Facultad de Ciencias Exactas, Ingeniería y Agrimensura
Departamento de Matemática - Escuela de Ciencias Exactas y Naturales
COMPLEMENTOS DE MATEMÁTICA II
Licenciatura en Ciencias de la Computación - Año 2023
Docentes: Francisco Vittone - Mauro Lucci - Delfina Martin

Unidad 2: Conjuntos ordenados.

1. Grafos dirigidos asociados a una relación.

En la Unidad anterior hemos visto como representar una relación en un conjunto finito a través de una matriz de ceros y unos. En el estudio de relaciones de orden (o preorden) resulta más util representar la relación a través de grafos dirigidos.

Definición **1.** *Sea V un conjunto finito no vacío. Un **grafo dirigido** (o **digrafo**) G sobre V está formado por los elementos de V, llamados **vértices** o **nodos** de G y un subconjunto E de $V \times V$, cuyos elementos se denominan **aristas dirigidas** o **arcos** de G. Denotamos $G = (V, E)$ un grafo dirigido cuyos vértices son los elementos de V y cuyas aristas son los elementos de E.*

*Si $(a, b) \in E$, la arista se representa gráficamente con una flecha dirigida de a hacia b. Una arista de la forma (a, a) se denomina un **lazo** en a.*

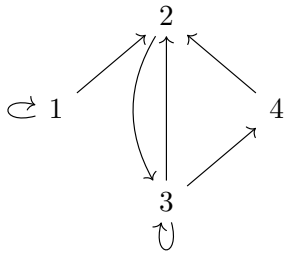
*Si $G' = (V', E')$ es un grafo dirigido tal que $V' \subseteq V$ y $E' \subseteq E$, decimos que G' es un **subgrafo** de G y lo denotamos $G' \subseteq G$.*

Definición **2.** *Si $\mathcal{R}$ es una relación en el conjunto finito no vacío A, el **grafo dirigido asociado a** $\mathcal{R}$ es aquel cuyos vértices son los elementos de A y sus aristas son los elementos de $\mathcal{R}$.*

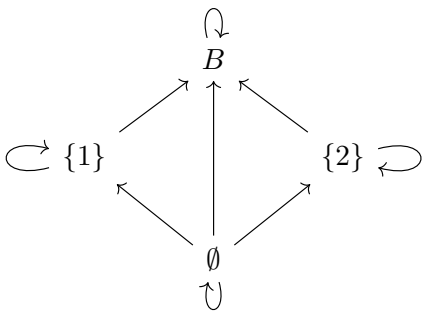
Ejemplo **1.** Consideremos $A = \{1, 2, 3, 4\}$ y $\mathcal{R}$ la relación en A cuya matriz asociada es

$$M(\mathcal{R}) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Entonces $\mathcal{R} = \{(1,1), (1,2), (2,3), (3,2), (3,3), (3,4), (4,2)\}$ y su grafo dirigido asociado es



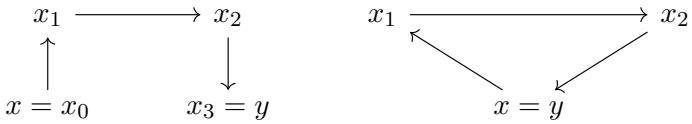
Ejemplo **2.** Consideremos el conjunto $B = \{1, 2\}$ y la relación $\mathcal{R}$ en $A = \mathcal{P}(B) = \{\emptyset, \{1\}, \{2\}, B\}$ dada por $C \mathcal{R} D$ si $C \subseteq D$. Entonces el grafo dirigido de $\mathcal{R}$ es



Definición **3.** *Sea $G = (V, E)$ un grafo dirigido y sean $x, y \in V$ dos vértices de V. Un* ***camino simple*** *de x a y es una sucesión finita de vértices $x_0 = x, x_1, \ldots, x_n = y$ tal que:*

1. *Cada vértice intermedio x_i, $i = 1, \ldots, n-1$, es distinto de x e y;*
2. *Los vértices intermedios son distintos 2 a 2, es decir, $x_i \neq x_j$ para cada $i, j \in \{1, \ldots, n-1\}$;*
3. *Existe una arista de G entre cada vértice y el siguiente, es decir, para cada $i = 1, \ldots, n$, $(x_{i-1}, x_i) \in E$.*

El número n se denomina la ***longitud*** *del camino simple. Si $x = y$, un camino simple de x a y se denomina un* ***ciclo*** *de G.*



camino simple en G *ciclo de G*

Ejemplos **3.** 1. Observando el grafo dirigido G de la relación $\mathcal{R}$ del Ejemplo 1, podemos concluir que la relación no es reflexiva, pues no hay lazos en 2 y 4. La relación tampoco es simétrica pues $(3, 4)$ es una arista de G pero $(4, 3)$ no lo es. Tampoco es antisimétrica, pues $(2, 3)$ y $(3, 2)$ son aristas de G, siendo $2 \neq 3$. Finalmente, la relación tampoco es transitiva puesto que $1, 2, 3$ es un camino simple en G, con lo cual $1 \mathcal{R} 2$ y $2 \mathcal{R} 3$, pero no hay una arista de 1 a 3 y por lo tanto $1 \not\mathcal{R} 3$.

2. Es facil concluir analizando el grafo de la relación del Ejemplo 2 que esta relación es reflexiva, antisimétrica y transitiva. Podemos generalizar estas observaciones para concluir que dada una relación $\mathcal{R}$ en un conjunto finito no vacío A cuyo grafo dirigido asociado es G, entonces

   - $\mathcal{R}$ es reflexiva, si para cada $x \in A$ existe un lazo en x.

     $\circlearrowright x \subset G$

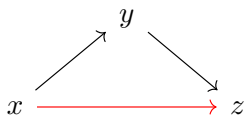
   - $\mathcal{R}$ es simétrica, si para cada arista (x, y) de G, (y, x) es una arista de G.

     $x \rightleftarrows y \subset G$

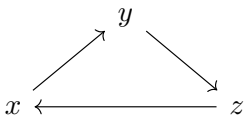
- $\mathcal{R}$ es antisimétrica si cada vez que (x, y) es una arista de G, con $x \neq y$, entonces (y, x) no es una arista de G.

$$x \longrightarrow y \ \subset G \quad \text{pero} \quad x \rightleftarrows y \ \not\subset G$$

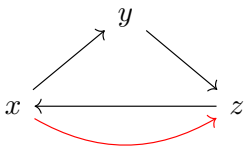
- $\mathcal{R}$ es transitiva, si para cada camino simple x, y, z de G, entonces (x, z) es una arista de de G.



Observación **1.** *Supongamos que $\mathcal{R}$ es una relación transitiva en un conjunto finito no vacío A tal que existen $x, y, z \in A$ que forman los vértices de un ciclo, esto es, el grafo dirigido de la siguiente figura es un subgrafo del grafo dirigido asociado a $\mathcal{R}$:*



Como la relación es transitiva, tendremos en realidad que el siguiente también es un subgrafo de G:



y por lo tanto

$$x \rightleftarrows z \ \subset G$$

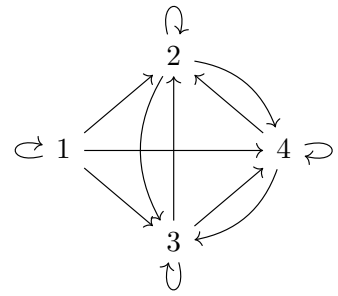
En particular, una relación transitiva en un conjunto finito cuyo grafo dirigido tiene un ciclo de longitud 3 no puede ser antisimétrica.

2. Conjuntos preordenados

Recordemos que una relación $\mathcal{R}$ en A es un **preorden** en A si $\mathcal{R}$ es reflexiva y transitiva.

Si $\mathcal{R}$ es un preorden en A, A se dice un **conjunto preordenado**. Como hemos notado en la unidad anterior, los preordenes incluyen a las relaciones de equivalencia y a las relaciones de orden. Dedicaremos a estas últimas la mayor parte de esta Unidad, pero antes recordaremos algunas relaciones importantes que son preordenes pero no son ni simétricas ni antisimétricas (y por ende no son relaciones de equivalencia ni relaciones de orden).

Ejemplo **4.** Consideremos la relación $\mathcal{R}$ en el conjunto $A = \{1, 2, 3, 4\}$ cuyo grafo dirigido asociado es

$G:$ 

Es fácil verificar a partir del grafo que $\mathcal{R}$ es una relación de preorden, que no es simétrica (pues $(1, 4) \in G$ pero $(4, 1) \notin G$) y no es antisimétrica pues es transitiva y posee al menos un ciclo de longitud 3. Verificaremos de todas maneras las propiedades reflexiva y transitiva a partir de la matriz de $\mathcal{R}$, que podemos reconstruir a partir de G (ver Ejercicio 9 de la Práctica 1). Esto puede resultar útil en grafos con mayor cantidad de vértices donde el análisis de la transtividad puede ser más complicado. En este caso, tenemos que

$$M(\mathcal{R}) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

Claramente $I_4 \leq M(\mathcal{R})$, pues posee todos 1 en la diagonal. Luego $\mathcal{R}$ es reflexiva.

Por otra parte, $M(\mathcal{R}) \cdot M(\mathcal{R}) = M(\mathcal{R})$ y por lo tanto $\mathcal{R}$ es transitiva.

Observemos que $M(\mathcal{R})^T \neq M(\mathcal{R})$ y por lo tanto $\mathcal{R}$ no es simétrica, como ya habíamos notado. Además

$$M(\mathcal{R}) * M(\mathcal{R})^T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix} \not\leq I_4$$

y por lo tanto $\mathcal{R}$ tampoco es antisimétrica.

Luego $\mathcal{R}$ es un preorden que no es ni una relación de equivalencia ni una relación de orden.

Ejemplo **5.** Consideremos en $\mathbb{Z} - \{0\}$ la relación $a \,\mathcal{R}\, b$ si $a \mid b$ (que leemos como "a *divide a* b"). Recordemos que

$$a \mid b \iff \exists\, k \in \mathbb{Z} \,:\, b = ka$$

Vimos en la Unidad 1 que $\mathcal{R}_{|\mathbb{N}}$ es una relación de orden en $\mathbb{N}$. Veremos aquí que en $\mathbb{Z} - \{0\}$ es sólo un preorden.

En efecto, con los mismos argumentos que en el item 1 de los Ejemplos 8 de la Unidad 1 se prueba que $\mathcal{R}$ es una relación reflexiva y transitiva que no es simétrica. Ahora bien, podemos observar que en $\mathbb{Z} - \{0\}$ tenemos $1 \mid -1$ y $-1 \mid 1$ pero $1 \neq -1$ (en efecto dejamos como ejercicio probar que $a \,\mathcal{R}\, b$ y $b \,\mathcal{R}\, a$ si y sólo si $a = \pm b$). Por lo tanto, a diferencia de lo que ocurre con su restricción a $\mathbb{N}$, $\mathcal{R}$ no es una relación antisimétrica en $\mathbb{Z} - \{0\}$.

Ejemplo **6.** Consideremos el conjunto $\mathcal{S}(\mathbb{R})$ formado por todas las funciones $f : \mathbb{N} \to \mathbb{R}$ (poniendo $a_n = f(n)$, suele representarse una tal función como $\{a_n\}_{n\in\mathbb{N}}$, por lo que f es la definición formal de lo que comunmente conocemos como una *sucesión* de números reales). Dadas f, $g \in \mathcal{S}(\mathbb{R})$, decimos que g **domina** a f si existen constantes $M \in \mathbb{R}^+$ y $n_0 \in \mathbb{N}$ tales que

$$|f(n)| \leq M|g(n)|, \quad \forall\, n \geq n_0.$$

Por ejemplo, consideremos las funciones $f_1(n) \equiv 1$, $f_2(n) = n$, $f_3(n) = 3n + 5$, $f_4(n) = n^2$.

a) Es fácil ver que f_2, f_3 y f_4 dominan a f_1: basta tomar $n_0 = 1$ y $M = 1$ en la definición. Pero f_1 no domina a ninguna de ellas. En efecto, si por ejemplo suponemos que f_1 domina a f_2, deberían existir $n_0 \in \mathbb{N}$ y $M \in \mathbb{R}^+$ tales que

$$n \leq M, \ \forall n \geq n_0.$$

Como M es una constante, esto implicaría que el conjunto de los números naturales es acotado superiormente, lo que sabemos que es falso (basta considerar $\tilde{n} = \lfloor M \rfloor + 1$ y tendremos $\tilde{n} > M$). Argumentos similares prueban que f_1 no domina a f_3 y a f_4 (dejamos la prueba como ejercicio).

b) Por otra parte, puesto que $3n + 5 > n$ y $n^2 \geq n$ para cada $n \in \mathbb{N}$, f_3 y f_4 dominan a f_2 (nuevamente podemos tomar $n_0 = 1$ y $M = 1$ en la definición). Pero f_2 también domina a f_3. En efecto, observemos que si $n \geq 5$, entonces

$$3n + 5 \leq 3n + n = 4n.$$

Por lo tanto basta tomar $n_0 = 5$ y $M = 4$ en la definición anterior.

c) Como f_4 domina a f_2, y por el item anterior f_2 domina a f_3, podemos obtener fácilmente que f_4 domina a f_3. En efecto, $f_2(n) \leq f_4(n)$ para cada $n \in \mathbb{N}$. Luego tomando $n_0 = 5$ y $M = 4$, tendremos que si $n \geq n_0$ entonces

$$f_3(n) \leq M f_2(n) \leq M f_4(n).$$

Definamos la relación $\mathcal{R}$ en $\mathcal{S}(\mathbb{R})$ por $f\,\mathcal{R}\,g$ si g domina a f. De los items $a)$ y $b)$ anteriores podemos deducir que $\mathcal{R}$ no es simétrica (item a)) ni antisimétrica (item b)).

Por otra parte, toda función se domina trivialmente a sí misma, dado que $|f(n)| \leq |f(n)|$ para todo $n \in \mathbb{N}$. Luego $\mathcal{R}$ es una relación reflexiva.

Imitando el argumento del item c) probaremos que $\mathcal{R}$ es una relación transitiva. En efecto, supongamos que $f, g, h \in \mathcal{S}(\mathbb{R})$ son tales que $f\,\mathcal{R}\,g$ y $g\,\mathcal{R}\,h$. Existirán $n_0, n_0' \in \mathbb{N}$ y $M, M' \in \mathbb{R}^+$ tales que

$$|f(n)| \leq M|g(n)|, \quad \forall\, n \geq n_0 \tag{1}$$

$$|f(n)| \leq M'|h(n)|, \quad \forall\, n \geq n_0' \tag{2}$$

Pongamos $n_1 = \max\{n_0, n_0'\}$ y $M_1 = MM'$. Tendremos que si $n \geq n_1$, entonces deben verificarse las inecuaciones dadas en 1 y 2. Entonces, si $n \geq n_1$,

$$|f(n)| \leq M|g(n)| \leq MM'|h(n)| = M_1|h(n)|$$

con lo cual $f \mathcal{R} h$.

Concluimos que $\mathcal{R}$ es una relación de preorden en $\mathcal{S}(\mathbb{R})$. Para una función $g \in \mathcal{S}(\mathbb{R})$ suele definirse el conjunto de las funciones dominadas por g como

$$O(g) = \{f \in \mathcal{S}(\mathbb{R}) \,:\, f \mathcal{R} g\}.$$

Si $f \in O(g)$ (o sea $f \mathcal{R} g$) suele decirse que f es *de orden* (a lo sumo) g. Dejamos como ejercicio probar las siguientes propiedades de los conjuntos $O(g)$:

1. Si $f \in O(g)$ y $k \in \mathbb{R}$, entonces $kf \in O(g)$.
2. Si $k \neq 0$, $O(g) = O(kg)$.
3. Si $f_1 \in O(g_1)$ y $f_2 \in O(g_2)$ entonces $f_1 f_2 \in O(g_1 g_2)$.
4. Si $f_1 \in O(g_1)$ y $f_2 \in O(g_2)$ entonces $f_1 + f_2 \in O(|g_1| + |g_2|)$.

3. Jerarquías en conjuntos preordenados

En un conjunto preordenados pueden existir elementos que tienen características particulares y que generalizan los conceptos que comunmente manejamos de máximo y mínimo:

Definición **4.** *Sea $\mathcal{R}$ un preorden en un conjunto no vacío A. Decimos que un elemento $a \in A$ es un elemento:*

- ***maximal*** *si para cada $x \in A$ tal que $a \mathcal{R} x$ se verifica $x \mathcal{R} a$.*
- ***minimal*** *si para cada $x \in A$ tal que $x \mathcal{R} a$ se verifica $a \mathcal{R} x$.*
- ***máximo*** *si para cada $x \in A$, $x \mathcal{R} a$.*
- ***mínimo*** *si para cada $x \in A$, $a \mathcal{R} x$.*

Claramente todo elemento máximo es maximal y todo mínimo es minimal, y la recíproca es, en general, falsa.

Ejemplo **7.** Consideremos la relación $\mathcal{R}$ del Ejemplo 4 en el conjunto $A = \{1, 2, 3, 4\}$. A partir del grafo dirigido asociado a $\mathcal{R}$ podemos verificar que 1 es un mínimo y es el único elemento minimal de $\mathcal{R}$. Por otra parte, 2, 3 y 4 son elementos maximales y máximos de $\mathcal{R}$.

Ejemplo **8.** Consideremos la relación $\mathcal{R}$ en $\mathbb{Z} - \{0\}$ dada por $x \mathcal{R} y$ si $x \mid y$ del Ejemplo 5. Que exista un elemento maximal quiere decir que existe $a \in \mathbb{Z} - \{0\}$ tal que cada vez que a divide a x, entonces x divide a a. Por las propiedades de $\mathcal{R}$, si existiese un elemento maximal a, debería ser $a = \pm x$ para cada x divisible por a, pero esto no ocurre, pues a divide a ka para cualquier $k \in \mathbb{Z}$. Por lo tanto $\mathcal{R}$ no tiene elementos maximales, y por lo tanto tampoco tiene máximo.

Analicemos la existencia de un elemento minimal. En este caso, buscamos $a \in Z - \{0\}$ tal que si x divide a a, entonces a divide a x. Nuevamente, si existe, un elemento minimal debe verificar $a = \pm x$ para cada uno de sus dividores x. Luego si a tiene 2 o más divisores positivos, a no puede ser minimal. Los únicos elementos que tienen exactamente un divisor positivo son 1 y -1, y resultan ser elementos minimales de $\mathcal{R}$. Además como $1 \mid x$ y $-1 \mid x$ para cada $x \in \mathbb{Z} - \{0\}$ resulta que 1 y -1 son mínimos para $\mathcal{R}$.

Ejemplo **9.** Para la relación $\mathcal{R}$ en $\mathcal{S}(\mathbb{R})$ del Ejemplo 6, resulta claro que la función $f(n) \equiv 0$ es un mínimo, y por lo tanto un elemento minimal. Veremos que f es un elemento minimal de $\mathcal{R}$ si y sólo si $f \in O(0)$. Observemos que $f \in O(0)$ si y sólo si existe $n_0 \in \mathbb{N}$ (y $M \in \mathbb{R}^+$, que como veremos es irrelevante) tal que para cada $n \geq n_0$

$$|f(n)| \leq M0 = 0 \iff f(n) = 0$$

es decir, que los elementos de $O(0)$ son aquellas funciones identicamente nulas a partir de un cierto n_0 (estas funciones suelen considerarse *sucesiones finitas*). Resulta claro entonces que si $f \in O(0)$, entonces $f \,\mathcal{R}\, g$ para cualquier otra función $g : \mathbb{N} \to \mathbb{R}$. Por lo tanto f es un mínimo, y en particular un elemento minimal.

Supongamos ahora que f es un elemento minimal de $\mathcal{R}$. Como $0\mathcal{R}f$, deberá ser $f\mathcal{R}0$, y por lo tanto $f \in O(0)$.

Luego todos los elementos minimales de $\mathcal{R}$ son mínimos y son los elementos de $O(0)$.

Ejercicio **1.** *¿Existen elementos maximales en $\mathcal{S}(\mathbb{R})$ para la relación $\mathcal{R}$ del Ejemplo 6?*

Ejemplo **10.** Sea $\sim$ una relación de equivalencia en un conjunto A. $\sim$ es en particular un preorden. Entonces, como $\sim$ es simétrica, dado un elemento $a \in A$, si $a \sim x$, entonces $x \sim a$, por lo tanto todo elemento es maximal. Análogamente todo elemento es minimal.

Ejercicio **2.** *¿Existe una relación de equivalencia que tenga máximos y/o mínimos? ¿Cual?*

Definición **5.** *Sea $\mathcal{R}$ un preorden en A, $B \subseteq A$ y $a \in A$. Decimos que*

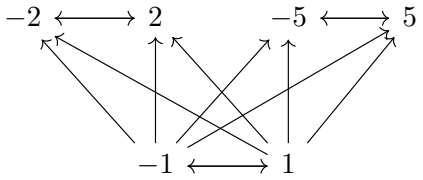
- *a es **cota superior** de B si $b \,\mathcal{R}\, a$ para cada $b \in B$. Si existe una cota superior de B decimos también que B está **acotado superiormente***
- *a es **cota inferior** de B si $a \,\mathcal{R}\, b$ para cada $b \in B$. Si existe una cota inferior de B decimos también que B está **acotado inferiormente***
- *a es un **supremo** de B si A es un mínimo de*

$$\{c \in A : c \text{ es cota superior de } B\}$$

- *a es un **ínfimo** de B si a es un máximo de*

$$\{c \in A : c \text{ es cota inferior de } A\}$$

Ejemplo **11.** Consideremos el conjunto $A \subset \mathbb{Z} - \{0\}$ de divisores de 10 distintos de ± 10 y la relación $\mathcal{R}$ en A que es la restricción de la relación "divide a" en $\mathbb{Z} - \{0\}$ a A. Observemos que $A = \{\pm 1, \pm 2, \pm 5\}$. Para representar gráficamente una relación que ya sabemos que es un preorden podemos obviar los lazos alrededor de cada vértice, recordando siempre que estos elementos están relacionados con sí mismos. Intentaremos además ordenar los vértices de manera *ascendente*, es decir, intentando que las flechas, en la medida de lo posible, apunten hacia arriba (veremos que en un orden parcial esto siempre es posible, pero puede ocurrir que en un preorden no lo sea). Podemos utilizar además "flechas con doble punta" para representar simultáneamente dos aristas (x, y) y (y, x) (nuevamente esto no puede ocurrir en el grafo de un orden parcial, pues la relación es en ese caso antisimétrica). Con estas consideraciones, podemos representar el grafo dirigido asociado a $\mathcal{R}$ de la siguiente manera:



Consideremos el conjunto $B = \{-2, 1, 5\} \subset A$. Observemos que B no es acotado superiormente en A pero sí es acotado inferiormente por 1 y -1. Ambos elementos son además ínfimos de B.

Si ahora consideramos $B = \{-2, 2\}$ entonces 2 y -2 son cotas superiores de B y son ambos supremos. Las cotas inferiores son 2, -2, 1 y -1, y los ínfimos de B también son 2 y -2.

Finalmente si $B = \{5\}$, 5 y -5 son cotas superiores y ambos supremos de B. 1, -1, 5 y -5 son cotas inferiores de B, y 5 y -5 son ínfimos.

Si ahora consideramos toda la relación "divide a" en $\mathbb{Z} - \{0\}$ y a todo A como un subconjunto de $\mathbb{Z} - \{0\}$ vemos que las cotas superiores de A son ± 10, ± 20, ± 30, etc. y los supremos de A son 10 y -10. Las únicas cotas inferiores son 1 y -1 que son a su vez ambos ínfimos.

Ejemplo **12.** Consideremos la relación $\mathcal{R}$ en $\mathcal{S}(\mathbb{R})$ dada en el ejemplo 6.

Sea $A = \{f_1, f_2, f_3, f_4\}$ las funciones de ese ejemplo, es decir, $f_1(n) \equiv 1$, $f_2(n) = n$, $f_3(n) = 3n + 5$, $f_4(n) = n^2$. Observemos que f_1 es una cota inferior de A y f_4 es una cota superior. En particular, como son elementos de A serán respectivamente un ínfimo y un supremo de A (¿Por qué?). Sin embargo no son los únicos. Dejamos como ejercicio probar que cualquier función constante es un ínfimo de A y cualquier función de la forma $f(n) = an^2 + bn + c$, con $a, b, c \in \mathbb{R}$ es un supremo de A.

Consideremos ahora para cada $k \in \mathbb{N}$ la función $g_k(n) = \frac{1}{n^k}$ y sea $B = \{g_k\}_{k \in \mathbb{N}} \subset \mathcal{S}(\mathbb{R})$. Entonces $g(n) \equiv 0$ es una cota inferior de B y $h(n) \equiv 1$ es una cota superior. Observemos además que $g_1(n) = \frac{1}{n}$ también es una cota superior de B, y por lo tanto es un supremo. Como $g_1 \mathcal{R} h$ pero $h \not\mathcal{R} g_1$, resulta que h no es supremo de B.

Dejamos como ejercicio determinar si B tiene otros supremos además de g_1. ¿Es g un ínfimo de B?

4. Conjuntos parcialmente ordenados (Posets)

Recordemos que una relación $\mathcal{R}$ en un conjunto A es una relación de **orden (parcial)** en A si $\mathcal{R}$ es reflexiva, antisimétrica y transitiva. Si $\mathcal{R}$ es un orden (parcial) en A, decimos que A es un **conjunto (parcialmente) ordenado**, o un **Poset** (del inglés *partially ordered set*). En general, denotaremos por $\preceq$ a un orden parcial. Es decir, si $\mathcal{R}$ es un orden parcial en A, escribimos

$$x \preceq y$$

para indicar que $x \mathcal{R} y$. Muchas veces decimos que x **precede** a y o es **anterior** a y o directamente que es **menor** a y si $x \preceq y$ y $x \neq y$. Trataremos de evitar en lo posible la terminología de "*menor a*" que reservaremos para el orden usual en los conjuntos numéricos. Sin embargo es usual encontrarla en la bibliografía, junto con la notación $\leq$ para lo que aquí hemos denotado $\preceq$.

Escribiremos

$$x \prec y$$

para indicar que $x \preceq y$ y $x \neq y$.

Definición **6.** *Sea $\preceq$ una relación de orden en un conjunto A. Dados $x, y \in A$, decimos que x e y son elementos **comparables** si se verifica $x \preceq y$ o $y \preceq x$ (observemos que como $\preceq$ es antisimétrica, estas dos condiciones se verifican simultáneamente sólo cuando $x = y$).*

*La relación $\preceq$ se denomina un **orden total** si todo par de elementos de A son comparables. En ese caso, A se dice un conjunto **totalmente ordenado**.*

Esta última definición justifica por qué llamamos *orden parcial* a una relación de orden.

Las relaciones de orden tienen las siguientes propiedades:

Lema **1.** *Sea $\preceq$ una relación de orden en un conjunto A y sea $B \subseteq A$, entonces:*

1. *$\preceq_{|B}$ es un orden en B. Si $\preceq$ es un orden total, entonces $\preceq_{|B}$ también lo es.*
2. *$s \preceq^{-1}$ es una relación de orden en A, denominada el **orden inverso** a $\preceq$ y denotada por $\succeq$. Si $\preceq$ es un orden total, entonces $\succeq$ también es un orden total.*

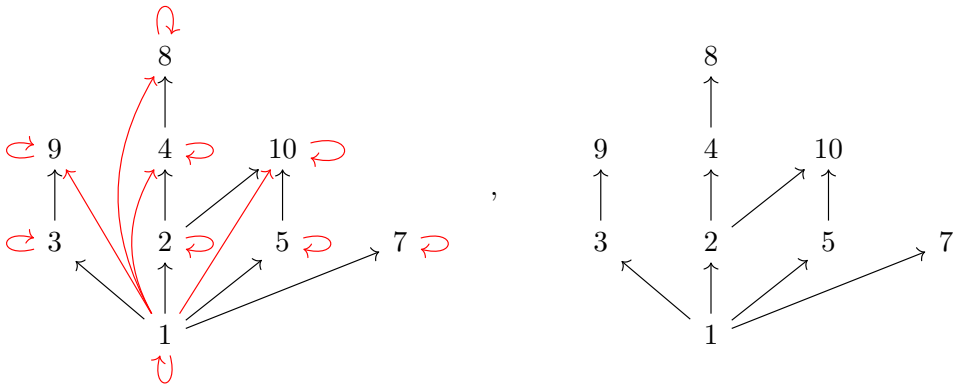
Ejercicio **3.** *Demostrar el Lema 1 (ver Ejercicios 7 y 8 de la Práctica 1)*

Por definición de la relación inversa, tendremos que

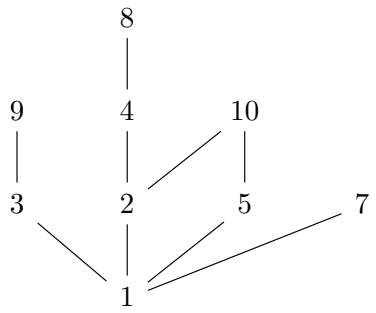
$$x \preceq y \iff y \succeq x.$$

Ejemplo **13. Divisibilidad** Vimos que la relación $n \mathcal{R} m$ si $n \mid m$ es un preorden en $\mathbb{Z} - \{0\}$, pero $\mathcal{R}_{|\mathbb{N}}$ es una relación de orden en $\mathbb{N}$. Se trata de un orden parcial, pues por ejemplo dos números primos cualesquiera no son comparables entre si (por ejemplo $2 \nmid 3$ y $3 \nmid 2$). Si restringimos la relación al subconjunto finito

$A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ tendremos que el grafo dirigido asociado es el siguiente:



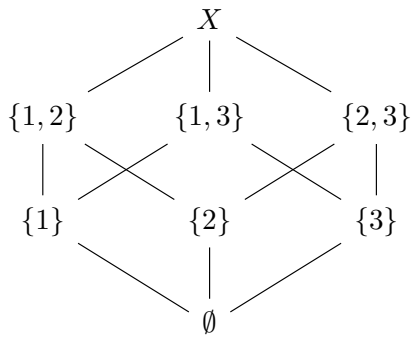
Observemos que en el grafo de la derecha hemos eliminado los lazos (como ya hicimos en los preórdenes) y las aristas en rojo del grafo de la izquierda. Cuando ya sabemos que estamos lidiando con una relación de orden, estos elementos son superfluos. Como la relación es reflexiva, sobreentendemos que en todo vértice del grafo hay un lazo, y por lo tanto no lo dibujamos. También sabemos que es transitiva, por lo tanto para cada camino simple que tengamos en el gráfo, el vértice inicial y el vértice final del camino deberían estar unidos por una arista, que también obviamos. Si además ubicamos los vértices de manera *ascendente* siembre tendremos un grafo del estilo de la derecha. Estos grafos se denominan **diagramas de Hasse** de una relación de orden. Como se sobreentiende que los vértices están ubicados de manera ascendente, también podríamos obviar colocar las flechas, sobreentendiendo que van en la dirección del vértice inferior al vértice superior. De esta manera, el diagrama de Hasse para la relación "divide a" en $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ es



Ejercicio **4.** *Probar que si el grafo dirigido G de una relación transitiva $\mathcal{R}$ tiene un ciclo de longitud mayor o igual a 3, entonces $\mathcal{R}$ no puede ser un orden parcial.*

Ejemplo **14. Contención de conjuntos** Consideremos un conjunto X cualquiera y sea $A = \mathcal{P}(x)$. La relación de contención $C \preceq D$ si $C \subseteq D$ define una relación de orden en A.

Tomemos por ejemplo el conjunto $X = \{1, 2, 3\}$. El diagrama de Hasse de la relación es en este caso:



Aqui podemos notar fácilmente que $\subseteq$ no es un orden total en $\mathcal{P}(X)$, pues por ejemplo $\{1\}$ y $\{2\}$ no son comparables.

Ejemplo **15. Orden producto y orden lexicográfico**. Sean $(A, \preceq_A)$ y $(B, \preceq_B)$ dos conjuntos parcialmente ordenados. Definamos en $A \times B$ la relación $\preceq_{prod}$ dada por

$$(a, b) \preceq_{prod} (c, d) \text{ si } a \preceq_A c \ \wedge \ b \preceq_B d$$

Dejamos como ejercicio verificar que $\preceq_{prod}$ es una relación de orden parcial en $A \times B$, que en general no es un orden total incluso si A y B son totalmente ordenados. Se denomina **orden producto**.

Consideremos por ejemplo el orden usual en $\mathbb{R}$ y tomemos el orden producto en $\mathbb{R} \times \mathbb{R}$. $\mathbb{R}$ con este orden es totalmente ordenado, pues dos elementos cualesquiera son comparables. Sin embargo $\mathbb{R} \times \mathbb{R}$ no es totalmente ordenado para $\leq_{prod}$: $(0, 1)$ y $(1, 0)$ no son comparables.

Otro orden posible en $A \times B$ es el denominado **orden lexicográfico**. Definimos la relación $\preceq_{lex}$ en $A \times B$ por

$$(a, b) \preceq_{lex} (c, d) \ \text{ si } \ (a \prec_A c) \vee (a = c \ \wedge \ b \preceq_B d)$$

El nombre de esta forma de ordenar un producto proviene del orden usual del diccionario: comparamos primero los primeros elementos, y sólo si estos son iguales procedemos a comparar los que siguen. Puede generalizarse a cualquier producto finito de conjuntos ordenados. Dejamos como ejercicio probar que $\preceq_{lex}$ es efectivamente una relación de orden, y en este caso se trata de un orden total si A y B son conjuntos totalmente ordenados.

Ejemplo **16. Relaciones de orden en los conjuntos numéricos.** Como hemos notado en el Ejemplo 13 de la Unidad 1 tenemos dos formas de definir los conjuntos numéricos: dando una teoría axiomática para $\mathbb{R}$ y definir $\mathbb{N}$, $\mathbb{Z}$ y $\mathbb{Q}$ como subconjuntos con ciertas propiedades de $\mathbb{R}$, o partir de una teoría axiomática en $\mathbb{N}$ y construir ciertos cocientes para definir $\mathbb{Z}$ y $\mathbb{Q}$ (la construcción de $\mathbb{R}$ en este caso es más compleja). En el primer caso, el orden de $\mathbb{R}$ mediante la relación $\leq$ ("menor o igual") se define axiomáticamente a través de los denominados *axiomas de orden*.

Veamos como podemos definir esta relación partiendo de los axiomas de Peano en $\mathbb{N}$. Recordemos que uno de los axiomas establece que existe una función $S : \mathbb{N} \to \mathbb{N}$, denominada "sucesor" que verifica:

1. Para todo $n \in \mathbb{N}$, la proposición $S(n) = 1$ es falsa. Es decir, 1 no es sucesor de ningún elemento de $\mathbb{N}$.

2. Para cada $n, m \in \mathbb{N}$, si $S(n) = S(m)$, entonces $n = m$.

y a partir de este axioma tenemos definida la suma como la función $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, dada por:

- $n + 1 = S(n)$, para cada $n \in \mathbb{N}$.
- $n + S(m) = S(n + m)$, para cada $n, m \in \mathbb{N}$.

y esta operación es asociativa y conmutativa.

Observemos que esta definición implica que en $\mathbb{N}$ se puede cancelar, es decir, si $n + k = n + k'$ entonces $k = k'$. En efecto, para $n = 1$ tenemos que $1 + k = 1 + k'$, entonces $S(k) = S(k')$ y por lo tanto $k = k'$. Si ahora suponemos que esta propiedad es válida para un cierto $n \in \mathbb{N}$, tendremos que

$$S(n) + k = S(n) + k' \;\Rightarrow\; S(n + k) = S(n + k') \;\Rightarrow\; n + k = n + k' \;\Rightarrow\; k = k'$$

con lo cual, por el principio de inducción, es válida para todo $n \in \mathbb{N}$.

Podemos definir la relación $\leq$ en $\mathbb{N}$ dada por

$$n \leq m \iff n = m \;\vee\; (\exists\, k \in \mathbb{N} : n + k = m)$$

Esta relación es claramente reflexiva. También es transitiva. En efecto, supongamos que $n, m, r \in \mathbb{N}$ son tales que $n \leq m$ y $m \leq r$. Si $n = m$ o $m = r$ entonces es claro que $n \leq r$. Supongamos entonces que $n \neq m$ y $m \neq r$. Existirán $k, k' \in \mathbb{N}$ tales que

$$m = n + k \;\wedge\; r = m + k'$$

Luego $r = m + k' = n + (k + k')$ y como $k + k' \in \mathbb{N}$ resulta $n \leq r$.

Para probar la antisimetría supongamos que $n, m \in \mathbb{N}$ son tales que $n \leq m$ y $m \leq n$. Si fuese $n \neq m$, existirían $k, k' \in \mathbb{N}$ tales que

$$m = n + k \;\wedge\; n = m + k' \implies n = n + k'', \text{con } k'' = k + k' \in \mathbb{N}.$$

Sumando 1 (o tomando sucesor) a ambos lados de la igualdad, tenemos que $n + 1 = n + (k'' + 1)$ y por lo que hemos probado anteriormente deberá ser $1 = k'' + 1 = S(k'')$, pero esto no puede ocurrir pues 1 no es el sucesor de ningún número.

Concluimos que $\leq$ es una relación de orden. Utilizando el Principio de inducción puede probarse que en realidad $\leq$ es un orden total en $\mathbb{N}$.

Recordemos que $\mathbb{Z} = N \times N/\sim$, donde $(a, b) \sim (c, d)$ si $a + d = c + b$. Definamos la relación $\mathcal{R}$ en $\mathbb{N} \times \mathbb{N}$ por $(a, b)\,\mathcal{R}\,(c, d)$ si $a + d \leq c + b$. Observemos que $\mathcal{R}$ verifica que si $(a, b) \sim (a', b')$ y $(c, d) \sim (c', d')$ entonces

$$(a, b)\,\mathcal{R}\,(c, d) \iff (a', b')\,\mathcal{R}\,(c', d')$$

(dejamos los detalles como ejercicio). Esto implica que $\mathcal{R}$ se *induce* al conjunto cociente $\mathbb{Z} = \mathbb{N} \times \mathbb{N}/\sim$, es decir, podemos definir

$$[(a, b)] \preceq [(c, d)] \;\Leftrightarrow\; (a, b)\,\mathcal{R}\,(c, d) \tag{3}$$

y esta será una relación bien definida, en el sentido en que no importa qué representantes de la clase de equivalencia elijamos siempre obtendremos el mismo resultado.

Ejercicio **5.** *Probar que la relación $\preceq$ en $\mathbb{Z}$ definida por (3) es una relación de orden en $\mathbb{Z}$.*

5. Jerarquías en un conjunto parcialmente ordenado

Como una relación de orden parcial es antisimétrica, podemos caracterizar los elementos maximales y minimales en un conjunto parcialmente ordenado de la siguiente manera:

Teorema **2.** *Sea $(A, \preceq)$ un conjunto parcialmente ordenado y sea $a \in A$. Entonces*

1. *a es un elemento minimal si para cada $x \in A$ se verifica que*

$$x \preceq a \implies x = a$$

2. *a es un elemento maximal si para cada $x \in A$ se verifica que*

$$a \preceq x \implies x = a.$$

Ejercicio **6.** *Demostrar el Teorema 2.*

Hemos visto en varios ejemplos que un conjunto preordenado puede tener varios máximos y mínimos o supremos e ínfimos. Esto no es cierto en un conjunto parcialmente ordenado:

Teorema **3.** *Si un conjunto parcialmente ordenado tiene un elemento máximo (o mínimo) entonces este elemento es único.*

Demostración. Supongamos que $(A, \preceq)$ es un conjunto parcialmente ordenado y a, a' son máximos de A. Entonces como a es máximo $x \preceq a$ para todo $x \in A$. En particular $a' \preceq a$. Aplicando ahora la definición de máximo a a' obtenemos que $a \preceq a'$. Como $\preceq$ es antisimétrica concluimos que $a' = a$. La demostración de la unicidad del mínimo es análoga y la dejamos como ejercicio. □

Corolario **4.** *Todo subconjunto de un conjunto parcialmente ordenado tiene a lo sumo un ínfimo y/o un supremo.*

Ejercicio **7.** *Probar el Corolario 4*

Teorema **5.** *Sea $(A, \preceq)$ un conjunto parcialmente ordenado. Si $B \neq \emptyset$ es un subconjunto finito de A, entonces $(B, \preceq_{|B})$ tiene al menos un elemento minimal y al menos un elemento maximal.*

Demostración. Supongamos que B es un subconjunto finito de A de cardinal n. Tomemos $b_1 \in B$ y consideremos el conjunto

$$B_1 = \{b \in B \,:\, b \prec b_1\}.$$

Observemos que $b_1 \notin B_1$, y por lo tanto B_1 tiene cardinal menor o igual a $n - 1$.

Si $B_1 = \emptyset$, entonces b_1 es un elemento minimal de B. Si $B_1 \neq \emptyset$, existirá $b_2 \in B$ tal que $b_2 \prec b_1$. Podemos entonces considerar

$$B_2 = \{b \in B \,:\, n \prec b_2\}$$

Nuevamente $b_2 \notin B_2$, y como $b_2 \prec b_1$, $b_1 \notin B_2$. Luego B_2 tiene cardinal a lo sumo $n-2$. Si $B_2 = \emptyset$, entonces b_2 es un elemento minimal de B. Si $B_2 \neq \emptyset$, existirá un elemento $b_3 \in B$ tal que $b_3 \prec b_2 \prec b_1$, con lo cual

$$B_3 = \{b \in B \,:\, b \prec b_3\}$$

es un conjunto finito de cardinal a lo sumo $n-3$.

Al cabo de k pasos habremos encontrado elementos $b_k \prec b_{k-1} \prec \cdots \prec b_1$ en B tal que b_k es un elemento minimal de B o bien existe $b_{k+1} \in B$ tal que $b_{k+1} \prec b_k$. Como B es finito, este proceso termina al cabo a lo sumo de n pasos obteniendo un elemento minimal de B.

La prueba de la existencia de un elemento maximal es análoga y se deja como ejercicio. □

Corolario **6.** *Todo conjunto finito totalmente ordenado tiene un máximo y un mínimo.*

Ejercicio **8.** *Demostrar el Corolario 6*

Claramente este resultado es falso para conjuntos infinitos, incluso para aquellos acotados superior o inferiormente. En $(\mathbb{R}, \leq)$ por ejemplo, cualquier intervalo abierto (a, b) con el orden inducido no posee elementos maximales ni minimales.

Una generalización del Teorema 5 nos la da el Lema de Zorn que enunciaremos a continuación. Este resultado tiene numerosas aplicaciones en muchas áreas de la matemática y es equivalente al axioma de elección en la teoría axiomática de conjuntos.

Definición **7.** *Sea $(A, \preceq)$ un poset. Un subconjunto $X \subseteq A$ se dice una* ***cadena*** *si $(X, \preceq_{|X})$ es un conjunto totalmente ordenado.*

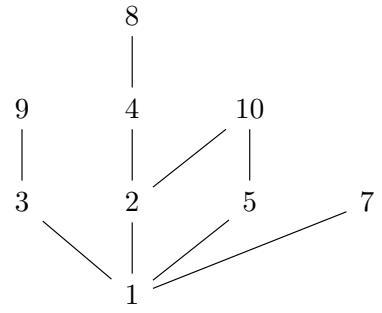
Ejemplos **17.**

1. En $(\mathbb{R}, \leq)$ cualquier subconjunto es una cadena. Más generalmente, si $(A, \preceq)$ está totalmente ordenado, cualquier subconjunto de A es una cadena.
2. En $(\mathbb{N}, |\,)$ (que no es totalmente ordenado) el conjunto de las potencias de 2, $B = \{2^k \,:\, k \in \mathbb{N}_0\}$ es una cadena.

Teorema **7** (Lema de Zorn)**.** *Sea $(A, \preceq)$ un poset no vacío. Si toda cadena en A tiene una cota superior, entonces A tiene al menos un elemento maximal.*

Ejercicio **9.** *Deducir el Teorema 5 del Lema de Zorn.*

Ejemplo **18.** Consideremos la relación $\preceq$ "divide a" en el conjunto $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, cuyo diagrama de Hasse, presentado en el Ejemplo 13 es el siguiente:



Tenemos en este caso que A no tiene máximo, pues no hay ningún elemento divisible por todos los elementos del conjunto. Sí tiene un mínimo, que es 1, que a su vez es el único elemento minimal. $7, 8, 9$ y 10 son elementos maximales.

Si ahora consideramos el subconjunto $B = \{2, 5\} \subset A$, tenemos que 10 es la única cota superior de B y es su supremo, a la vez que 1 es la única cota inferior de B, y es su ínfimo.

Si tomamos $C = \{2, 3, 5\}$, podemos observar que este subconjunto no tiene cotas superiores, y por lo tanto no tiene supremo. Nuevamente, 1 es la única cota inferior y el ínfimo de C.

Ejemplo **19.** Consideremos ahora el conjunto parcialmente ordenado $(\mathbb{N}, \mid)$. En este caso es fácil ver que existe un mínimo, 1, que el único número que divide a todos los naturales. Dejamos como ejercicio probar que esta relación no tiene máximo.

Si $B \subset \mathbb{N}$ es un conjunto finito cualquiera, B está acotado inferiormente (pues 1 es una cota inferior) y superiormente (pues el producto de todos sus elementos es una cota superior). Para analizar la existencia de ínfimo de B, debemos pensar si existe un elemento $a \in \mathbb{N}$ tal que $a \mid x$ para cada $x \in B$ (a es una cota inferior de B) y tal que para cualquier otra cota inferior b de B, $b \mid a$. Ahora bien, cualquier otra cota inferior de B será un elemento $b \in \mathbb{N}$ tal que $b \mid x$ para cada $x \in B$, con lo cual estamos buscando un elemento $a \in \mathbb{N}$ tal que

$$(a \mid x \; \forall x \in B) \; \wedge \; (\forall b \in \mathbb{N} : b \mid x, \; \forall x \in B \; \Rightarrow \; b \mid a) \tag{4}$$

Un elemento que verifique estas características para un conjunto finito de números se denomina el **máximo común divisor** de esos números. Puede probarse que el máximo común dividor siempre existe (lo haremos en el Teorema 16). Por lo tanto todo subconjunto finito de $(\mathbb{N}, \mid)$ tiene un ínfimo, que es el máximo común divisor de sus elementos.

De manera similar, B tiene un supremo, que es el **mínimo común múltiplo** de sus elementos, y está caracterizado por ser el único elemento $c \in \mathbb{N}$ tal que

$$(x \mid c \; \forall x \in B) \; \wedge \; (\forall b \in \mathbb{N} : x \mid b, \; \forall x \in B \; \Rightarrow \; c \mid b). \tag{5}$$

Si consideramos por ejemplo el conjunto $B = \{30, 70, 80\}$, tenemos que las cotas inferiores de B, que son los divisores comunes de sus elementos, son 1, 2, 5 y 10. El ínfimo del conjunto es el máximo común divisor de 30, 70 y 80 que es $a = 10$.

B está acotado superiormente por infinitos elementos, pero una cota superior obvia es $b = 30 \cdot 70 \cdot 80 = 168000$. Sin embargo, la menor de las cotas inferiores es $c = 1680$, que es el mínimo común múltiplo de 30, 70 y 80.

Ejercicio **10.** *Consideremos la restricción del orden parcial "divide a" a* $\mathbb{N} - \{1\}$*. ¿Cuáles son los elementos minimales? ¿Sigue siendo cierto que todo subconjunto finito de* $\mathbb{N} - \{1\}$ *tiene un ínfimo?*

Ejemplo **20.** Consideremos un conjunto $X \neq \emptyset$ cualquiera y la relación de orden $\subseteq$ en $\mathcal{P}(X)$. Entonces X es el elemento máximo y $\emptyset$ es el mínimo. Probaremos en la Práctica 2 que cualquier subconjunto de $\mathcal{P}(X)$ tiene supremo e ínfimo.

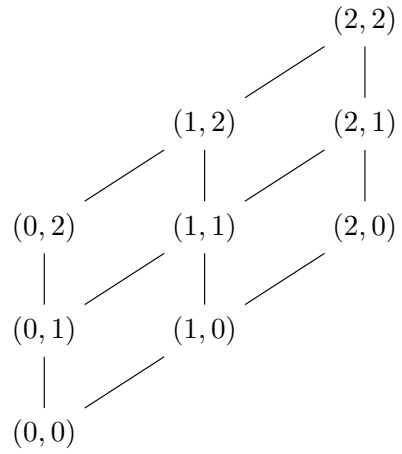
Ejemplo **21.** Sea $A = \{0, 1, 2\}$ con el orden usual $\leq$ y consideremos los conjuntos ordenados $(A \times A, \preceq_{prod})$ y $(A \times A, \preceq_{lex})$ introducidos en el Ejemplo 15.

Observemos que

$$(0,0) \preceq_{lex} (0,1) \preceq_{lex} (0,2) \preceq_{lex} (1,0) \preceq_{lex} (1,1) \preceq_{lex} (1,2) \preceq_{lex} (2,0) \preceq_{lex} (2,1) \preceq_{lex} (2,2)$$

y por lo tanto su diagrama de Hasse es una "línea vertical", es decir son trazos verticales entre cada nodo. Por lo tanto $(0,0)$ y $(2,2)$ son el mínimo y el máximo y cualquier subconjunto de $B \subset A \times A$ tiene ínfimo y supremo, que son a su vez el mínimo y el máximo del conjunto ordenado $(B, \preceq_{lex|B})$.

Por otra parte, el diagrama de Hasse para $(A \times A, \preceq_{prod})$ es



Aquí tenemos nuevamente que $(0,0)$ es mínimo y $(2,2)$ es máximo. Si consideramos por ejemplo $B = \{(0,0), (0,1), (1,0), (0,2), (1,1), (2,0)\}$ tendremos que $(B, \preceq_{prod|B})$ tiene un mínimo, $(0,0)$, pero no tiene máximo. En cambio posee tres elementos maximales, $(0,2)$, $(1,1)$ y $(2,0)$. Como subconjunto de $A \times A$, B tiene ínfimo $(0,0)$, y tiene supremo $(2,2)$ que es su única cota superior.

Para finalizar esta sección mencionaremos el **principio de dualidad** que rige en los conjuntos ordenados. Hemos observado que si $(A, \preceq)$ es un conjunto ordenado, entonces $(A, \succeq)$ también lo es, siendo $\succeq$ la relación inversa a $\preceq$. El principio de dualidad consiste en que cualquier proposición que involucre cotas inferiores, elementos minimales, mínimos o ínfimos en $(A, \preceq)$ sigue siendo válida en $(A, \succeq)$ cambiando estos elementos por cotas superiores, elementos maximales, máximos o supremos respectivamente (y también cambiando cotas superiores en $(A, \preceq)$ por cotas inferiores en $(A, \succeq)$ etc.). En particular, dejamos como ejercicio probar las siguientes propiedades:

Teorema **8.** *Sea $(A, \preceq)$ un conjunto parcialmente ordenado y sea $\succeq$ el orden inverso de $\preceq$. Entonces*

1. *Si a es un elemento minimal (resp. maximal) de $(A, \preceq)$, entonces a es un elemento maximal (resp. minimal) de $(A, \succeq)$.*

2. *Si a es un mínimo (resp. máximo) de $(A, \preceq)$, entonces a es un máximo (resp. mínimo) de $(A, \succeq)$.*

3. *Sea $B \subseteq A$. Si a es una cota inferior de B (resp. cota superior) en $(A, \preceq)$, entonces a es una cota superior de B (resp. cota inferior) en $(A, \succeq)$.*

4. *Sea $B \subseteq A$. Si a es el ínfimo de B (resp. supremo) en $(A, \preceq)$, entonces a es el supremo de B (resp. ínfimo) en $(A, \succeq)$.*

Ejemplo **22.** Consideremos en $\mathbb{N}$ el orden $\succeq$ dado por $a \succeq b$ si a es múltiplo de b. Como a es múltiplo de b si y sólo si b divide a a, resulta que $\succeq$ es la relación inversa de la relación "divide a" en $\mathbb{N}$. Por lo tanto $\succeq$ tiene un máximo en 1 (dado que $a \succeq 1$ para cada $a \in \mathbb{N}$). Por otra parte, si restringimos $\succeq$ al conjunto $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ podemos obtener el diagrama de Hasse de $\succeq$ invirtiendo el diagrama de Hasse de la relación "divide a" presentado en el Ejemplo 13:

Diagrama de Hasse de "divide a"

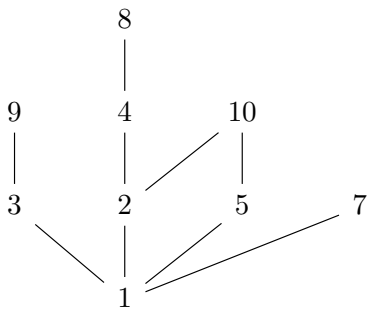
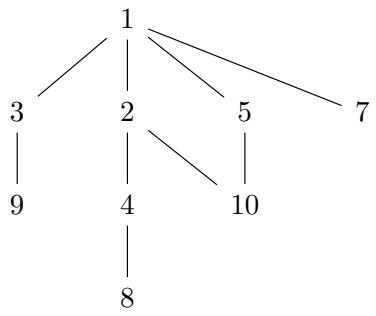


diagrama de Hasse de $\succeq$



Observemos que como $(A, \mid)$ no tiene máximo, $(A, \succeq)$ no tiene mínimo. Como $8, 9, 10$ y 7 son elementos maximales de $(A, \mid)$, estos mismos elementos son minimales en $(A, \succeq)$.

Si ahora consideramos el subconjunto $B = \{2, 5\} \subset (A, \mid)$ tenemos que 10 es la única cota superior de B y es su supremo, a la vez que 1 es la única cota inferior de B, y es su ínfimo. Por lo tanto 10 es el ínfimo de B en $(A, \succeq)$ y 1 es su supremo.

Si tomamos $C = \{2, 3, 5\}$, C no tiene supremo en $(A, \mid)$ y 1 es el ínfimo de C en $(A, \mid)$. Por lo tanto C no tiene ínfimo en $(A, \succeq)$ y su supremo es 1.

6. Morfismos de posets

Dados dos conjuntos parcialmente ordenados $(A, \preceq_A)$ y $(B, \preceq_B)$ nos interesa estudiar aquellas funciones $f : A \to B$ que "preservan" el orden:

Definición **8.** *Sean $(A, \preceq_A)$ y $(B, \preceq_B)$ dos posets y sea $f : (A, \preceq_A) \to (B, \preceq_B)$. Decimos que:*

- *f es un **morfismo de orden** (o **morfismo de posets**) si para cada $x, y \in A$ se verifica*

$$x \preceq_A y \implies f(x) \preceq_B f(y)$$

- *f es un **isomorfismo** de $(A, \preceq_A)$ en $(B, \preceq_B)$ si f es un morfismo de orden biyectivo tal que $f^{-1} : (B, \preceq_B) \to (A, \preceq_A)$ es un morfismo de orden.*

Ejemplo **23.** Consideremos las funciones $f = Id : (\mathbb{N}, \mid) \to (\mathbb{N}, \leq)$ y $g = Id : (\mathbb{N}, \leq) \to (\mathbb{N}, \mid)$. Observemos que en términos formales f y g son la misma función. Veremos que tienen comportamientos distintos según los órdenes que consideremos en $\mathbb{N}$.

Observemos que si $a \mid b$ entonces $a \leq b$ (pues existe $k \geq 1$ tal que $b = ka$). Luego $f = Id : (\mathbb{N}, \mid) \to (\mathbb{N}, \leq)$ es un morfismo de orden. Sin embargo $g = Id : (\mathbb{N}, \leq) \to (\mathbb{N}, \mid)$ no es un morfismo de orden. En efecto $2 \leq 3$ y sin embargo $2 \nmid 3$. Como $g = f^{-1}$, f no es un isomorfismo de $(\mathbb{N}, \mid)$ en $(\mathbb{N}, \leq)$.

Teorema **9.** *Sean $(A, \preceq_A)$ y $(B, \preceq_B)$ dos conjuntos parcialmente ordenados y sea $f : (A, \preceq_A) \to (B, \preceq_B)$ un morfismo de orden. Entonces:*

1. *f es un isomorfismo de $(A, \preceq_A)$ en $(B, \preceq_B)$ si y sólo si f es sobreyectiva y se verifca que para cada $x, y \in A$,*
$$x \preceq_A y \iff f(x) \preceq_B f(y). \tag{6}$$
2. *f es un isomorfismo de $(A, \preceq_A)$ en $(B, \preceq_B)$ si y sólo si f^{-1} es un isomorfismo de $(B, \preceq_B)$ en $(A, \preceq_B)$.*
3. *Si $f : (A, \preceq_A) \to (B, \preceq_B)$ y $g : (B, \preceq_B) \to (C, \preceq_C)$ don morfismos de orden, entonces*
$$g \circ f : (A, \preceq_A) \to (C, \preceq_C)$$
es un morfismo de orden. Si f y g son isomorfismos, entonces $g \circ f$ es un isomorfismo.

Demostración. 1. $\Rightarrow$) Supongamos que f es un isomorfismo de $(A, \preceq_A)$ en $(B, \preceq_B)$. Entonces f es biyectiva, con lo cual en particular es sobreyectiva, y se verifica que para cada $x, y \in A$,
$$x \preceq_A y \implies f(x) \preceq_B f(y).$$
Debemos entonces probar que si $x, y \in A$ son tales que $f(x) \preceq_B f(y)$ entonces $x \preceq_A y$. Para ello observemos que como f es un isomorfismo, f^{-1} es un morfismo de orden. Luego tendremos:
$$f(x) \preceq_B f(y) \implies f^{-1}(f(x)) \preceq_A f^{-1}(f(y)) \implies x \preceq_A y.$$
$\Leftarrow$) Supongamos que f es sobreyectiva y vale (6). Veamos primero que f es inyectiva. Sean $x, y \in A$ tales que $f(x) = f(y)$. Entonces tendremos que $f(x) \preceq_B f(y)$ y $f(y) \preceq_B f(x)$. Luego por (6), resultará $x \preceq_A y$ y $y \preceq_A x$, con lo cual $x = y$.

Concluimos que f es biyectiva. Veamos ahora que f^{-1} también es un morfismo de orden. Sean $v, w \in B$ tales que $v \preceq_B w$. Como f es biyectiva, existirán únicos $x, y \in A$ tales que $f(x) = v$, $f(y) = w$. Luego $f(x) \preceq_B f(y)$ y de (6), resulta $x \preceq_A y$. Pero $x = f^{-1}(v)$ e $y = f^{-1}(w)$.

2. Es inmediata de la definición de isomorfismo. Dejamos los detalles como ejercicio.

3. Sean $x, y \in A$ tales que $x \preceq_A y$. Como f es un morfismo de orden tendremos que $f(x) \preceq_B f(y)$, y como g es un morfismo de orden, resultará entonces $g(f(x)) \preceq_C g(f(y))$. Luego $g \circ f$ es un morfismo de orden. Dejamos la última afirmación como ejercicio.

□

Corolario **10.** *Sea* Poset *el conjunto de todos los conjuntos parcialmente ordenados. Entonces la relación* $\sim$ *en* Poset *dada por* $(A, \preceq_A) \sim (B, \preceq_B)$ *si existe un isomorfismo* f *de* $(A, \preceq_A)$ *en* $(B, \preceq_B)$ *es una relación de equivalencia.*

Ejercicio **11.** *Probar el Corlorario 10*

En vistas del Corolario 10, si existe un isomorfismo f de $(A, \preceq_A)$ en $(B, \preceq_B)$ decimos que $(A, \preceq_A)$ y $(B, \preceq_B)$ son **posets isomorfos**.

Hemos visto en el Ejemplo 23 que $Id : (\mathbb{N}, |\,) \to (\mathbb{N}, \leq)$ no es un isomorfismo de posets. Sin embargo, esto NO implica que estos posets no sean isomorfos, pues podría existir otra función que sí sea un isomorfismo. En general, para probar que dos posets no son isomorfos debemos encontrar alguna propiedad que se preserve por isomorfismos y que tenga uno de ellos pero no tenga el otro. Estas propiedades se denominan **invariantes**. Dejamos como ejercicio probar el siguiente resultado en el que incluimos los invariantes fundamentales por isomorfismos de posets:

Teorema **11.** *Sean* $(A, \preceq_A)$, $(B, \preceq_B)$ *posets y sea* $f : (A, \preceq_A) \to (B, \preceq_B)$ *un isomorfismo. Entonces:*

1. *A y B tienen el mismo cardinal.*
2. *A es totalmente ordenado si y sólo si B es totalmente ordenado.*
3. *$a \in A$ es un elemento maximal (resp. minimal) de A si y sólo si $f(a)$ es un elemento maximal (resp. minimal) de B.*
4. *$a \in A$ es un máximo (resp. mínimo) de A si y sólo si $f(a)$ es un máximo (resp. mínimo) de B.*
5. *Sea $X \subseteq A$. $a \in A$ es una cota superior (resp. inferior) de X si y sólo si $f(a)$ es una cota superior (resp. inferior) de $f(X)$.*
6. *Sea $X \subseteq A$. $a \in A$ es el supremo (resp. ínfimo) de X si y sólo si $f(a)$ es el supremo (resp. ínfimo) de $f(X)$.*

Ejemplo **24.** Claramente para cualquier poset $(A, \preceq)$, la función identidad $Id : (A, \preceq) \to (A, \preceq)$ es un isomorfismo de $(A, \preceq)$ en $(A, \preceq)$.

Esto no es cierto si en A tomamos dos órdenes distintos. En efecto, como vimos, la función identidad $Id : (\mathbb{N}, |\,) \to (\mathbb{N}, \leq)$ no es un isomorfismo de posets.

Más aún, estos posets no son isomorfos pues $(\mathbb{N}, \leq)$ es totalmente ordenado y $(\mathbb{N}, |\,)$ no lo es (o sea, no puede existir ninguna otra función entre ellos que sea un isomorfismo de posets).

Ejemplo **25.** Sea A un conjunto finito de cardinal n y sean $\preceq$ y $\ll$ dos órdenes totales en A. Observemos que como A es finito y todos sus elementos son comparables 2 a 2 para $\preceq$, podemos escribir $A = \{a_1, a_2, \ldots, a_n\}$ donde

$$a_1 \preceq a_2 \preceq \cdots \preceq a_n$$

y más aún, $a_i \preceq_A a_j$ si y sólo si $i \leq j$.

Como A es también totalmente ordenado para $\ll$, existirá una permutación $\Phi : \{1, \ldots, n\} \to \{1, \ldots, n\}$ (o sea, una función biyectiva), tal que

$$a_{\Phi(1)} \ll a_{\Phi(2)} \ll \cdots \ll a_{\Phi(n)}$$

y nuevamente tenemos que $a_{\Phi(i)} \ll a_{\Phi(j)}$ si y sólo si $i \leq j$.

Consideremos la función $f : (A, \preceq) \to (A, \ll)$ dada por

$$f(a_i) = a_{\Phi(i)}.$$

Claramente f es biyectiva, pues Φ es biyectiva. Sean $x, y \in A$. Existirán $i, j \in \{1, \ldots, n\}$ tales que $x = a_i$ e $y = a_j$. Entonces

$$x \preceq y \iff a_i \preceq a_j \iff i \leq j \iff a_{\Phi(i)} \ll a_{\Phi(j)} \iff f(x) \ll f(y).$$

Concluimos que f es un isomorfismo de $(A, \preceq)$ en $(A, \ll)$. Más aún, de este ejemplo obtenemos que existen $n!$ ordenes totales distintos en A (¿por qué?) todos isomorfos entre sí, y además todos isomorfos al conjunto totalmente ordenado $(\{1, \ldots, n\}, \leq)$. En consecuencia, dos conjuntos finitos totalmente ordenados del mismo cardinal son isomorfos.

Observemos que esto implica que si $\succeq$ es el orden inverso a $\preceq$ en A, entonces $(A, \preceq)$ y $(A, \succeq)$ son isomorfos. En efecto, si ordenamos $A = \{a_1, a_2, \ldots, a_n\}$ como antes, la función $g : (A, \preceq) \to (A, \succeq)$ dada por $g(a_j) = a_{(n+1)-j}$ es un isomorfismo de posets.

Ejemplo **26.** $(\mathbb{N}, \leq)$ y $(\mathbb{N}, \geq)$ son conjuntos totalmente ordenados no isomorfos, dado que $(\mathbb{N}, \leq)$ tiene mínimo y $(\mathbb{N}, \geq)$ no tiene. Sin embargo existe un **anti-isomorfismo** entre estos conjuntos (un anti-isomorfismo entre $(A, \preceq_A)$ y $(B, \preceq_B)$ es un isomorfismo de $(A, \preceq_A)$ en $(B, \succeq_B)$).

Consideremos ahora S_0 el conjunto de números naturales pares y S_1 el conjunto de números naturales impares. Observemos que $\{S_0, S_1\}$ es una partición de $\mathbb{N}$. Definamos la relación $\preceq$ en $\mathbb{N}$ como sigue:

- Si $x \in S_0$ y $y \in S_1$, $x \preceq y$.
- Si $x, y \in S_0$, $x \preceq y$ si y sólo si $x \leq y$.
- Si $x, y \in S_1$, $x \preceq y$ si y sólo si $y \leq x$.

Observemos que $\preceq$ es claramente reflexiva, pues un elemento $x \in \mathbb{N}$ está en sólo uno de los subconjuntos S_0 y S_1 y por lo tanto resulta $x \preceq x$ si y sólo si $x \leq x$ (si $x \in S_0$) o $x \geq x$ (si $x \in S_1$). Luego para cada $x \in \mathbb{N}$, $x \preceq x$.

Supongamos ahora que $x, y \in \mathbb{N}$ son tales que $x \preceq y$ y $y \preceq x$. Si $x \in S_0$ e $y \in S_0$, entonces $x \leq y$ y $y \leq x$ con lo cual $x = y$. Observemos que si $x \in S_0$, como $y \preceq x$, y no puede pertenecer a S_1, con lo cual el anterior es el único caso que puede darse.

Si ahora $x \in S_1$, como $x \preceq y$, tenemos que y no puede pertenecer a S_0, y por lo tanto el único caso que debemos analizar es $y \in S_1$. Tendremos entonces que

$$x \preceq y \ \wedge \ y \preceq x \implies x \geq y, \ \wedge \, y \geq x \implies x = y.$$

Concluimos que $\preceq$ es antisimétrica.

Procediendo de manera similar (analizando por casos), se prueba que $\preceq$ es transitiva (dejamos los detalles como ejercicio).

Luego $\preceq$ es una relación de orden en $\mathbb{N}$. Observemos que $(\mathbb{N}, \preceq)$ es totalmente ordenado. En efecto, sean $n, m \in \mathbb{N}$. Si $n = m$, n y m son claramente comparables así que supondremos que son distintos. Si $n \in S_0$ y $m \in S_1$, entonces por definición $n \preceq m$. Si $n \in S_1$ y $m \in S_0$, entonces $m \preceq n$. Si $n, m \in S_0$, como $n \leq m$ o $m \leq n$, resulta $n \preceq m$ o $m \preceq n$, y un razonamiento similar prueba que n y m son comparables si ambos están en S_1.

Veamos finalmente que $(\mathbb{N}, \leq)$ y $(\mathbb{N}, \preceq)$ no son isomorfos. Supongamos que existe un isomorfismo $f : (\mathbb{N}, \leq) \to (\mathbb{N}, \preceq)$ y sea $A = f^{-1}(S_1)$. Entonces $A \subseteq (\mathbb{N}, \leq)$ es no vacío y por lo tanto tiene un mínimo $a \in A$ (todo subconjunto de $(\mathbb{N}, \leq)$ tiene un mínimo. Este resultado muy intuitivo no es trivial, lo probaremos en la próxima sección). Luego, por el Teorema 11, $f(a)$ debe ser un mínimo de S_1. Sin embargo, si $f(a) \in S_1$, $f(a) + 2$ también es un elemento de S_1 tal que $f(a) + 2 > f(a)$, y por lo tanto $f(a) + 2 \prec f(a)$, lo que contradice la definición de mínimo.

De manera similar puede probarse que no existe un anti-isomorfismo de $(\mathbb{N}, \leq)$ en $(\mathbb{N}, \preceq)$.

7. Conjuntos bien ordenados

Definición **9.** *Un poset $(A, \preceq)$ se dice un **conjunto bien ordenado** si para cualquier subconjunto no vacío B de A, $(B, \preceq_{|B})$ tiene un mínimo (denominado **primer elemento**). La relación $\preceq$ se dice en este caso un **buen orden**.*

Ejemplos **27.**

1. $(\mathbb{R}, \leq)$ no es un conjunto bien ordenado. En efecto, basta considerar cualquier intervalo abierto (a, b), que con el orden restringido no tiene un mínimo.
2. Por el Corolario 6, todo conjunto finito totalmente ordenado es bien ordenado.
3. $(\mathbb{N}, \preceq)$, donde $\preceq$ es el orden del Ejemplo 26, no es bien ordenado (hemos probado allí que el subconjunto S_1 de números impares no tiene mínimo).

Lema **12.** *Si $(A, \preceq)$ es un conjunto bien ordenado, entonces $\preceq$ es un orden total.*

Demostración. Sean $x, y \in A$. Entonces $B = \{x, y\}$ es no vacío y por lo tanto tendrá un mínimo, que deberá ser x o y. Se debe verificar entonces $x \preceq y$ o $y \preceq x$, con lo cual x e y son comparables. □

Como consecuencia del Teorema 11 tenemos:

Lema **13.** *Si $(A, \preceq_A)$ y $(B, \preceq_B)$ son conjuntos ordenados isomorfos, entonces $(A, \preceq)$ es un conjunto bien ordenado si y sólo si $(B, \preceq_B)$ es bien ordenado.*

Teorema **14** (Principio del Buen Orden)**.** *$(\mathbb{N}, \leq)$ es un conjunto bien ordenado.*

Demostración. Sea $A \neq \emptyset$ un subconjunto de $\mathbb{N}$. Si $1 \in A$, entonces $1 \leq n$ para cada $n \in A$ y por lo tanto A tiene un mínimo. Supongamos entonces que $1 \notin A$ y, por el absurdo, que A no tiene mínimo. Consideremos el conjunto

$$K = \{k \in \mathbb{N} : k \notin A \text{ y } k < n, \ \forall n \in A\}.$$

Observemos que $1 \in K$. Tomemos $k \in K$ y veamos que $S(k) = k + 1 \in K$. Como $k \in K$, deberá ser $k' \in K$ para todo $k' \leq k$. En caso contrario, existiría un elemento $n \in A$ tal que $n \leq k'$ y por la transitividad de $\leq$, tendríamos $n \leq k$, lo que contradice el hecho que $k \in K$.

Como no existe ningún número natural entre k y $k + 1$ (este hecho puede probarse fácilmente usando los axiomas de Peano), deberá ser $k + 1 \leq n$ para cada $n \in A$. Luego si $k + 1 \in A$, $k + 1$ sería un primer elemento de A, lo cual es absurdo. Por lo tanto $k + 1 \notin A$ y por lo tanto $k + 1 \in K$.

Concluimos por el principio de inducción que $K = \mathbb{N}$, y por lo tanto $A = \emptyset$, lo que contradice la hipótesis. □

Observación **2.** *El Principio del Buen Orden es equivalente al Principio de Inducción, es decir, que si en los axiomas de Peano reemplazamos este último por el primero, obtendremos el Principio de Inducción como un Teorema.*

En efecto, supongamos que reemplazamos el Axioma 3 en los Axiomas de Peano por el enunciado del Principio del Buen Orden. Demostraremos entonces que el principio de inducción sigue siendo válido. Sea $K \subseteq \mathbb{N}$ tal que $1 \in K$ y si $k \in K$, entonces $S(k) \in K$. Debemos probar que $K = \mathbb{N}$. Consideremos entonces el conjunto $A = \mathbb{N} - K$. Si $A \neq \emptyset$, entonces por el Principio del Buen Orden existirá un primer elemento k_0 de A. Observemos que $k_0 \neq 1$ pues por hipótesis $1 \in K$. Sea k_0' tal que $S(k_0') = k_0$. Como k_0 es el primer elemento de A y $k_0' < k_0$, tendremos que $k_0' \notin A$. Luego $k_0' \in K$. Pero entonces, por hipótesis $k_0 = S(k_0') \in K$, lo cual es absurdo. Concluimos que $A = \emptyset$ y por lo tanto $K = \mathbb{N}$.

El Principio del Buen en $(\mathbb{N}, \preceq)$ permite demostrar muchas propiedades importantes de los números enteros. Antes de finalizar esta unidad con el principio de buena ordenación, incluimos una serie de estas propiedades que ya han aparecido o que serán útiles más adelante.

Teorema **15** (Algoritmo de la división)**.** *Sean a y b números enteros con $a > 0$. Entonces existen únicos números enteros q y r tales que $b = qa + r$ y $0 \leq r < a$.*

Demostración. Existencia: Comencemos observando que si $a \mid b$, entonces el resultado es válido tomando $r = 0$. Supongamos entonces que $a \nmid b$.

Sea $S = \{b - ta : t \in \mathbb{Z}, b - ta > 0\}$. Veamos primero que $S \neq \emptyset$. Si $b > 0$, tomando $t = 0$ resulta $b = b - ta > 0$ y por lo tanto $b \in S$. Si fuese $b \leq 0$, tomemos $t = b - 1 \in \mathbb{Z}$. Entonces

$$b - ta = b - (b - 1)a = b(1 - a) + a > 0$$

puesto que $a > 0$ y $(1 - a) \leq 0$. Luego $b - ta = b(1 - a) + a \in S$ y nuevamente $S \neq \emptyset$.

Como $S \subseteq \mathbb{N}$, por el principio de la buena ordenación, S tiene un elemento mínimo que denotaremos por r. En particular, como $r \in S$, existirá $q \in \mathbb{Z}$ tal que $r = b - qa$ y $r > 0$. Solo nos queda probar que $r < a$. Si fuese

$r = a$, tendríamos que $b = (q+1)a$ de donde $a \mid b$, en contra de lo que estamos suponiendo. Si fuese $r > a$, entonces $r = a + c$ para algún $c \in \mathbb{N}$ y entonces

$$b - qa = r = a + c \;\Rightarrow\; c = b - (q+1)a > 0$$

con lo cual $b - (q+1)a \in S$. Pero $b - (q+1)a < b - qa = r$ contradiciendo que r es el elemento mínimo de S. Concluimos que $0 \leq r < a$ como queríamos ver. Dejamos la prueba de la unicidad como ejercicio. □

Teorema **16.** *Cualesquiera sean $a, b \in \mathbb{N}$, existe el máximo común divisor de a y b.*

Demostración. Recordemos que el máximo común divisor de a y b, definido por (4), es un número natural c tal que $c \mid a$, $c \mid b$ y $d \mid c$ para cualquier otro divisor común d de a y b.

Consideremos el conjunto

$$S = \{as + bt \,:\, s, t \in \mathbb{Z},\, as + bt > 0\}$$

de las combinaciones lineales enteras positivas de a y b. Observemos que como $a + b > 0$ tomando $s = t = 1$ resulta $a + b \in S$, y por lo tanto $S \neq \emptyset$. Sea c el elemento mínimo de S (que existe por el Principio del Buen Orden). Afirmamos que c es el máximo común divisor de a y b.

Como $c \in S$, existirán $x, y \in \mathbb{Z}$ tales que $c = ax + by$.

Supongamos que $d \in \mathbb{N}$ es tal que $d \mid a$ y $d \mid b$. Entonces es fácil ver que d divide a cualquier combinación lineal entera de a y b. En particular, $d \mid c$. Solo nos queda ver entonces que $c \mid a$ y $c \mid b$.

Supongamos que $c \nmid a$. Por el algoritmo de la división, existirán $q \in \mathbb{Z}$ y $r \in \mathbb{N}$ tales que $a = qc + r$ y $r < c$. Entonces

$$r = a - cq = a - q(ax + by) = (1 - qx)a + (-qy)b > 0.$$

Luego $r \in S$, y como $r < c$ esto contradice el hecho que c es el mínimo de S. Por lo tanto $c \mid a$. De manera análoga se prueba que $c \mid b$. □

Corolario **17.** *El máximo común divisor entre a y b es la única combinación entera positiva de a y b que divide a a y b.*

Ejercicio **12.** *Demostrar el Corolario 17.*

Ejercicio **13.** *Sia $a_1, \ldots, a_n$ son números naturales, probar que existen su máximo común divisor y su mínimo común múltiplo (definido en (5)). Extender estos resultados a un conjunto finito de números enteros.*

Definición **10.** *Un número entero k se dice **primo** si tiene exactamente dos divisores positivos: 1 y k. Si k tiene más de dos divisores positivo, k se dice **compuesto** (en consecuencia 1 no es ni primo ni compuesto).*

*Dos enteros a y b se denominan **coprimos** o **primos relativos** si $mcd(a, b) = 1$ (mcd denota el máximo común divisor).*

Ejercicio **14.** *Probar que a y b son coprimos si y sólo si existen $x, y \in \mathbb{Z}$ tales que $ax + by = 1$.*

Teorema **18.** *Sea $n \in \mathbb{N}$ un número compuesto. Entonces existe un número primo p tal que $p \mid n$.*

Demostración. Supongamos lo contrario y consideremos el conjunto S de todos los números naturales compuestos que no tienen divisores primos. Estamos suponiendo que $S \neq \emptyset$, y por el principio de buena ordenación S tiene un elemento mínimo m. Entonces m es compuesto y por lo tanto $m = m_1 \cdot m_2$, con $1 < m_1 < m$ y $1 < m_2 < m$. De estas desigualdades obtenemos que ni m_1 ni m_2 están en S. Pero entonces alguno de los dos es primo, o alguno tiene un divisor primo, que a su vez será divisor de m. Esto contradice el hecho que $m \in S$, con lo cual $S = \emptyset$. □

Teorema **19** (Euclides)**.** *Existen infinitos números primos.*

Demostración. Supongamos por el contrario que existe sólo una cantidad finite $p_1, \ldots, p_k$ de números primos positivos y definamos

$$B = p_1 p_2 \cdot \ldots \cdot p_k + 1.$$

Como $B > p_i$ para cada $1 \leq i \leq k$, B no puede ser primo. Como además $B > 1$, B es compuesto. Así, por el Teorema 18, existe un primo, que deberá ser alguno de los p_i, digamos p_j, tal que $p_j \mid B$. Pero además $p_j \mid p_1 p_2 \cdot \ldots \cdot p_k$ de donde resulta que $p_j \mid 1$ lo cual es absurdo. □

Teorema **20** (Teorema Fundamental de la Aritmética)**.** *Cada entero $n > 1$ puede escribirse de manera única como un producto de factores primos, excepto por el orden de los mismos.*

Demostración. Existencia: Supongamos que la existencia de la factorización por primos no fuese cierta. Entonces, por el principio de buena ordenación, existirá un primer entero $m > 1$ tal que m no puede expresarse como producto de factores primos. En particular m no es primo (pues en ese caso constaría de un único factor primo) y por lo tanto, al ser $m > 1$, m debe ser compuesto.

Sean m_1, m_2 con $1 < m_1, m_2 < m$ tales que $m = m_1 m_2$. Como m es el menor número que no puede expresarse como producto de números primos, tanto m_1 como m_2 admitirán una factorización en factores primos, y por consiguiente también lo hará m, lo cual es absurdo.

Unicidad: Puesto que el Teorema es sobre números naturales mayores que uno, aplicaremos la forma alternativa del principio de inducción para el caso base $n_0 = 2$. El teorema es en este caso trivialmente cierto: siendo 2 un número primo, no admite ninguna otra descomposición en factores de ningún tipo. Supongamos que la unicidad es válida para todos los números naturales $2, 3, 4, \ldots, n-1$ y veamos que también es válida para n. Supongamos que n puede escribirse como

$$n = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k} = q_1^{t_1} q_2^{t_2} \cdots q_r^{t_r}$$

donde cada p_i y cada q_j es un número primo. También supondremos que los números están ordenados de modo que $p_1 < p_2 < \cdots < p_k$ y $q_1 < q_2 < \cdots < q_r$ y que cada $s_i \geq 1$, $r_j \geq 1$.

Tomemos el número primo p_1 y supongamos que $p_1 \neq q_j$ para cada $j = 1, \ldots, r$. Como p_1 y cada q_j son primos distintos, es fácil ver que $(p_1 : q_j^{t_j}) = 1$ para cada $j = 1, \ldots, r$. Por otra parte p_1 divide a $n = q_1^{t_1} \cdots q_r^{t_r}$. Como $(p_1 : q_1^{t_1}) = 1$, por el Ejercicio 18 de la Unidad 2, deberá ser

$$p_1 \mid q_2^{t_2} \cdots q_r^{t_r}.$$

Pero nuevamente, $(p_1 : q_2^{t_2}) = 1$ y por lo tanto

$$p_1 \mid q_3^{t_3} \cdots q_r^{t_r}.$$

Si aplicamos reiteradamente el mismo argumento llegaremos a que debe ser $p_1 \mid q_r^{s_r}$ lo que es absurdo. Por lo tanto, deberá existir j_0 tal que $p_1 = q_{j_0}$. Observemos que j_0 debe ser igual a 1. En efecto, tenemos que $q_1 \mid n$, y con el mismo argumento, existirá p_{i_0} tal que $q_1 = p_{i_0}$. Si $i_0 > 1$, como hemos ordenado los factores primos de menor a mayor, tendremos:

$$p_1 < p_{i_0} = q_1 < q_{j_0}$$

lo cual es absurso. Concluimos que $p_1 = q_1$.

Veamos ahora que $s_1 = t_1$. Recordemos que estamos realizando la prueba por inducción. Aplicaremos en este momento la hipótesis inductiva. Como $p_1 \mid n$ y $s_1 \geq 1$, tenemos que

$$n_1 = \frac{n}{p_1} = p_1^{s_1 - 1} p_2^{s_2} \cdots p_k^{s_k} = p_1^{t_1 - 1} q_2^{t_2} \cdots q_r^{t_r} \in \mathbb{Z}.$$

Pero $n_1 < n$, luego por hipótesis inductiva su factorización en primos es única salvo orden. Pero como los primos están ordenados de menor a mayor, concluimos que $k = r$, cada $p_i = q_i$ y cada $s_i = t_i$. □

Corolario **21.** *Sean $x, y \in \mathbb{N}$. Entonces el máximo común divisor de x e y ($mcd(x, y)$) es el producto de los factores primos comunes de x e y elevados al mínimo exponente en el que aparecen y el mínimo común múltiplo de x e y ($mcm(x, y)$) es el producto de los factores comunes y no comunes elevados al máximo exponente en el que aparecen.*

Para finalizar esta Unidad enunciaremos un resultado muy importante conocido como el **Principio de buena ordenación**. Este resultado es equivalente al Lema de Zorn (Teorema 7). Nos limitaremos a dar una prueba para conjuntos finitos o infinitos numerables.

Teorema **22** (Principio de buena ordenación)**.** *Todo conjunto no vacío X admite una relación de orden $\preceq$ tal que $(X, \preceq)$ es un conjunto bien ordenado.*

Demostración. Como hemos adelantado, haremos la prueba solo para el caso en que X es finito o X es infinito numerable. En el primer caso, $X = \{a_1, \ldots, a_n\}$ y por lo tanto definiendo $a_i \preceq a_j$ si y sólo si $i \leq j$, X resulta totamente ordenado. Luego cualquier subconjunto no vacío de $(X, \preceq)$ es finito y totalmente ordenado y por lo tanto tiene un mínimo.

Supongamos ahora que X es infinito numerable. Entonces existe una función biyectiva $f : \mathbb{N} \to X$. Podemos "copiar" el buen orden $\leq$ de $\mathbb{N}$ a X de la siguiente manera: si $x, y \in X$, definimos $\preceq$ en X tal que

$$x \preceq y \iff f^{-1}(x) \leq f^{-1}(y).$$

Observemos que por el Teorema 9 f^{-1} es un isomorfismo de orden, y por lo tanto $(X, \preceq)$ y $(\mathbb{N}, \leq)$ son isomorfos. Luego por el Lema 13 y el Principio del Buen Orden, $(X, \preceq)$ es un conjunto bien ordenado. □