{Z} + b'\mathbb{Z} = \{a'm + b'n \mid m, n \in \mathbb{Z}\}$$

Por tanto,

$$d\mathbb{Z} = \{d(a'm + b'n) \mid m, n \in \mathbb{Z}\} = \{am + bn \mid m, n \in \mathbb{Z}\} = a\mathbb{Z} + b\mathbb{Z}$$

y en conclusión, $d = \text{mcd}(a,b)$. □

## Algoritmo de Euclides para hallar el mcd

Este algoritmo se basa fundamentalmente en la siguiente propiedad:
Sean $a$ y $b \in \mathbb{N}^*$, y $q$ y $r \in \mathbb{Z}$ tales que:

$$a = qb + r \quad \text{y} \quad 0 < r < b$$

Entonces, $\text{mcd}(a,b) = \text{mcd}(b,r)$.
Obsérvese en primer lugar que dados $a$ y $b \in \mathbb{N}^*$, la existencia de $q$ y $r \in \mathbb{Z}$ tales que $a = qb + r$ y $0 < r < b$ tiene lugar si y sólo si $b$ no es un divisor de $a$.
De $a = qb + r$, se deduce que todo divisor de $b$ y de $r$ es un divisor de $a$.
De $r = a - qb$, se deduce que todo divisor de $a$ y de $b$ es un divisor de $r$.

Por tanto, los divisores comunes de $a$ y $b$ coinciden con los divisores comunes de $b$ y $r$. En consecuencia, $\text{mcd}(a,b) = \text{mcd}(b,r)$.

Veamos como se calcula el $\text{mcd}(a,b)$. Supongamos $a$ y $b \in \mathbb{N}^*$ con $a > b$.
i) Si $b$ divide a $a$, entonces $\text{mcd}(a,b) = b$.
ii) Si $b$ no divide a $a$, haciendo la división entera de $a$ entre $b$, tenemos:

$$a = qb + r, \quad 0 < r < b \quad \text{y} \quad \text{mcd}(a,b) = \text{mcd}(b,r)$$

La descripción del algoritmo es la siguiente:
Pongamos $r_0 = a$, $r_1 = b$, $q_1 = q$ y $r_2 = r$ y sustituyendo:

$$r_0 = q_1 r_1 + r_2, \quad \text{mcd}(r_0, r_1) = \text{mcd}(r_1, r_2) \quad \text{y} \quad 0 < r_2 < r_1$$

Iteramos el proceso con $b$ y $r$, es decir, con $r_1$ y $r_2$.
i) Si $r_2$ divide a $r_1$ entonces $\text{mcd}(r_0, r_1) = \text{mcd}(r_1, r_2) = r_2 = r$.
ii) Si $r_2$ no divide a $r_1$ , entonces existen $q_2, r_3 \in \mathbb{N}$ tales que:

$$r_1 = q_2 r_2 + r_3, \quad \text{mcd}(r_0, r_1) = \text{mcd}(r_1, r_2) = \text{mcd}(r_2, r_3) \quad \text{y} \quad 0 < r_3 < r_2 < r_1$$

Se reitera el proceso, que se termina en un número finito de pasos pues los restos que se van obteniendo satisfacen

$$r_0 > r_1 > r_2 \cdots > 0$$

Por consiguiente, para un $k$ dado, se verifica que $r_{k+1} = 0$ y $r_k \neq 0$, en cuyo caso $r_{k-1} = q_k r_k$ y por tanto $\text{mcd}(a,b) = \text{mcd}(r_{k-1}, r_k) = r_k$.
En conclusión el máximo común divisor es el último resto no nulo en las divisiones enteras sucesivas.

**Ejemplo 5.48** Se busca el máximo común divisor de $a = 4704$ y $b = 903$. Se tiene:

$$\begin{aligned} 4704 &= 5 \cdot 903 + 189 \\ 903 &= 4 \cdot 189 + 147 \\ 189 &= 1 \cdot 147 + 42 \\ 147 &= 3 \cdot 42 + 21 \\ 42 &= 2 \cdot 21 + 0 \quad \text{es decir:} \quad \text{mcd}(4704, 903) = 21 \end{aligned}$$

Los resultados se pueden hallar y disponer sobre una tabla del tipo siguiente:

| | 4704 | 903 | 189 | 147 | 42 | 21 |
|---|---|---|---|---|---|---|
| Cociente | | 5 | 4 | 1 | 3 | 2 |
| Resto | | 189 | 147 | 42 | 21 | 0 |

**Ejemplo 5.49** Veamos un ejemplo práctico para hallar un par de elementos $u$ y $v$ que verifiquen la identidad de Bézout. Buscamos en el ejemplo anterior $u$ y $v$ tales que $4704 \cdot u + 903 \cdot v = 21$ pues $\text{mcd}(4704, 903) = 21$. En la penúltima igualdad del algoritmo de Euclides despejamos 21,

$$\begin{aligned}
21 &= 147 - 3 \cdot 42 \text{ despejamos 42 en la igualdad anterior,} \\
21 &= 147 - 3(189 - 147) = 4 \cdot 147 - 3 \cdot 189 \text{ despejamos 147 en la igualdad anterior,} \\
21 &= 4(903 - 4 \cdot 189) - 3 \cdot 189 = 4 \cdot 903 - 19 \cdot 189 \text{ despejamos 189 en la igualdad anterior.} \\
21 &= 4 \cdot 903 - 19(4704 - 5 \cdot 903) = 99 \cdot 903 - 19 \cdot 4704.
\end{aligned}$$

**Definición 5.50** Sean $a$ y $b \in \mathbb{Z}^*$, se dice que $a$ y $b$ son **primos entre sí** si $\text{mcd}(|a|, |b|) = 1$.

De la identidad de Bézout se deduce sin dificultad el siguiente teorema:

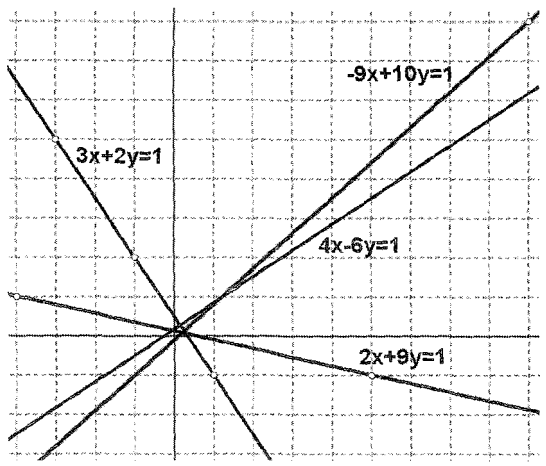



Figura 5.8: Ecuaciones en $\mathbb{Z} \times \mathbb{Z}$

**Teorema 5.51 (de Bézout)** Sean $a$ y $b \in \mathbb{N}^*$. Los números $a$ y $b$ son primos entre sí si y sólo si existen $u, v \in \mathbb{Z}$ tales que $au + bv = 1$.

Una consecuencia importante del teorema de Bézout es el siguiente resultado que se conoce como **teorema de Gauss**.

**Teorema 5.52** Si $a$ y $b$ son primos entre sí y $a$ divide a $bc$ entonces $a$ divide a $c$.

**Demostración:** Si $a$ y $b$ son primos entre sí, por el teorema de Bézout existen $u$ y $v \in \mathbb{Z}$ tales que:

$$\begin{aligned} & au + bv = 1 \\ \text{multiplicando por } c: \quad & acu + bcv = c \\ \text{como } bc = ak \text{ con } k \in \mathbb{Z}, \quad & acu + akv = c \\ & a(cu + kv) = c \\ \text{En consecuencia:} \quad & a \text{ divide a } c \end{aligned}$$

□

**Ejercicio 5.53** Demuestre que si $a$ y $b$ son primos entre sí y $k$ es tal que $a \mid k$ y $b \mid k$ entonces $ab \mid k$.
**Solución:** Si $a \mid k$, existe $n \in \mathbb{Z}$ tal que $an = k$. Por tanto, $b \mid an$ y como $\text{mcd}(a, b) = 1$, del teorema de Gauss de deduce que $b \mid n$. En consecuencia, existe $m \in \mathbb{Z}$ tal que $n = bm$. Resulta pues que $abm = k$, y se deduce que $ab \mid k$. □

**Ejercicio 5.54** Demuestre que si $\text{mcd}(a, b) = 1$ y $\text{mcd}(a, c) = 1$, entonces $a$ y $bc$ son primos entre sí.
**Solución:** Del teorema de Bézout se deduce que existen $u, v, n$ y $m \in \mathbb{Z}$ tales que $au + bv = 1$ y $an + cm = 1$. Multiplicando término a término ambas ecuaciones resulta que $(au + bv)(an + cm) = 1$, esto es, $a(aun + bvn + ucm) + bc(vm) = 1$. Utilizando el teorema de Bézout, se deduce que $a$ y $bc$ son primos entre sí. □

**Ejercicio 5.55** Halle todas las soluciones enteras de la ecuación $-5x + 3y = 1$.
**Solución:** Teniendo en cuenta que $\text{mcd}(3, 5) = 1$, se halla una solución particular de la ecuación procediendo como en el ejemplo 5.49. Se halla $x_p = 1$ e $y_p = 2$.
Se considera la ecuación $-5x + 3y = 0$. El par $(x, y)$ es solución de $-5x + 3y = 0$ si y sólo si el par $(x + x_p, y + y_p)$ es solución de $-5x + 3y = 1$. ¿Por qué?
En consecuencia, hallamos las soluciones enteras de $5x = 3y$.
De $3 \mid 5x$ y puesto que 3 y 5 son primos entre sí, el teorema de Gauss asegura que $3 \mid x$. Por tanto, $x = 3k$ con $k \in \mathbb{Z}$ y sustituyendo en $5x = 3y$, resulta que $5 \cdot (3k) = 3y$, es decir, $y = 5k$. En consecuencia, todas las soluciones enteras de la ecuación $-5x + 3y = 1$ son todos los pares $(x, y)$ que son de la forma $(1 + 3k, 2 + 5k)$ con $k \in \mathbb{Z}$. □

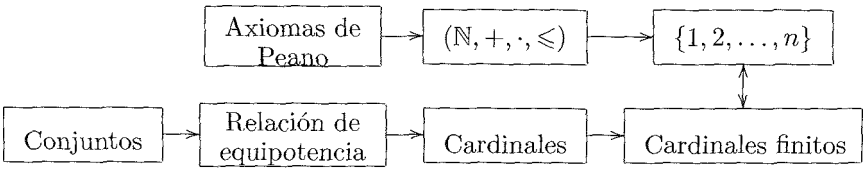
# Comentarios

## Los números naturales y los números cardinales finitos

En este capítulo hemos fundamentado el conjunto $\mathbb{N}$ de los números naturales mediante los axiomas de Peano. Nos han permitido definir dos operaciones y una relación de orden compatible con las operaciones.

En el capítulo 3, aparece el concepto de número cardinal. Son las "clases"que la relación de equipotencia establece en la colección de todos los conjuntos. Recordamos que dos conjuntos son equipotentes si existe una aplicación biyectiva de uno de ellos al otro. En los comentarios finales de los capítulos 3 y 4 hemos definido una "relación de orden" y dos "operaciones" en la colección de los números cardinales, basándonos exclusivamente en propiedades de la teoría de conjuntos.

Finalmente en la sección 5.2, hemos establecido, como definición, una correspondencia entre los subconjuntos de $\mathbb{N}$ de la forma $\{1, 2, 3, \ldots, n\}$ y los cardinales finitos. Esto es, $\mathbb{N}$ puede intuirse como el conjunto de los cardinales finitos.
En definitiva:




Veamos como partiendo de los cardinales se puede construir un modelo de $\mathbb{N}$. Para facilitar la lectura, recopilamos las definiciones y propiedades necesarias de los cardinales que ya enunciamos, en el capítulo 3 o en los comentarios de los capítulos 3 y 4, y que no hacen alusión a los números naturales.

- Conjuntos equipotentes: Dos conjuntos $A$ y $B$ tienen el mismo cardinal si existe una aplicación biyectiva de $A$ a $B$.

La relación anterior es una relación de "equivalencia" entre conjuntos. Se puede considerar que el cardinal de un conjunto $A$, $\mathrm{Card}(A)$, es la colección de todos los conjuntos que son equipotentes a $A$.
Observamos que todos los conjuntos unitarios son equipotentes. Escribimos:

- $\mathrm{Card}(\emptyset) = 0$, que se denomina número cardinal 0.
- $\mathrm{Card}(\{x\}) = 1$, que se denomina número cardinal 1.

Como $\emptyset$ y $\{x\}$ no son equipotentes, se obtiene que $0 \neq 1$.
Hemos definido los números cardinales 0 y 1 sin recurrir a los números naturales. Nuestro propósito es definir cardinal finito sin necesidad de recurrir a los números naturales. Recordemos que la suma de cardinales definida en los comentarios del capítulo anterior era:

- Si $A \cap B = \emptyset$, $a = \text{card}(A)$ y $b = \text{card}(B)$, Entonces :

$$a + b = \text{card}(A \cup B)$$

En particular, si $B = \{x\}$ y $x \notin A$ se obtiene que $a + 1 = \text{card}(A \cup \{x\})$.

**Definición 5.56** El número cardinal $a$ es finito si y sólo si $a + 1 \neq a$.

Un número cardinal no finito se denomina infinito. Asimismo, un conjunto es finito o infinito si su cardinal es respectivamente finito o infinito. En particular, 0 es un cardinal finito pues $0 \neq 1$ y $1 = 0 + 1$, y en consecuencia $0 \neq 0 + 1$. Ya se pueden definir los números naturales mediante un axioma.

**Definición 5.57** La colección de los números cardinales finitos es un conjunto que denominamos conjunto de los números naturales y que denotamos por $\mathbb{N}$.

Observamos que se verifica que $0 \in \mathbb{N}$ y por tanto el axioma $A_1$ de los axiomas de Peano. Se puede demostrar que se satisfacen los axiomas $A_2$, $A_3$ y $A_4$ de los axiomas de Peano, véase la sección 5.1, siendo $a + 1$ el sucesor de $a$. Para el lector interesado en demostrarlo, le aconsejamos seguir el siguiente esquema. Demuestre lo siguiente:

- Dados dos cardinales $a$ y $b$, si $a + 1 = b + 1$ entonces $a = b$.
- Si $a \in \mathbb{N}$ entonces $a + 1 \in \mathbb{N}$ (Razone por reducción al absurdo).
- Deduzca $A_2$ y $A_4$.
- Deduzca $A_3$ de las propiedades de la suma de cardinales (véanse los comentarios del capítulo anterior).

Si finalmente imponemos que el conjunto de los números cardinales finitos cumpla el principio de inducción o axioma $A_5$, ya podríamos desde aquí deducir todo lo hecho en este capítulo sobre $\mathbb{N}$. Tenemos definida la suma y producto de cardinales y en particular de cardinales finitos. Sólo habría que comprobar que la suma y producto de cardinales finitos son finitos que se demuestra por inducción. De hecho, las propiedades de los ejercicios 4.42 y 4.44 para cardinales restringidas a cardinales finitos son las mismas que las de las proposiciones 5.2 y 5.4. Asímismo, la relación establecida entre la suma de cardinales y la relación de orden en los cardinales en el ejercicio 4.43 ha sido la que hemos utilizado para definir la relación de orden en $\mathbb{N}$ (véase la definición 5.6).