Matemática Discreta[1]

Notas del curso 2024

Centro de Matemática
Facultad de Ciencias - Universidad de la República

por Emiliano Sequeira

[1]Estas notas son una adaptación de las notas del curso del año 2020. La presente versión se ajusta a lo dado en clase y aporta material extra en los apéndices de cada capítulo.

Índice general

Capítulo 1

Conjuntos y Funciones

La teoría de conjuntos es una teoría axiomática, es decir que parte de conceptos primitivos (en este caso el de *conjunto* y el de *pertenencia*) que están regidos por una lista de sentencias (axiomas) de las cuales se deducen todos los teoremas. En estas notas trabajaremos de manera un poco informal sin especificar los axiomas. Así, por ejemplo, mostraremos construcciones de ciertos conjuntos sin justificar por qué estos están bien definidos dentro de la teoría. Para un seguimiento más profundo de estos temas recomendamos por ejemplo la lectura de [H].

El concepto de **conjunto** representa la idea intuitiva de una colección de objetos, a los que llamamos **elementos**. Escribiremos $x \in X$ para indicar que el elemento x **pertenece** al conjunto X.

Un conjunto queda determinado por sus elementos, es decir que si X y Y son dos conjuntos, entonces $X = Y$ si y solo si tienen los mismos elementos. Esto nos dice que para definir un conjunto debemos, en principio, determinar cuáles son sus elementos. Esto lo podemos hacer, por ejemplo, enumerándolos explícitamente (*por extensión*) o identificarlos mediante una propiedad determinada (*por especificación*). Así por ejemplo puede definirse un conjunto X como el que contiene exactamente los elementos a,e,i,o y u, o como el conjunto de todas las vocales utilizadas en el español.

Decimos que un conjunto A está **contenido** o **incluido** en otro conjunto B si para todo $x \in A$ se tiene $x \in B$. También diremos en este caso que A es **subconjunto** de B o que B **contiene** a A y lo escribiremos $A \subset B$. Observar que $A = B$ si y solo si $A \subset B$ y $B \subset A$. También escribiremos $A \not\subset B$ para indicar que A no está incluido en B, y $A \subsetneq B$ para indicar que A está incluido en B pero estos conjuntos no son iguales.

Ejemplo 1.0.1. Definimos los siguientes conjuntos:

V_U es el conjunto de todos los seres vivos del Universo.

V_T es el conjunto de todos los seres vivos de la Tierra.

A es el conjunto de todos los animales.

P es el conjunto de todos los perros.

Según nuestro conocimiento podemos escribir: $P \subsetneq A \subsetneq V_T \subset V_U$.

El **conjunto vacío** se notará por $\emptyset$. Este es un conjunto que no tiene elementos. Observar que si X es cualquier conjunto, entonces $\emptyset \subset X$.

1.1. Operaciones entre conjuntos

La **unión** de dos conjuntos A y B es el conjunto

$$A \cup B = \{x : x \in A \text{ o } x \in B\}.$$

Observar que A y B son ambos subconjuntos de $A \cup B$. Más aún, $A \cup B$ es el menor conjunto que contiene a A y B, es decir que si otro conjunto C cumple $A \subset C$ y a $B \subset C$, entonces $A \cup B \subset C$.

A partir de la definición dada es claro que el conjunto vacío actúa como neutro de la unión, es decir que para todo conjunto A se tiene $A \cup \emptyset = A$.

Proposición 1.1.1. *La unión de conjuntos es asociativa. Es decir que si A, B y C son tres conjuntos, entonces*

$$A \cup (B \cup C) = (A \cup B) \cup C.$$

Demostración. Para esto simplemente observamos que $x \in A \cup (B \cup C)$ si y solo si se da alguna de las siguientes condiciones: (1) $x \in A$, (2) $x \in B$, (3) $x \in C$.

De la misma forma se observa que $x \in (A \cup B) \cup C$ si y solo si se cumple (1), (2) o (3). $\square$

Observar que la Proposición 1.1.1 permite dar una definición para la unión de tres conjuntos.

Consideremos ahora una colección de conjuntos $\mathcal{C}$ (es decir, $\mathcal{C}$ es un conjunto cuyos elementos son otros conjuntos). Definimos la unión de $\mathcal{C}$ por

$$\bigcup \mathcal{C} = \big\{x : x \in C \text{ para algún } C \in \mathcal{C}\big\}.$$

Observar que si $\mathcal{C} = \{A, B\}$, entonces

$$\bigcup \mathcal{C} = A \cup B.$$

Si tomamos los conjuntos $A_1, \ldots, A_n$ escribimos

$$A_1 \cup \ldots \cup A_n = \bigcup \mathcal{C},$$

donde $\mathcal{C} = \{A_1, \dots, A_n\}$.

Si $\{A_i\}_{i\in I}$ es una familia indexada de conjuntos (esto quiere decir que para cada $i \in I$ se tiene un conjunto A_i, más tarde se dará una definición más formal), definimos su unión por

$$\bigcup_{i\in I} A_i = \bigcup \mathcal{A},$$

donde $\mathcal{A} = \{A_i : i \in I\}$. Es decir,

$$\bigcup_{i\in I} A_i = \big\{x : x \in A_i \text{ para algún } i \in I\big\}.$$

Ejemplos 1.1.2. 1. Ponemos $A = \{*, +, -\}$ y $B = \{0, 1\}$ (considerar en ambos casos los elementos simplemente como símbolos), luego

$$A \cup B = \{*, +, -, 0, 1\}.$$

2. Sea I el conjunto de todos los equipos de la primera división del fútbol uruguayo y para cada $i \in I$ ponemos A_i el conjunto de todos los jugadores del equipo i. Luego $\bigcup_{i\in I} A_i$ es el conjunto de todos los jugadores de la primera división del futbol uruguayo.

Definimos la **intersección** de dos conjuntos A y B por

$$A \cap B = \big\{x : x \in A \text{ y } x \in B\big\}.$$

Este conjunto está contenido tanto en A como en B. Además, si otro conjunto C cumple $C \subset A$ y $C \subset B$, entonces $C \subset A \cap B$, es decir que $A \cap B$ es el conjunto más grande que está contenido tanto en A como en B.

Para esta operación el conjunto vacío no es neutro como para a unión. Lo que sucede es que $A \cap \emptyset = \emptyset$ para todo conjunto A.

Ejercicio 1.1.3. Probar que la intersección es asociativa.

En general, si $\mathcal{C}$ es una colección de conjuntos, su intersección es definida por

$$\bigcap \mathcal{C} = \big\{x : x \in C \ \forall C \in \mathcal{C}\big\}.$$

Si $\mathcal{C}$ está indexada ($\mathcal{C} = \{C_i\}_{i\in I}$), entonces también escribimos

$$\bigcap \mathcal{C} = \bigcap_{i\in I} C_i.$$

Ejemplos 1.1.4. 1. Consideramos $A = \{0, 1, 2, 3\}$ y $B = \{0, 2, 4, 6\}$, luego

$$A \cap B = \{0, 2\}.$$

2. Sea $\mathcal{C}$ la colección de todos los subconjuntos del conjunto $\{1, 2, \dots, 10\}$. Observamos que para cualquier número entre 1 y 10, existe un conjunto $C \subset \mathcal{C}$ que no lo tiene como elemento. Luego
$$\bigcap \mathcal{C} = \emptyset.$$

La **resta** de conjuntos se define de la siguiente manera:

$$A \setminus B = \big\{x \in A : x \notin B\big\}.$$

Observar que mientras la unión y la intersección son operaciones conmutativas ($A \cup B = B \cup A$ y $A \cap B = B \cap A$), la resta no lo es. Un ejemplo simple que muestra esto es el siguiente: si A es no vacío, entonces

$$A \setminus \emptyset = A \text{ y } \emptyset \setminus A = \emptyset.$$

Si $A \subset X$, entonces definimos el **complemento** de A en X como el conjunto $A^c = X \setminus A$. Esta notación será usada cuando sea claro cuál es el conjunto X.

Ejercicio 1.1.5. Probar que:

1. Si $A, B \subset X$, entonces $A \setminus B = A \cap B^c$.

2. Si $A \subset B \subset X$, entonces $B^c \subset A^c$ (tanto A^c como B^c son los complementos en X).

Ejercicio 1.1.6. (Leyes de De Morgan)

1. Sean A y B dos subconjuntos de un conjunto X. Probar
   - $(A \cup B)^c = A^c \cap B^c$, y
   - $(A \cap B)^c = A^c \cup B^c$.

2. Generalizando lo anterior, expresar $(\cup_{i \in I} A_i)^c$ y $(\cap_{i \in I} A_i)^c$ en función de los A_i^c. Donde $\{A_i\}_{i \in I}$ es una familia de subconjuntos de X.

Por último definimos el **producto cartesiano** de dos conjuntos A y B como el conjunto de pares ordenados formados por un elemento de A y un elemento de B. Esto es,
$$A \times B = \{(a, b) : a \in A \text{ y } b \in B\}.$$

Observar que como se trata de pares ordenados, el producto cartesiano no es conmutativo.

Ejemplos 1.1.7. 1. Si $A = \emptyset$ o $B = \emptyset$, entonces $A \times B = \emptyset$.

2. Si $A = \{1, 2\}$ y $B = \{6, 7, 8\}$, entonces

$$A \times B = \{(1, 6), (1, 7), (1, 8), (2, 6), (2, 7), (2, 8)\}.$$

3. La hora dada por un reloj electrónico tiene la forma xx:xx, donde los espacios de la izquierda corresponde a la hora y los de la derecha corresponde a los minutos. Podemos entonces ver el conjunto de los posibles horarios dados por el reloj como $A \times B$ donde
$$A = \{00, \ldots, 23\} \text{ y } B = \{00, \ldots, 59\}.$$

1.2. Funciones

Fijemos dos conjuntos X y Y. Se llama **relación** de X a Y a cualquier subconjunto de $X \times Y$.

Una **función** de X a Y es una relación $f \subset X \times Y$ que cumple que para todo $x \in X$ existe un único $y \in Y$ tal que $(x, y) \in f$. En este caso llamamos **dominio** de f al conjunto X y **codominio** al conjunto Y. Escribimos $f : X \to Y$ para indicar que f es una función de X a Y.

Ejemplos 1.2.1. 1. La única función posible $f : \emptyset \to Y$ es la función vacía, es decir, $f = \emptyset$.

2. Sea X cualquier conjunto. Definimos la función **identidad** en X por

$$id_X : X \to X,\ id_X(x) = x \ \ \forall x \in X.$$

3. Si $A \subset Y$ definimos la función **inclusión** por

$$i : A \to X,\ i(a) = a \ \ \forall a \in A.$$

Si $A = X$, entonces i no es otra cosa que la identidad.

4. Tomemos $y_0 \in Y$. La función constante y_0 es

$$f : X \to Y, f(x) = y_0 \ \ \forall x \in X.$$

5. Si $f : X \to Y$ es una función y $A \subset X$, podemos considerar la **restricción** de f a A como la función

$$f|_A : A \to Y,\ f|_A(a) = f(a) \ \ \forall a \in A.$$

Dada una función $f : X \to Y$ y dos conjuntos $A \subset X$ y $B \subset Y$, definimos

- El conjunto **imagen** de A por f como $f(A) = \{f(a) : a \in A\} \subset Y$.
- El conjunto **preimagen** de B por f como $f^{-1}(B) = \{a \in X : f(a) \in B\} \subset X$.

También denominaremos **imagen de f** al conjunto $f(X)$.

Observar que $f(X)$ puede no ser igual a Y. En caso de que así sea diremos que f es **sobreyectiva**. También diremos que f es **inyectiva** si $f(x) \neq f(x')$ si $x \neq x'$, es decir que $f(x) = f(x')$ implica $x = x'$; y que es **biyectiva** si es a la vez inyectiva y sobreyectiva.

Observación 1.2.2.
1. La inclusión $i : A \to X$ (si $A \subset X$) es siempre inyectiva pero no es sobreyectiva salvo que A sea igual a X.
2. Una función constante $f : X \to Y$ no es inyectiva, salvo que X sea un conjunto unitario; y solo es sobreyectiva si Y es un conjunto unitario.

Ejercicio 1.2.3. Consideremos una función $f : X \to Y$ y dos conjuntos $A \subset X$ y $B \subset Y$. Probar:

1. $A \subset f^{-1}(f(A))$ y la igualdad se da si y solo si f es inyectiva.
2. $f(f^{-1}(B)) \subset B$ y la igualdad se da si y solo si f es sobreyectiva.

Ejercicio 1.2.4. Probar que dadas una función $f : X \to Y$ y dos familias de subconjuntos $\{A_i\}_{i\in I}$ y $\{B_i\}_{i\in I}$ con $A_i \subset X$ y $B_i \subset Y$ para todo $i \in I$, se tiene

1. $f\left(\bigcup_{i\in I} A_i\right) = \bigcup_{i\in I} f(A_i)$.
2. $f\left(\bigcap_{i\in I} A_i\right) \subset \bigcap_{i\in I} f(A_i)$. ¿Se da la igualdad en general?
3. $f^{-1}\left(\bigcup_{i\in I} B_i\right) = \bigcup_{i\in I} f^{-1}(B_i)$.
4. $f^{-1}\left(\bigcap_{i\in I} B_i\right) = \bigcap_{i\in I} f^{-1}(B_i)$.

1.2.1. Composición y función inversa

La **composición** de dos funciones $f : X \to Y$ y $g : Y \to Z$ es la función

$$g \circ f : X \to Z, \quad g \circ f(x) = g(f(x)) \; \forall x \in X.$$

Observar que la composición de funciones es asociativa, es decir, $f \circ (g \circ h) = (f \circ g) \circ h$.

Ejercicio 1.2.5. Supongamos que tenemos dos funciones $f, g : X \to X$. ¿Se cumple necesariamente $f \circ g = g \circ f$?

En el caso $X = Z$ decimos que g es **inversa** de f si $g \circ f = id_X : X \to X$ y $f \circ g = id_Y : Y \to Y$. Si f tiene una inversa diremos que es **invertible**. Observar que si g es inversa de f, entonces f es inversa de g.

Proposición 1.2.6. *Tomemos una función $f : X \to Y$. Entonces f es invertible si y solo si es biyectiva.*

Demostración. ($\Rightarrow$) Sea g una inversa de f. Para ver que f es inyectiva supongamos que $f(x) = f(x')$, luego

$$x = g \circ f(x) = g(f(x)) = g(f(x')) = g \circ f(x') = x'.$$

Concluimos entonces que f es inyectiva.

Observar además que si $y \in Y$, entonces $f(g(y)) = y$, es decir que y está en la imagen de f. Luego f es sobreyectiva.

($\Leftarrow$) Ahora suponemos que f es biyectiva. Definimos la función g de la siguiente manera: para $y \in Y$ sabemos que existe un único $x \in X$ tal que $f(x) = y$. Ponemos entonces $g(y) = x$. Es directo ver que g es la inversa de f. $\square$

La proposición anterior tiene la siguiente consecuencia:

Proposición 1.2.7. *Si $f : X \to Y$ es una función invertible, entonces su inversa es única.*

Demostración. Supongamos que g y h son dos inversas de f, queremos ver que $g(y) = h(y)$ para todo $y \in Y$. Como f es biyectiva podemos tomar x tal que $f(x) = y$, luego

$$g(y) = g(f(x)) = x = h(f(x)) = h(y).$$

$\square$

En virtud de la proposición anterior podemos hablar de <u>la</u> *inversa* de una función invertible f (y no solo de <u>una</u> *inversa*), para la que adoptamos la notación f^{-1} (tener cuidado de no confundir con el conjunto de las preimágenes).

Ejercicio 1.2.8. Consideremos dos funciones $f : X \to Y$ y $g : Y \to Z$. Probar que

1. si f y g son inyectivas, entonces $g \circ f$ es inyectiva.
2. si f y g son sobreyectivas, entonces $g \circ f$ es sobreyectiva.
3. si f y g son biyectivas, entonces $g \circ f$ es biyectiva.

Una función $f : X \to Y$ es **invertible a izquierda** si existe $g : Y \to X$ tal que $g \circ f = id_X$. Por otro lado decimos que f es **invertible a derecha** si existe $g : Y \to X$ tal que $f \circ g = id_Y$.

Ejercicio 1.2.9. Probar que una función

1. es invertible a izquierda si y solo si es inyectiva.

2. es invertible a derecha si y solo si es sobreyectiva.

1.2.2. Familias indexadas de conjuntos y productos cartesianos

Una **familia indexada de conjuntos** es una colección de conjuntos $\mathcal{C}$ junto con una función sobreyectiva $f : I \to \mathcal{C}$, donde I es un conjunto al cual llamamos **conjunto de índices**. Usaremos la notación

$$\{C_i\}_{i \in I}$$

para referirnos a una familia de conjuntos indexada por I. En este caso C_i es el conjunto $f(i)$.

Observar que si por ejemplo la colección $\mathcal{C}$ tiene un solo conjunto C, entonces $\{C_i\}_{i \in I}$ es una forma de tomar tantas copias del conjunto C como elementos tenga I.

Recordemos la definición de producto cartesiano que vimos anteriormente. Observar que un par ordenado (a, b) puede verse como una función $f : \{0, 1\} \to A \cup B$, $f(0) = a$ y $f(1) = b$. Luego $A \times B$ puede ser visto como el conjunto de todas las funciones $f : \{0, 1\} \to A \cup B$ que cumplen $f(0) \in A$ y $f(1) \in B$. Esta idea nos permite generalizar la noción de producto cartesiano.

Sea $\{A_i\}_{i \in I}$ una familia indexada de conjuntos. Definimos su **producto cartesiano** como el conjunto

$$\prod_{i \in I} A_i = \left\{ f : I \to \bigcup_{i \in I} A_i : f(i) \in A_i \right\}.$$

Si $A_i = A$ para todo $i \in I$, entonces notaremos

$$\prod_{i \in I} A_i = A^I,$$

que es simplemente el conjunto de todas las funciones de I en A.

1.3. Apéndice

I. El conjunto de los números naturales $\mathbb{N}$, que se estudia en el Capítulo 2, puede construirse a partir del conjunto vacío de la siguiente manera:

$$\begin{aligned}
&0 := \emptyset \\
&1 := \{0\} = \{\emptyset\} \\
&2 := \{0,1\} = \{\emptyset, \{\emptyset\}\} \\
&3 := \{0,1,2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \\
&\vdots \\
&n := \{0, 1, \ldots, n-1\} \\
&\vdots
\end{aligned}$$

A partir de esta construcción es fácil definir el orden en los números naturales. Simplemente establecemos que $n < m$ si $n \in m$.

II. Así como consideramos conjuntos de números naturales, también podemos considerar otros conjuntos de números como $\mathbb{Z}$ (conjunto de números enteros), $\mathbb{Q}$ (conjunto de números racionales), $\mathbb{R}$ (conjunto de números reales) o $\mathbb{C}$ (conjunto de números complejos). Estos se relacionan de la siguiente forma:

$$\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C}.$$

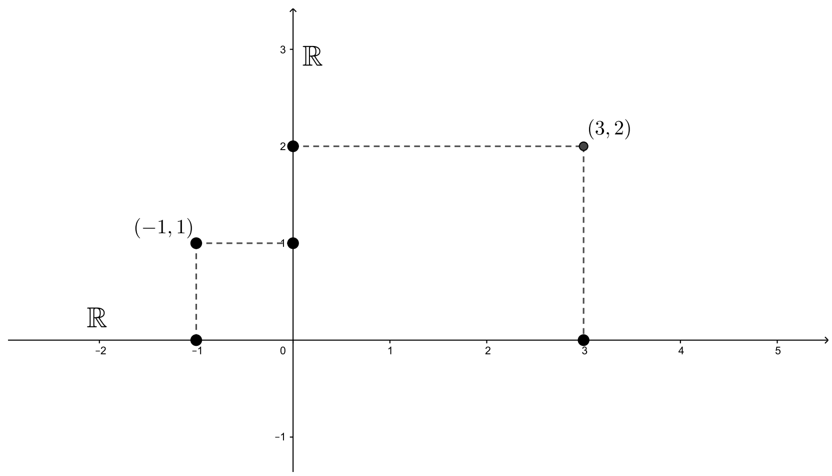
III. **Ejemplo:** Para cada número primo $p \in \mathbb{N}$ definimos el conjunto

$$A_p = \{pn : n \in \mathbb{N}\}.$$

Notamos por $\mathcal{P}$ al conjunto de todos los números primos, luego

$$\bigcup_{p \in \mathcal{P}} A_p = \{0, 1, 2, 3, 4, \ldots\} \text{ y } \bigcap_{p \in \mathcal{P}} A_p = \{0\}.$$

IV. **Ejemplo:** El producto cartesiano de la recta real $\mathbb{R}$ con si misma es el plano $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$. De esta manera los puntos del plano quedan determinados por sus dos coordenadas reales, como se ve en la siguiente figura.



V. Se puede definir la **unión disjunta** entre dos conjuntos A y B por

$$A \sqcup B = (A \times \{0\}) \cup (B \times \{1\}).$$

De esta forma A se identifica con el subconjunto $A \times \{0\}$ y B con el subconjunto $B \times \{1\}$.

VI. Una **sucesión** en un conjunto X es una función de la forma $f : \mathbb{N} \to X$. Se suele usar la notación $\{x_n\}$ o $\{a_n\}$ para indicar la función f (de esta forma $x_n = f(n)$ o $a_n = f(n)$). Según lo visto anteriormente el espacio de sucesiones en el conjunto X es $X^{\mathbb{N}}$. Veamos algunos ejemplos de sucesiones, reconociendo si se trata de funciones inyectivas y/o sobreyectivas.

1. La sucesión en $\mathbb{N}$ definida por $x_n = 2n$ es inyectiva pero no sobreyectiva. Lo mismo para la sucesión $x_n = n^2$.
2. La sucesión en $\mathbb{Z}$ dada por $x_n = (-1)^n$ no es ni inyectiva ni sobreyectiva.
3. La sucesión en $\mathbb{N}$ definida por $x_n = |10-n|$ es sobreyectiva pero no inyectiva. (Aquí $|x|$ indica el valor absoluto de x.)

Capítulo 2

Números naturales

En este capítulo trabajaremos con el conjunto de números naturales $\mathbb{N}$, entendiendo este como un conjunto que cumple las siguientes condiciones:

(1) Existe un elemento de $\mathbb{N}$ al que llamamos **cero** y denotamos por 0.

(2) Existe una función inyectiva $S : \mathbb{N} \to \mathbb{N}$ que cumple $S(\mathbb{N}) = \mathbb{N} \setminus \{0\}$. Llamamos a $S(n)$ el **sucesor** de n.

(3) **Principio de Inducción:** si $A \subset \mathbb{N}$ es un conjunto que contiene al cero y que cumple $S(A) \subset A$, entonces $A = \mathbb{N}$.

Las condiciones anteriores se conocen como *axiomas de Peano* y dan lugar a la teoría axiomática de los números naturales. De esta forma los primeros números naturales se expresan de la siguiente manera:

$$1 = S(0),\ 2 = S(1) = S(S(0)),\ 3 = S(2) = S(S(S(0))),\ \ldots$$

A veces se considera que 1 es el primer natural. En ese caso se debería cambiar 0 por 1 en los axiomas de Peano. En cualquier caso, la notación que se le da al primer elemento al que refieren los axiomas no es importante en esencia. De hecho, todas las ternas consistentes en un conjunto, un primer elemento y una función sucesor que satisfacen los axiomas de Peano son equivalentes. Para ser más precisos con esto podemos decir que si $(\mathbb{N}_1, x_1, S_1)$ y $(\mathbb{N}_2, x_2, S_2)$ son dos ternas que cumplen los axiomas de Peano, cada una de las cuales consiste en un conjunto, un primer elemento y una función sucesor, entonces existe una función biyectiva $f : \mathbb{N}_1 \to \mathbb{N}_2$ tal que $S_2 \circ f = f \circ S_1$. Damos una prueba de esto en el Apéndice.

Una particularidad importante de los naturales es que las funciones de la forma $f : \mathbb{N} \to X$ (donde X es un conjunto cualquiera) pueden ser definidas por recurrencia. Esto consiste en definir $f(0)$ y expresar $f(S(n))$ en función de $f(n)$. El Principio de Inducción es lo que garantiza que esta definición cubre todo el conjunto de los números naturales.

Más precisamente, puede pensarse que si $A \subset \mathbb{N}$ es el conjunto de los naturales n para los cuales $f(n)$ está definido, entonces claramente $0 \in A$, y si $n \in A$, entonces $S(n)$ también pertenece a A, ya que $f(S(n))$ está definio en función de $f(n)$, luego se debe cumplir $A = \mathbb{N}$. En la siguiente sección veremos varios ejemplos de este tipo de definiciones.

2.1. Operaciones en $\mathbb{N}$

Definimos la suma en $\mathbb{N}$ como una función $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ que cumple:

- $n + 0 = n$ para todo $n \in \mathbb{N}$.
- $n + S(m) = S(n + m)$ para todo $n, m \in \mathbb{N}$.

La definición anterior puede interpretarse de la siguiente manera: Para cada n se define por recurrencia una función $f_n : \mathbb{N} \to \mathbb{N}$ y luego se nota $n + m := f_n(m)$. Es decir que f_n es la función que suma n a izquierda.

Observar que $n + 1 = S(n + 0) = S(n)$. Esto nos da otra forma de notar al sucesor de un número natural.

Proposición 2.1.1. *La suma es asociativa, es decir,* $(n + m) + k = n + (m + k)$ *para todo* $k, n, m \in \mathbb{N}$.

Observar que la asociatividad de la suma nos permite escribir sin ambigüedad expresiones como $n + m + k := (n + m) + k = n + (m + k)$.

Demostración. Consideramos el conjunto

$$A = \big\{k \in \mathbb{N} : (n + m) + k = n + (m + k) \ \forall n, m \in \mathbb{N}\big\}.$$

Observamos que:

- $\underline{0 \in A}$: $(n + m) + 0 = n + m = n + (m + 0)$.
- $\underline{S(A) \subset A}$: Supongamos que $k \in A$, es decir, $(n + m) + k = n + (m + k)$ para todo $n, m \in \mathbb{N}$. Luego

  $$(n+m)+S(k) = S((n+m)+k) = S(n+(m+k)) = n+S(m+k) = n+(m+S(k)).$$

Luego por el Principio de Inducción $A = \mathbb{N}$. $\square$

La estructura de la demostración anterior se conoce como *prueba por inducción*, y consiste en probar que las dos condiciones del Principio de Inducción son satisfechas por conjunto conveniente para luego concluir que dicho conjunto coincide con $\mathbb{N}$. La primera condición ($0 \in A$) se denomina *paso base* y la segunda *paso inductivo*.

Observar que la pertenencia a A equivale a satisfacer una propiedad ($(n+m)+k = n+(m+k)$ para todo $n, m \in \mathbb{N}$). Por otro lado, dada dicha propiedad queda definido A como el conjunto de los naturales que la satisfacen. Esto permite reformular la prueba de la siguiente manera: sea P la propiedad definida por

$$P(n) \Leftrightarrow (n+m)+k = n+(m+k) \text{ para todo } n, m \in \mathbb{N}.$$

Luego probamos:

Paso base: $P(0)$ (o 0 satisface P).

Paso inductivo: $P(n) \Rightarrow P(n+1)$ (o, si n satisface P, entonces $S(n)$ también satisface P).

Tenemos entonces una formulación equivalente del Principio de Inducción en términos de propiedades en lugar de conjuntos. Vamos a aplicarlo en la demostración de la siguiente propiedad.

Lema 2.1.2. *Para todo $n \in \mathbb{N}$ se cumple $0 + n = n + 0 = n$ y $n + 1 = 1 + n$.*

Demostración. Definimos la propiedad P de forma tal que

$$P(n) \Leftrightarrow 0 + n = n.$$

Probarmos los dos pasos de la inducción:

Paso base: Es evidente ya que por definición de la suma $0 + 0 = 0$.

Paso inductivo: Supongamos que $0 + n = n$, luego $0 + S(n) = S(0 + n) = S(n)$.

Por el Principio de Inducción tenemos $0 + n = n = n + 0$ para todo $n \in \mathbb{N}$.

La otra parte se prueba de forma similar. □

De aquí en adelante no usaremos una notación determinada para referirnos a la propiedad P a la que hacemos referencia, simplemente explicitaremos qué es lo que deseamos probar.

Proposición 2.1.3. *La suma es conmutativa, es decir $n + m = m + n$ para todo $n, m \in \mathbb{N}$.*

Demostración. Ahora la propiedad a probar sobre n es que $n + m = m + n$ para todo $m \in \mathbb{N}$. Observar que el paso base se prueba en el lema anterior, así que resta probar el paso inductivo.

Supongamos que $n + m = m + n$ para todo $m \in \mathbb{N}$, luego

$$\begin{aligned} m + S(n) &= S(m + n) = S(n + m) = n + S(m) \\ &= n + (m + 1) = n + (1 + m) = (n + 1) + m = S(n) + m, \end{aligned}$$

donde en la primera, tercera y septima igualdad se usa la definición de la suma, en la segunda se usa la suposición de que n conmuta con todos los naturales, en quinta que 1 conmuta con todos los naturales (por le lema anterior) y en la sexta la propiedad asociativa. Tenemos entonces que $S(n) + m = m + S(n)$, lo que concluye la prueba por inducción. □

Probarmos una propiedad más de la suma:

Proposición 2.1.4. *Se cumple la propiedad cancelativa de la suma, es decir, si $n, m, k \in \mathbb{N}$ son tales que $n + k = m + k$, entonces $n = m$.*

Demostración. Lo probamos por inducción en k fijando n y m. Observamos primero que si $k = 0$ la igualdad nos queda $n = n + 0 = m + 0 = m$.

Supongamos que la propiedad se cumple para cierto k. Luego, si $n+S(k) = m+S(k)$, se tiene por la definición de la suma la igualdad $S(n + k) = S(m + k)$. La inyectividad de S implica $n + k = m + k$, de donde deducimos $n = m$.

Habiendo probado los dos pasos de la inducción concluimos la tesis de la proposición. □

Definimos el **producto** de la siguiente manera:

- $n \cdot 0 = 0$
- $n \cdot S(m) = n \cdot m + n$

Escribimos también $nm = n \cdot m$.

Proposición 2.1.5. *El producto es conmutativo, asociativo y cumple la propiedad distributiva con respecto a la suma, es decir:*

$$n(m + k) = nm + nk \ \forall n, m, k \in \mathbb{N}.$$

La prueba de la proposición anterior se deja como ejercicio. Se sugiere aplicar argumentos similares a los utilizados para probar las propiedades de la suma.

Proposición 2.1.6. *Si $n, m \neq 0$, entonces $nm \neq 0$.*

Demostración. Tanto n como m deben ser sucesores. Escribimos $n = S(n')$ y $m = S(m')$. Luego

$$nm = n \cdot S(m') = nm' + n = nm' + S(n') = S(nm' + n').$$

Tenemos entonces que nm es sucesor, por lo que no puede ser igual a 0. $\square$

Por último, de forma similar a como lo hicimos para la suma y el producto, definimos la **potencia**:

- $n^0 = 1$
- $n^{k+1} = n^k \cdot n$

Ejercicio 2.1.7. Probar que la potencia cumple las siguientes propiedades:

- $(nm)^k = n^k m^k$
- $n^{k+r} = n^k + n^r$
- $n^{kr} = \left(n^k\right)^r$

2.2. Orden en $\mathbb{N}$

Dados dos naturales n y m decimos que n es **menor o igual** a m (o que m es **mayor o igual** a n), y escribimos $n \leq m$, si existe $k \in \mathbb{N}$ tal que $n+k = m$. Si además $k \neq 0$ decimos que n es **menor** que m (o que m **mayor** que n), y escribiremos $n < m$. Esto último es equivalente a $n \leq m$ y $n \neq m$.

A partir de esto definimos la **resta** en $\mathbb{N}$ de la siguiente forma: si $n \leq m$, entonces $n - m$ es el único natural k que cumple $m = n + k$. Aquí la unicidad es garantizada por la propiedad cancelativa, ya que si $m = n + k = n + r$, entonces $k = r$.

Proposición 2.2.1. *1. $n \leq n$ y $n < S(n)$ para todo $n \in \mathbb{N}$.*

2. $0 \leq n$ para todo $n \in \mathbb{N}$, y si $n \leq 0$, entonces $n = 0$.

3. Si $n \leq m$ y $m \leq k$, entonces $n \leq k$.

4. Si $n \leq m$ y $m \leq n$, entonces $n = m$.

5. Dados $n, m \in \mathbb{N}$ se tiene o bien $n \leq m$ o bien $n \geq m$.

6. *Si* $n \leq m$ *y* $k \in \mathbb{N}$, *entonces*

$$n + k \leq m + k \text{ y } nk \leq mk.$$

Si $n < m$, *entonces* $n + k < m + k$; *y si además* $k \neq 0$, *entonces* $nk < mk$.

7. *Si* $n \leq x \leq S(n)$, *entonces* $x = n$ *o* $x = S(n)$.

El punto *2* dice que 0 es el elemento mínimo con respecto al orden definido. El punto *3* se conoce como *propiedad transitiva*, mientras que *4* es la *propiedad antisimétrica.* El punto *5* dice que todos los naturales son comparables, también se dice en este caso que el orden es *total.* El punto *6* expresa la *monotonía* de la suma y el producto. Por último, el punto *7* nos dice que el orden es discreto.

Demostración. 1. Es claro ya que $S(n) = n + 1$.

2. La primera parte es evidente. Supongamos que $n \leq 0$, luego existe $k \in \mathbb{N}$ tal que $n+k = 0$. Si $k \neq 0$, entonces k es sucesor, es decir que existe k' tal que $S(k') = k$, luego $0 = n + k = n + S(k') = S(n + k')$, es decir que 0 es sucesor, y esto es absurdo. Concluimos entonces que $k = 0$ y por lo tanto $0 = n + k = n + 0 = n$.

3. Tomamos $\ell, r \in \mathbb{N}$ tal que $n + \ell = m$ y $m + r = k$. Luego $n + \ell + r = k$, por lo que $n \leq k$.

4. Supongamos que $n + \ell = m$ y $m + r = n$, entonces $n = m + r = n + \ell + r$. Por la propiedad cancelativa de la suma se tiene $\ell + r = 0$ y por lo tanto $\ell, r \leq 0$. Por el punto *2* se tiene $\ell = r = 0$ y luego $n = m$.

5. Vamos a probarlo por inducción en n. Observar que si $n = 0$, entonces el punto *2* nos dice que n es comparable con todo $m \in \mathbb{N}$.

   Supongamos que n es comparable con todos los naturales, es decir que para todo $m \in \mathbb{N}$ se tiene $n \leq m$ o $m \geq n$. Para probar que esto también es cierto para $S(n)$ distinguimos dos casos:

   - Si $n \geq m$, entonces $S(n) \geq m$ por el punto *3*.
   - En el otro caso existe $k \neq 0$ tal que $m = n + k$. Como $k \neq 0$, este debe ser sucesor, por lo que existe $k' \in \mathbb{N}$ tal que $k = S(k')$, luego $m = n + S(k') = S(n) + k'$ y por lo tanto $S(n) \leq m$.

6. La primera parte es directa, ya que si $m = n + \ell$, entonces $m + k = n + k + \ell$. Además, si la desigualdad es estricta, entonces $\ell \neq 0$, por lo que la segunda desigualdad también es estricta.

   Para la otra parte tenemos $mk = (n + \ell)k = nk + \ell k$, por lo que $n + k \leq m + k$. Si $\ell, k \neq 0$, entonces la desigualdad es estricta.

7. Lo probamos por inducción.

   Para $n = 0$ tenemos $0 \leq x \leq 1$. Si $x \neq 0$, entonces x debe ser sucesor, es decir que existe $x' \in \mathbb{N}$ tal que $x' + 1 = x$. Por el punto anterior se tiene $1 = 0 + 1 \leq x' + 1 = x$. Por el punto *4* $x = 1$.

   Supongamos ahora que se cumple para n y tomemos $x \in \mathbb{N}$ tal que

   $$n + 1 \leq x \leq n + 2.$$

   Como x debe ser diferente de 0, debe tener un predecesor x'. Si $x' \geq n + 1$, entonces $n + 2 = n + 1 + 1 \leq x' + 1 = x$. Esto implica $x = n + 2$. Por otra parte, si $x' < n + 1$, entonces debe cumplirse $x' \leq n$ y entonces $x \leq n + 1$, por lo que $x = n + 1$.

□

Observación 2.2.2. Dado un $k \in \mathbb{N}$ consideramos el conjunto

$$N_k = \big\{n \in \mathbb{N} : n \geq k\big\}.$$

Este cumple los axiomas de Peano con k como su primer elemento. Para ver esto basta observar que $S\big(N(k)\big) = N_k \setminus \{k\}$ y que se cumple el Principio de Inducción a partir de k: Si $A \subset N_k$ contiene a k y cumple $S(A) \subset A$, entonces $A = N_k$.

Para probar esto último puede considerarse $\tilde{A} = A \cup N_k^c$. Es claro que $0 \in \tilde{A}$ ya que $0 \in N_k$. Además, si $n \in \tilde{A}$, entonces hay tres opciones:

- Si $n < k - 1$, entonces $S(n) = n + 1 \in N_k^c \subset \tilde{A}$.
- Si $n = k - 1$, entonces $S(n) = k \in A \subset \tilde{A}$.
- En el otro caso $n \in A$ y por lo tanto $S(n) \in A \subset \tilde{A}$.

Luego por el Principio de Inducción $\tilde{A} = \mathbb{N}$ y por lo tanto $A = N_k$.

Esto es lo que permite probar que ciertas propiedades se cumplen a partir de un natural en particular (no necesariemante desde cero).

2.3. Inducción fuerte y Principio del Buen Orden

El Principio de Inducción admite la siguiente formulación equivalente:

Principio de Inducción Fuerte: Todo subconjunto $A \subset \mathbb{N}$ que contiene a 0 y que cumple que $m \in A$ para todo $m < n$ implica $n \in A$, debe ser igual a $\mathbb{N}$.

Al igual que sucede con la primera formulación del Principio de Inducción, el Principio de Inducción Fuerte puede expresarse en función de una propiedad que puede ser satisfecha por los naturales: Si P es una propiedad (que puede o no satisfacer $n \in \mathbb{N}$) de forma tal que

- 0 satisface P (o $P(0)$), y
- $P(m)$ para todo $m < n$ implica $P(n)$,

entonces todo natural n satisface P.

Además, argumentando de forma similar a la Observarción 2.2.2 puede verse que la inducción fuerte puede hacerse a partir de cualquier natural.

Antes de probar la equivalencia entre el Principio de Inducción y el Principio de Inducción Fuerte veamos una aplicación de este último. Para esto haremos primero las siguientes definiciones:

- Diremos que un número natural m **divide** a otro natural n si existe $q \in \mathbb{N}$ tal que $n = mq$. También decimos en este caso que m es **divisor** de n o que n es **múltiplo** de m.
- Un natural p es **primo** si tiene exactamente dos divisores: 1 y p.

Observamos que si m es divisor de $n \neq 0$, entonces $m \leq n$ por el punto *6* de la Proposición 2.2.1. Por otro lado, cualquier natural es divisor de 0 y por lo tanto este no es primo.

También podemos observar que 1 no es primo ya que tiene un solo divisor. Sin embargo, $2 = S(1)$ es primo, ya que como todos sus divisores deben ser menores o iguales que 2 (y no nulos), entonces el punto *7* de la Proposición 2.2.1 nos dice que estos solo pueden ser 1 y 2.

Teorema 2.3.1. *Todo natural mayor o igual a 2 tiene un divisor primo.*

Demostración. El paso base ($n = 2$) está resuelto. Supongamos entonces que todo $m \in \mathbb{N}$ con $2 \leq m < n$ tiene un divisor primo. Si n no es primo, entonces debe tener un divisor k con $1 < k < n$. Esto implica que se puede escribir $k = pr$ con p primo y $r \in \mathbb{N}$, y luego $n = k\ell = pr\ell$ para algún $\ell \in \mathbb{N}$.

Por el Principio de Inducción Fuerte se deduce la tesis del teorema. $\square$

Proposición 2.3.2. *El Principio de Inducción (PI) es equivalente al Principio de Inducción Fuerte (PIF).*

Demostración. Supongamos que se cumple PIF. Observar que la hipótesis de PIF es más débil que la de PI, luego si se cumple la hipótesis de PI debe cumplirse la de PIF y luego su tesis (que es la misma tesis de PI). Esto prueba que PIF implica PI.

Supongamos ahora que se cumple PI y que $A \subset \mathbb{N}$ es un conjunto que contiene a 0 y que cada vez que se cumpla $m \in A$ para todo $m < n$ debe cumplirse $n \in A$. Vamos a probar que $A = \mathbb{N}$.

Definimos
$$\tilde{A} = \{n \in \mathbb{N} : m \in A \textit{ para todo } m \leq n\} \subset A.$$
Es claro que $0 \in \tilde{A}$. Además, si $n \in \tilde{A}$, entonces $n+1$ debe pertenecer a A y luego a $\tilde{A}$.

Por PI esto permite concluir que $\tilde{A} = \mathbb{N}$, y esto a su vez implica $A = \mathbb{N}$. □

El siguiente teorema es consecuencia del Principio de Inducción Fuerte.[1]

Teorema 2.3.3 (Principio del Buen Orden)**.** *Todo subconjunto no vacío de $\mathbb{N}$ tiene mínimo. Es decir, si $A \subset \mathbb{N}$ es no vacío, existe $m \in A$ tal que $m \leq n$ para todo $n \in A$.*

Demostración. Sea $A \subset \mathbb{N}$ no vacío. Si $0 \in A$, entonces 0 es mínimo (punto *2* de la Proposición 2.2.1). Supongamos que no es así y consideremos el conjunto A^c, que contiene a 0.

Como $A^c \neq \mathbb{N}$ no puede cumplirse el paso inductivo (de la inducción fuerte), es decir que no es cierto que $m \in A^c$ para todo $m < n$ implica $n \in A^c$. Esto nos dice que existe un natural n que no está en A^c (o, de forma equivalente, $n \in A$) que cumple que $m \in A^c$ para todo $m < n$. Este n debe ser el mínimo de A, ya que todos los naturales menores están en A^c. □

Como aplicación del Principio del Buen Orden obtenemos la siguiente propiedad, clásica en la teoría de los números naturales:

Teorema 2.3.4 (División entera)**.** *Sean n y m dos números naturales con $m \neq 0$. Entonces existen naturales q y r tales que*

(i) $n = qm + r$,

(ii) $r < m$.

Demostración. Si $n = 0$ entonces la tesis se cumple con $q = r = 0$.

Si $n \neq 0$ consideramos el conjunto
$$A = \{x \in \mathbb{N} : n < xm\}.$$
Observamos que $n + 1 \in A$; luego, al ser A no vacío, el Principio del Buen Orden nos dice que existe un mínimo $p \in A$. Este mínimo además tiene que ser diferente de 0 porque n lo es, luego tiene sentido considerar $q = p - 1$.

Podemos afirmar que $qm \leq n$, porque si no q pertenecería a A y eso no puede ser ya que p es el mínimo de este conjunto. Luego tiene sentido considerar $r = n - qm$, con lo que se cumple la igualdad (i).

[1] De hecho el Principio del Buen Orden es equivalente al Principio de Inducción. Se deja como ejercicio la otra implicación.

Veamos por último que $r < m$: si $m \leq r$, entonces tenemos

$$n = qm + r \geq qm + m = (q+1)m = pm.$$

Como $p \in A$ tenemos que $n < pm \leq n$, lo que es absurdo. $\square$

Ejercicio 2.3.5. Probar que la descomposición en el teorema anterior es única dado n y m.

2.4. Números enteros

La suma en $\mathbb{N}$ tiene un elemento neutro (el cero) y cumple que dados dos elementos $n, m \in \mathbb{N}^*$, se tiene $n+m > 0$. Es decir que una suma de elementos no nulos nunca puede dar cero, por lo que ningún número natural tiene *opuesto*. Si agregamos los opuestos de los números naturales construimos otro conjunto al que denominamos conjunto de *números enteros* y notamos por $\mathbb{Z}$. A continuación mostramos una manera de construir este conjunto.

Consideremos un elemento (fuera de $\mathbb{N}$) al que notamos por -1, luego ponemos

$$\mathbb{Z} = \big(\{-1\} \times \mathbb{N}^*\big) \cup \{(0,0)\} \cup \big(\{1\} \times \mathbb{N}^*\big), \tag{2.1}$$

donde $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$. De esta forma expresamos el signo de un elemento de $\mathbb{Z}$ en la primera coordenada y el valor absoluto en la segunda. El elemento 0 de $\mathbb{N}$ se identifica con $(0,0)$ y los $n \in \mathbb{N}^*$ con los pares de la forma $(1, n)$. En virtud de esta identificación notamos $(0,0) = 0$, $(1, n) = n$ y $(-1, n) = -n$.

Las operaciones y el orden en $\mathbb{Z}$ puede hacerse a partir de las operaciones y el orden definidos en $\mathbb{N}$. En este punto el lector está en condiciones de hacerlo como ejercicio, lo que sugerimos hacer (de todos modos lo hecemos en el Apéndice **II**). Lo que debe cumplirse al definir la suma es que $-n + n = 0$ (es decir que $-n$ es el opuesto de n).

2.5. Apéndice

I. Mostramos a continuación que todos los conjuntos (junto con su primer elemento y una función sucesor) que cumplen los axiomas de Peano son, en algún sentido, equivalentes.

Proposición 2.5.1. *Supongamos que* $(\mathbb{N}_1, x_1, S_1)$ *y* $(\mathbb{N}_2, x_2, S_2)$ *son dos ternas que cumplen los axiomas de Peano, entonces* $f : \mathbb{N}_1 \to \mathbb{N}_2$ *tal que* $S_2 \circ f = f \circ S_1$.

Demostración. Definimos la función f por recurrencia:

- $f(x_1) = x_2$
- Si $f(x) = y$, entonces $f(S_1(x)) = S_2(y)$.

Hay varias cosas a probar:

(i) $f(S_1(x)) = S_2(f(x))$ para todo $x \in \mathbb{N}_1$

(ii) f es biyectiva.

El primer punto es consecuencia directa de la definición de f y el Principio de Inducción. Para probar el segundo puede definirse por recurrencia una función $g : \mathbb{N}_2 \to \mathbb{N}_1$ de la siguiente manera:

- $g(x_2) = x_1$
- Si $g(y) = x$, entonces $g(S_2(y)) = S_1(x)$.

Consideremos el conjunto

$$A = \{x \in \mathbb{N}_1 : g(f(x)) = x\}.$$

Es claro que $g(f(x_1)) = x_1$. Además, si $x \in A$, luego

$$g(f(S_1(x))) = g(S_2(f(x))) = S_1(g(f(x))) = S_1(x),$$

por lo que $S_1(x) \in A$. Por inducción $A = \mathbb{N}_1$, es decir que $g \circ f = id_{\mathbb{N}_1}$. De forma análoga se prueba que $f \circ g = id_{\mathbb{N}_2}$, por lo que g es la inversa de f y como consecuencia f es biyectiva. □

II. Definimos la suma de $(\sigma_1, n), (\sigma_2, m) \in \mathbb{Z}$ de la siguiente manera:

- Si $\sigma_1 = \sigma_2 = \sigma$, entonces $(\sigma_1, n) + (\sigma_2, m) = (\sigma, n + m)$;
- si $\sigma_1 \neq \sigma_2$, entonces

$$(\sigma_1, n) + (\sigma_2, m) = \begin{cases} (\sigma_1, n - m) & \text{si } n > m \\ (\sigma_2, m - n) & \text{si } n < m. \\ (0, 0) & \text{si } n = m. \end{cases}$$

El producto se define por

$$(\sigma_1, n) \cdot (\sigma_2, m) = (\sigma_1 \cdot \sigma_2, n \cdot m),$$

donde se establece que

$$-1 \cdot (-1) = 1, \quad -1 \cdot 0 = 0 \cdot (-1) = 0 \quad y \quad -1 \cdot 1 = 1 \cdot (-1) = -1.$$

En $\mathbb{Z}$ puede definirse la resta para cualquier par de elementos x, y por

$$x - y = x + (-1 \cdot y).$$

Se deja como ejercicio probar que las propiedades de la suma y el producto de $\mathbb{N}$ se siguen cumpliendo para $\mathbb{Z}$.

El orden en $\mathbb{Z}$ se puede definir a partir de la suma de la misma forma que se hace para los naturales: Si $x, y \in \mathbb{Z}$, entonces $x \leq y$ si y solo si existe $k \in \mathbb{N}$ tal que $x + k = y$.

Capítulo 3

Relaciones

Como se ve en el Capítulo 1, una relación de un conjunto X a un conjunto Y es un subconjunto del producto cartesiano $X \times Y$. Allí definimos a las funciones como un tipo especial de relación. En este capítulo nos centraremos en relaciones contenidas en un producto de la forma $X \times X$. Una relación $\mathcal{R}$ de esta forma será llamada simplemente **relación en** X y escribiremos $x\mathcal{R}y$ si $(x, y) \in \mathcal{R}$, y $x \not\mathcal{R} y$ si $(x, y) \notin \mathcal{R}$.

La definición dada pretende modelar el concepto coloquial de relación y cobrará sentido en cada caso. Por ejemplo podemos considerar H el conjunto de la humaniad. Luego la relación de ser parientes puede caracterizarse como el conjunto de los pares $(x, y) \in H \times H$ que cumplen que x es parientes de y.

En este capítulo vamos a estudiar principalmente dos tipos especiales de relaciones: las relaciones de orden y las relaciones de equivalencia.

3.1. Relaciones de orden

En el capítulo anterior definimos en $\mathbb{N}$ las relaciones $\leq$ y $<$. En la Proposición 2.2.1 se muestran algunas propiedades de estas relaciones que serán importantes en este capítulo. Por ejemplo la relación $\leq$ cumple:

- $n \leq n$ para todo $n \in \mathbb{N}$ (es reflexiva)
- Si $n \leq m$ y $n \leq n$, entonces $n = m$ (es antisimétrica)
- Si $n \leq m$ y $m \leq k$, entonces $n \leq k$ (es transitiva)

Inspirados en este ejemplo haremos la siguiente definición general: Una relación $\mathcal{R}$ en un conjunto X es una **relación de orden amplio** si es reflexiva, antisimétrica y transitiva. Generalmente usaremos para las relaciones de orden amplio la notación: $\leq$ o $\preceq$.

Por otro lado, la relación $<$ en los naturales cumple:

- $n < m$ implica que no se cumple $m < n$ (es asimétrica)
- Si $n < m$ y $m < k$, entonces $n < k$ (es transitiva)

Decimos que $\mathcal{R}$ es una **relación de orden estricto** si es asimétrica y transitiva. Para las relaciones de orden estricto usamos generalmente la notación: $<$ o $\prec$.

Proposición 3.1.1. *Si $\leq$ es una relación de orden amplio en un conjunto, entonces la relación $<$ definida por*

$$x < y \Leftrightarrow x \leq y \text{ y } x \neq y$$

es una relación de orden estricto.

Por otro lado, si $<$ es una relación de orden estricto, entonces la relación definida por

$$x \leq y \Leftrightarrow x < y \text{ o } x = y$$

es una relación de orden amplio.

Demostración. Se deja como ejercicio. □

La proposición anterior nos dice que dar una relación de orden amplio o una relación de orden estrico es equivalente, es decir que al definir una se define automáticamente la otra. Otra forma de verlo es la siguiente: Si $\mathcal{R} \subset X \times X$ es una relación de orden amplio, entonces $\tilde{\mathcal{R}} = \mathcal{R} \setminus \{(x, x) : x \in X\}$ es una relación de orden estricto; por otro lado, si $\tilde{\mathcal{R}} \subset X \times X$ es una relación de orden estricto, entonces la relación $\mathcal{R} = \tilde{\mathcal{R}} \cup \{(x, x) : x \in X\}$ es de orden amplio.

Un **conjunto ordenado** es un par $(X, \mathcal{R})$ donde X es un conjunto y $\mathcal{R}$ es una relación de orden (amplio o estricto) en X. En virtud de la proposición anterior observamos que es lo mismo que $\mathcal{R}$ se a de orden amplio o estricto. Observar que si $A \subset X$, entonces la relación $\mathcal{R}$ define una relación de orden en A. Puede entonces considerarse el conjunto ordenado $(A, \mathcal{R})$ (donde se usa la notación $\mathcal{R}$ también para la restricción de la relación a A).

Ejemplos 3.1.2. Sea X un conjunto cualquiera.

1. La relación nula ($\emptyset \subset X \times X$) es de orden estricto en el conjunto X. Esta es la relación de orden estricto más chica que se puede definir en X.
2. La menor relación de orden amplio que se puede definir en X es la identidad: $\mathcal{R} = \{(x, x) : x \in X\}$. Además esta es la que corresponde a la relación vacía según la Proposición 3.1.1.

Diremos que $(X, \mathcal{R})$ es un **conjunto totalmente ordenado** si, como sucede con los números naturales, dado un par de elementos $x, y \in X$ con $x \neq y$, se tiene $x\mathcal{R}y$ o $y\mathcal{R}x$. Es decir que todos los elementos son comparables.

Ejemplos 3.1.3.

1. El orden usual en $\mathbb{Z}$ es definido de la siguiente manera:

$$x \leq y \Leftrightarrow x + k = y \text{ para algún } k \in \mathbb{N}.$$

   Esta relación de orden amplio es total.

2. Consideramos H el conjunto de la humanidad y definimos la relación $<$ por

$$x < y \Leftrightarrow x \text{ desciende de } y.$$

   Esta es una relación de orden estricto que no es total.

3. El alfabeto tiene un orden dado: $a < b < \cdots < z$. Consideramos ahora P el conjunto de todas las palabras del idioma español, luego definimos en P un orden (estricto) de la siguiente manera: si $p_1 = x_1 x_2 \ldots x_n$ y $p_2 = y_1 y_2 \ldots y_m$ son dos palabras, entonces $p_1 < p_2$ si y solo si se da una de las siguientes condiciones:

   - Existe un índice $i \in \big\{1, \ldots, \min\{n, m\}\big\}$ tal que $x_j = y_j$ para todo $j < i$ y $x_i < y_i$.
   - $x_i = y_i$ para todo $i \in \big\{1, \ldots, \min\{n, m\}\big\}$ y $n < m$.

   Este orden es total.

4. Sea $(X, \leq)$ e $(Y, \preceq)$ son dos conjuntos ordenados. En este caso $\leq$ y $\preceq$ denotan los órdenes amplios, y $<$ y $\prec$ denotan los correspondientes órdenes estrictos. Inspirados en el ejemplo anterior definimos el **orden lexicográfico** en el producto $X \times Y$ de la siguiente forma: $(x, y) \leq_L (x', y')$ si

   - $x < x'$, o
   - $x = x'$ e $y \preceq y'$,

   Observar que si $(X, \leq)$ e $(Y, \preceq)$ son conjuntos totalmente ordenados, entonces también lo es $(X \times Y, \leq_L)$.

   El orden lexicográfico puede definirse de forma similar en el producto de una cantidad finita cualquiera de conjuntos.

5. Dado un conjunto cualquiera X consideramos su **conjunto potencia** o **conjunto de partes**

$$\mathcal{P}(X) = \{A : A \subset X\}.$$

   Ponemos en $\mathcal{P}(X)$ el orden (amplio) $A \leq B$ si y solo si $A \subset B$. Este no es un orden total, salvo que X sea vacío o un conjunto unitario.

Fijemos ahora $(X, \leq)$ un conjunto ordenado (vamos a asumir que $\leq$ es una relación de orden amplio). Decimos que

- $m \in X$ es un elemento **minimal** si $x \leq m$ implica $x = m$.
- $M \in X$ es un elemento **maximal** si $M \leq x$ implica $x = m$.
- $m \in X$ es un **mínimo** si $m \leq x$ para todo $x \in X$.
- $M \in X$ es un **máximo** si $x \leq M$ para todo $x \in X$.

Observar que si $(X, \leq)$ tiene un máximo, entonces este es único y es claramente un elemento maximal. Algo análogo puede decirse del mínimo.

Ejemplos 3.1.4. 1. En el orden de la inclusión en $\mathcal{P}(X)$ tiene un mínimo, que es $\emptyset$, y un máximo, que es X.

2. En $X = \mathbb{N} \setminus \{0, 1\}$ definimos la siguiente relación de orden (amplio):

$$n \preceq m \text{ si } n \text{ es divisor de } m.$$

Observamos que:

- La relación de orden no es total, pues por ejemplo 2 y 3 no se relacionan entre sí.
- Los elementos minimales de X son los números primos.
- No existen elementos maximales en X.

Sea $(X, \leq)$ un conjunto ordenado y $A \subset X$. Decimos que un elemento $x \in X$ es:

- una **cota superior** de A si $a \leq x$ para todo $a \in A$.
- una **cota inferior** de A si $x \leq a$ para todo $a \in A$.

Ejemplos 3.1.5. 1. Consideramos $X = \{1, 2, 3, 4, 5\}$ y ponemos en $\mathcal{P}(X)$ el orden dado por la inclusión. Sea $\mathcal{P}_3 \subset \mathcal{P}$ la colección de subconjuntos de X con tres elementos. Observar que la única cota inferior de $\mathcal{P}_3$ es $\emptyset$ y la única cota superior es X.

2. En el producto $\mathbb{Z} \times \mathbb{Z}$ ponemos el orden lexicográfico en base al orden usual en $\mathbb{Z}$. Consideramos los conjuntos

$$A = \mathbb{Z} \times \{0\} \text{ y } B = \{0\} \times \mathbb{Z}.$$

Observar que A no tiene cota inferior ni cota superior, mientras que B si las tiene (por ejemplo $(-1, 0)$ es una cota inferior y $(1, 0)$ es una cota superior). Sin embargo B no tiene maximales ni minimales.

3.2. Relaciones de equivalencia

Una relación $\mathcal{R}$ en un conjunto X es una **relación de equivalencia** si es:

- reflexiva: $x\mathcal{R}x$ para todo $x \in X$.
- simétrica: $x\mathcal{R}y$ implica $y\mathcal{R}x$.
- transitiva: $x\mathcal{R}y$ e $y\mathcal{R}z$ implica $x\mathcal{R}z$.

Generalmente se usará para las relaciones de equivalencia la notación: $\sim$, $\approx$, $\simeq$, $\cong$, $\equiv$ o $\asymp$.

Ejemplos 3.2.1. 1. Consideramos el conjunto de todas las rectas del plano, notado por $\mathcal{R}$. Ponemos la siguiente relación:

$$r_1 \sim r_2 \Leftrightarrow r_1 \text{ paralela a } r_2.$$

Observar que $\sim$ es una relación de equivalencia en $\mathcal{R}$.

2. Fijemos $n \in \mathbb{Z}$ y consideremos en $\mathbb{Z}$ la relación $\equiv_n$, definida por

$$a \equiv_n b \Leftrightarrow a - b \text{ es múltiplo de } n.$$

Aquí la noción de *múltiplo* puede definirse de la misma forma que para los números naturales.

Veamos que esta es una relación de equivalencia:

- Es reflexiva: $a - a = 0$ es múltiplo de n para todo $a \in \mathbb{Z}$, es decir que $a \equiv_n a$ para todo a.
- Es simétrica: si $a \equiv_n b$, entonces $a - b = kn$ para algún $k \in \mathbb{Z}$. Luego $b - a = -kn$, lo que quiere decir que $b \equiv_n a$.
- Es transitiva: supongamos que $a \equiv_n b$ y $b \equiv_n c$. Esto implica que existen k y h tal que $a - b = kn$ y $b - c = hn$, luego

$$a - c = a - b + b - c = kn + hn = (k + h)n.$$

Por lo tanto $a \equiv_n c$.

Esta relación se conoce como **congruencia módulo** n.

Dada una relación de equivalencia $\sim$ en un conjunto X, definimos la **clase de equivalencia** de un elemento $x \in X$ como el subconjunto de todos los elementos de X que se relacionan con x, es decir,

$$[x] = \{y \in X : x \sim y\} \subset X.$$

Observar que la transitividad implica que si $x \sim y$, entonces $[x] = [y]$.

Por ejemplo, para la congruencia módulo 3 podemos mirar la clase del cero:

$$[0] = \{n \in \mathbb{Z} : n - 0 \text{ es múltiplo de } 3\} = \{3m : m \in \mathbb{Z}\}.$$

Este es el conjunto de todos los números enteros que son múltiplos de 3. En general, en la congruencia módulo n, la clase del 0 para la congruencia módulo n es siempre el conjunto de los múltiplos de n.

Definimos el **conjunto cociente** de una relación $\sim$ en X como el conjunto de todas las clases de equivalencia, esto es

$$X/\sim = \{[x] : x \in X\} \subset \mathcal{P}(X);$$

y la **proyección al cociente** como la función

$$\pi : X \to X/\sim, \ \pi(x) = [x].$$

Ejemplo 3.2.2. En la congruencia módulo n observamos que $a \equiv_n b$ si y solo si tienen el mismo resto al dividirlos entre n, es decir que si $a = nq_1 + r_1$ y $b = nq_2 + r_2$ son equivalentes si y solo si $r_1 = r_2$. Esto implica que

$$\mathbb{Z}_n := \big(\mathbb{Z}/\equiv_n\big) = \big\{[0], [1], \ldots, [n-1]\big\}.$$

Además, la proyección al cociente está dada por $\pi(a) = [r]$, donde $a = nq + r$.

En $\mathbb{Z}_n$ puede definirse una suma y un producto como sigue:

- $[a] + [b] = [a + b]$
- $[a] \cdot [b] = [a \cdot b]$.

Para ver que están bien definido hay que probar que no depende de los representantes que se tome en cada clase, es decir que si $a \cong_n a'$ y $b \cong_n b'$, entonces $[a + b] = [a' + b']$ y $[a \cdot b] = [a' \cdot b']$. Esto se deja como ejercicio.

3.2.1. Números racionales

Consideremos en el conjunto $X = \mathbb{Z} \times \mathbb{Z}^*$ la relación dada por

$$(n, m) \sim (k, r) \Leftrightarrow nr = mk.$$

Veamos primero que es una relación de equivalencia:

- Es reflexiva: $(n, m) \sim (n, m)$ porque claramente $nm = nm$.

- Es simétrica: si $(n,m) \sim (k,r)$, entonces $nr = mk$. Esto implica que $mk = nr$ y luego $(k,r) \sim (n,m)$.

- Supongamos que $(n,m) \sim (k,r)$ y $(k,r) \sim (\ell,h)$, es decir, $nr = mk$ y $kh = r\ell$. Luego multiplicando la primera igualdad por h se tiene

$$nrh = mkh = mr\ell.$$

  Como $r \neq 0$ podemos usar la propiedad cancelativa para obtener $nh = m\ell$*Probar como ejercicio que se cumple la propiedad cancelativa del producto en los enteros.*, lo que significa que $(n,m) \sim (\ell,h)$.

Adoptaremos la notación n/m para referirnos a la clase de (n,m) y escribimos $\mathbb{Q} := X/\sim$. Este cociente es el conjunto de los **números racionales**.

A partir de esta construcción podemos observar que los números enteros pueden verse como un subconjunto de los números racionales. Más precisamente lo hacemos mediante la función inyectiva

$$i : \mathbb{Z} \to \mathbb{Q},\ i(n) = \frac{n}{1}.$$

Definimos las operaciones suma y producto en $\mathbb{Q}$ de la siguiente manera:

$$\frac{n}{m} + \frac{k}{r} = \frac{nr + km}{mr}; \qquad \frac{n}{m} \cdot \frac{k}{r} = \frac{nk}{mr}.$$

Se deja como ejercicio probar que estas operaciones están bien definidas, es decir que si $n/m = n'/m'$ y $k/r = k'/r'$, entonces

$$\frac{nr + km}{mr} = \frac{n'r' + k'm'}{m'r'} \text{ y } \frac{nk}{mr} = \frac{n'k'}{m'r'}.$$

Observar que las operaciones definidas en $\mathbb{Q}$ extienden a las operaciones definidas en $\mathbb{Z}$:

$$i(n) + i(m) = \frac{n}{1} + \frac{m}{1} = \frac{n+m}{1} = i(n+m)$$

y

$$i(n) \cdot i(m) = \frac{n}{1} \cdot \frac{m}{1} = \frac{nm}{1} = i(nm).$$

La relación de orden usual en los números racionales es definida de la siguiente manera:

$$\frac{n}{m} \leq \frac{k}{r} \Leftrightarrow nr \leq km,$$

donde los representantes son tomados de forma tal que $m, r > 0$ y el símbolo $\leq$ en la derecha indica el orden de los enteros. Observar que $(\mathbb{Q}, \leq)$ es un conjunto totalmente ordenado.

3.2.2. Particiones

Una **partición** de un conjunto X es una familia P de subconjuntos de X (es decir que $P \subset \mathcal{P}(X)$) tal que:

1. Si A y B pertenecen a P y son diferentes, entonces $A \cap B = \emptyset$. Dicho de otra forma, los elementos de P son disjuntos dos a dos.

2. La unión de los elementos de P es todo X, es decir $\bigcup P = X$.

Ejemplos 3.2.3.
1. Si X es cualquier conjunto, entonces $P = \{\{x\} : x \in X\}$ es una partición; también lo es $P = \{X\}$.

2. Consideremos $X = \{1, 2, 3, 4, 5, 6\}$ y los subconjuntos
$$A = \{1\},\ B = \{2, 5\},\ C = \{3, 4, 6\} \text{ y } D = \{1, 6\}.$$
Aquí tenemos por ejemplo que $P_1 = \{A, B, C\}$ es una partición pero $P_2 = \{B, D\}$ y $P_3 = \{B, C, D\}$ no lo son.

En la siguiente proposición vemos que dar una relación de equivalencia en un conjunto es equivalente a dar una partición del mismo.

Proposición 3.2.4.
1. *Si $\sim$ es una relación de equivalencia en el conjunto X, entonces el cociente $X/\sim$ es una partición en X.*

2. *Sea P una partición en un conjunto X. Entonces existe una única relación de equivalencia $\sim$ en X tal que $X/\sim = P$.*

Demostración. Para probar la primera parte vemos primero que las clases de equivalencia de la relación $\sim$ son disjuntas dos a dos. Si no fuese así tendríamos dos clases diferentes $[x]$ e $[y]$ que no son disjuntas. Esto quiere decir que existe z en la intersección de ambas, o dicho de otro modo $z \sim x$ y $y \sim z$. La transitividad de $\sim$ implica que $x \sim y$ y luego $[x] = [y]$.

Por otro lado es claro que todo elemento $x \in X$ pertenece a una clase de equivalencia, luego la unión de todas las clases de equivalencia es el conjunto X.

Para la segunda parte alcanza con definir $\sim$ de la siguiente forma:
$$x \sim y \Leftrightarrow \exists A \in P \text{ tal que } x, y \in A.$$
No es dificil verificar que $\sim$ es una relación de equivalencia.

Para probar la unicidad supongamos que $\sim$ y $\simeq$ son dos relaciones de equivalencia tal que $X/\sim = X/\simeq = P$. Veamos que $x \sim y$ si y solo si $x \simeq y$:
$$\begin{aligned} x \sim y &\Leftrightarrow x \text{ e } y \text{ pertenecen a la misma clase de equivalencia para } \sim \\ &\Leftrightarrow x \text{ e } y \text{ pertenecen a la misma clase de equivalencia para } \simeq \\ &\Leftrightarrow x \simeq y. \end{aligned}$$
$\square$

3.3. Matriz asociada a una relación

Consideremos el conjunto $X = \{x_1, \dots, x_n\}$. La **matriz asociada** a una relación $\mathcal{R}$ en X es una matriz (a_{ij}) tal que

$$a_{ij} = \begin{cases} 1 & \text{si } x_i \mathcal{R} x_j \\ 0 & \text{en otro caso} \end{cases}$$

Tener en cuenta que la definición de matriz asociada depende del órden dado en el conjunto X, por lo que hay tres datos que son necesarios para determinarla: el conjunto, la relación y un órden total en el conjunto.

Ejemplo 3.3.1. Tomemos $X = \{1, 2, 3, 4\}$ y la relación

$$\mathcal{R} = \{(1,1), (1,2), (1,4), (2,3), (4,1), (4,4)\}.$$

Su matriz asociada nos queda:

$$\begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

Observar que dada una matriz de $n \times n$ y un conjunto X con n elementos dispuestos en cierto orden, existe una única relación de equivalencia cuya matriz asociada es la dada.

Ejercicio 3.3.2. Determinar qué propiedades tiene la matriz asociada a una relación:

1. Reflexiva
2. Simétrica
3. Antisimétrica
4. Asimétrica

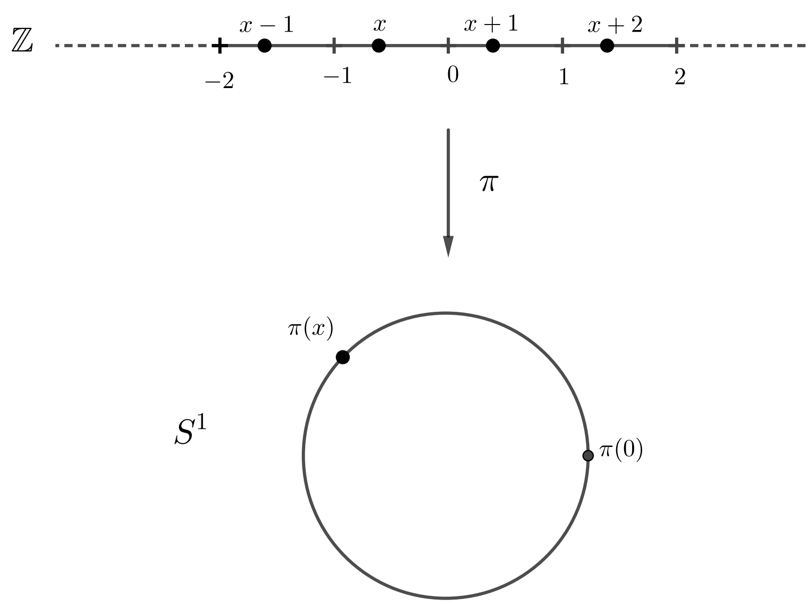
Más adelante nos interesará contar el número de relaciones que cumplan con determinadas propiedades. En ese caso la representación matricial de las relaciones nos será útil.

3.4. Apéndice

I. Ejemplo: Ponemos en $\mathbb{R}$ la siguiente relación:

$$x \sim y \Leftrightarrow x - y \in \mathbb{Z}.$$

Se deja como ejercicio probar que $\sim$ es una relación de equivalencia.



El conjunto cociente de esta relación puede verse geométricamente como el círculo

$$S^1 = \{z \in \mathbb{C} : |z| = 1\}.$$

Observar que de esta forma la proyección queda $\pi : \mathbb{Z} \to S^1,\ \pi(x) = e^{2\pi i x}$.

Capítulo 4

Finitud y numerabilidad

Nos enfocamos aquí en un par de preguntas:

- ¿Qué es contar?
- ¿Qué significa que un conjunto tenga n elementos?

Para ilustrar un poco esto antes de verlo más formalmente consideremos el conjunto $\{a, b, c, d, e\}$. Lo que uno hace al contar este conjunto es señalar cada elemento y decir en orden los números naturales a partir del 1, como se muestra en la siguiente figura:

$$\begin{array}{ccccc} \{a, & b, & c, & d, & e\} \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 & 4 & 5 \end{array}$$

Cuando ya no quedan elementos que etiquetar, se toma el último natural usado y se declara: "El conjunto tiene 5 elementos".

Mirando la figura podemos observar que allí se establece una función entre el conjunto $\{a, b, c, d, e\}$ y el conjunto $\{1, 2, 3, 4, 5\}$. Vemos además que esta función es biyectiva.

Podría pasar que dado un conjunto X no fuera posible llevar a cabo este proceso de manera de agotar todos sus elementos. En ese caso estamos en presencia de lo que llamamos un conjunto infinito.

4.1. Conjuntos finitos

Diremos que un conjunto X es **finito** si es vacío o bien existe una función biyectiva

$$f : \{1, \dots, n\} \to X$$

para algún $n \in \mathbb{N}^* = \mathbb{N} \setminus \{0\}$. En ese caso diremos que n es el **cardinal** de X (notamos $\#X = n$). Si X no es finito diremos que es **infinito**.

Para ver que no hay ambigüedad en la definición de cardinal hay que probar que si existe una función biyectiva $f : \{1, \dots, n\} \to X$, entonces no existe ninguna función biyectiva $g : \{1, \dots, m\} \to X$ con $n \neq m$. Esto es consecuencia del siguiente resultado:

Teorema 4.1.1 (Principio del Palomar)**.** *Consideremos un número natural cualquiera n. Luego no existe ninguna función de $\{1, \dots, n+1\}$ a $\{1, \dots, n\}$ que sea inyectiva.*

Demostración. Vamos a proceder por inducción en n.

Si $n = 1$, entonces existe una única función $f : \{1, 2\} \to \{1\}$, definida por

$$f(1) = f(2) = 1.$$

Es claro que f no es inyectiva.

Supongamos que no existe ninguna función inyectiva de $\{1, \dots, n+1\}$ a $\{1, \dots, n\}$ y que tenemos $f : \{1, \dots, n+2\} \to \{1, \dots, n+1\}$. Si f fuera inyectiva definiremos otra función inyectiva $g : \{1, \dots, n+1\} \to \{1, \dots, n\}$, lo que nos dara una contradicción con la hipótesis de inducción.

Distinguimos dos casos:

- Si $n+1 \notin f(\{1, \dots, n+1\})$, entonces podemos definir g como la restricción de f al conjunto $\{1, \dots, n+1\}$.

- En el otro caso ponemos $a \in f^{-1}(\{n+1\})$ y $b = f(n+2)$. Observar que $a \neq n+2$ y $b \neq n+1$. Definimos entonces g de la siguiente manera:

$$g(x) = \begin{cases} f(x) & \text{si } x \neq a \\ b & \text{si } x = a \end{cases}$$

  Esta función es inyectiva, lo que nos lleva a una contradicción.

Por Principio de Inducción tenemos la tesis del teorema. $\square$

El nombre *Principio del Palomar* se debe a su formulación más popular: No pueden meterse $n+1$ palomas en n jaulas sin que dos palomas compartan jaula.

Observar que si hay dos funciones biyectivas $f : \{1, \dots, n\} \to X$ y $g : \{1, \dots, m\} \to X$ con $n > m$, entonces $F = g^{-1} \circ f = \{1, \dots, n\} \to \{1, \dots, m\}$ es biyectiva. Esto niega el Principio del Palomar ya que $F|_{\{1,\dots,m+1\}} : \{1, \dots, m+1\} \to \{1, \dots, m\}$ es inyectiva. Concluimos entonces que el cardinal del conjunto X está bien definido.

Corolario 4.1.2. *1. Si $\#X = n$ y $\#Y = n$ con $n > m$, entonces no existe una función inyectiva $f : X \to Y$.*

2. $\mathbb{N}$ es un conjunto infinito.

Demostración. 1. Tomamos dos funciones biyectivas $g : \{1, \ldots, n\} \to X$ y $h : Y \to \{1, \ldots, m\}$. Si existe $f : X \to Y$ inyectiva, luego la función

$$F = h \circ f \circ g : \{1, \ldots, n\} \to \{1, \ldots, m\}$$

es inyectiva y por lo tanto también lo es $F|_{\{1,\ldots,m+1\}}$, lo que contradice el Principio del Palomar. Luego no existe tal función f.

2. Si $\mathbb{N}$ es finito, entonces existe $f : \mathbb{N} \to \{1, \ldots, n\}$ para algún $n \geq 1$ (sabemos que $\mathbb{N} \neq \emptyset$). Luego $f|_{\{1,\ldots,n+1\}}$ es inyectiva, lo que contradice el Principio del Palomar. $\square$

Decimos que dos conjuntos X e Y son **equipotentes** si existe una función biyectiva $f : X \to Y$. Notaremos en este caso $X \simeq Y$. A partir de esto uno puede decir que X tiene cardinal n si $X \simeq \{1, \ldots, n\}$.

Ejercicio 4.1.3. Sea $\mathcal{X}$ una colección de conjuntos. Probar que la equipotencia define una relación de equivalencia en $\mathcal{X}$. Describir su cociente en el caso de que los elementos de $\mathcal{X}$ sean todos conjuntos finitos.

Observar que si X e Y son equipotentes, entoces X es finito si y solo si Y lo es. En la siguiente proposición se ven otras formas de comprobar que un conjunto es finito a partir de la comparación con un segundo conjunto.

Proposición 4.1.4. *Sea X un conjunto finito. Entonces:*

1. si $A \subset X$, entonces A es finito.

2. si existe $f : Y \to X$ inyectiva, entonces Y es finito.

3. si existe $f : X \to Y$ sobreyectiva, entonces Y es finito.

Demostración. 1. Si $A = \emptyset$, entonces no hay nada que probar, por lo que asumiremos que $A \neq \emptyset$. Tomamos una función biyectiva $f : \{1, \ldots, n\} \to X$ y escribimos $f(k) = x_k$. Es decir que podemos escribir $X = \{x_1, \ldots, x_n\}$ y considerar en X el orden $x_1 < x_2 < \cdots < x_n$. Definimos por recurrencia la siguiente función:

- $h(1) = \min A$,
- Si $h(k)$ está definido y $A \neq \{h(1), \ldots, h(k)\}$, entonces ponemos $h(k + 1) = \min A \setminus \{h(1), \ldots, h(k)\}$.

Este proceso se termina si al cabo de m pasos se llega a $A = \{h(1), \ldots, h(m)\}$. En ese caso queda definida una función biyectiva $h : \{1, \ldots, m\} \to A$. Observamos que esto efectivamente sucede en a lo sumo n pasos porque para todo k se da $h(k) \geq x_k$.

2. Por la primera parte $f(Y) \subset X$ es finito; luego, como f es inyectiva, define una biyección entre Y y $f(Y)$, por lo que Y es finito.

3. Escribimos $X = \{x_1, \ldots, x_n\}$ y lo ordenamos como en la primera parte. Luego podemos definir la función $g : Y \to X$, $g(y) = \text{mín}\, f^{-1}(y)$. Como g es inyectiva la parte anterior nos dice que Y debe ser finito.

□

Para terminar con esta sección veamos cómo se comporta la noción de cardinal con las operaciones definidas para conjuntos.

Proposición 4.1.5. *Sean X e Y dos conjuntos finitos.*

1. *Si X y Y son disjuntos, entonces $\#(X \cup Y) = \#X + \#Y$.*
2. $\#(X \times Y) = (\#X) \cdot (\#Y)$.

Demostración. 1. Escribimos $X = \{x_1, \ldots, x_m\}$ e $Y = \{y_1, \ldots, y_n\}$. Definimos la función $f : \{1, \ldots, m+n\} \to X \cup Y$ por:

$$f(k) = \begin{cases} x_k & \text{si } k \leq m \\ y_{k-m} & \text{si } k > m \end{cases}$$

Puede verse de forma directa que f es biyectiva.

2. Para esta parte cambiamos un poco la numeración de X e Y y escribimos $X = \{x_0, \ldots, x_{n-1}\}$ e $Y = \{y_0, \ldots, y_{m-1}\}$. Definimos $g : \{0, \ldots, nm-1\} \to X \times Y$ por

$$g(k) = (x_r, y_q), \text{ donde } k = qm + r.$$

Puede verificarse que g es biyectiva observando que la función $(x_r, y_q) \mapsto qm + r$ es su inversa.

□

La primera igualdad de la proposición anterior se conoce como *Principio de la Suma* y es uno de los principios fundamentales de la combinatoria. Observar que como la unión y la suma son asociativas puede concluirse que si $A_1, \ldots, A_k$ son conjuntos disjuntos dos a dos, entonces

$$\#(\bigcup_{i=1}^{k} A_i) = \sum_{i=1}^{k} \#A_i.$$

La segunda igualdad se conoce como el *Principio del Producto*. Este será generalizado en el próximo capítulo con el fin de ser aplicado a problemas de conteo.

Corolario 4.1.6. *(Principio del Palomar, versión general) Sean n y m dos naturales no nulos, X un conjunto finito con $nm+1$ elementos e Y un conjunto finito con n elementos. Luego si $f : X \to Y$ es una función cualquiera, existe $y \in Y$ tal que $\#f^{-1}(y) \geq m+1$.*

Demostración. Escribimos $Y = \{y_1, \ldots, y_n\}$. Observamos que los conjuntos

$$f^{-1}(y_1), \ldots, f^{-1}(y_n)$$

son disjuntos, luego el Principio de la Suma nos dice que

$$\#X = \#\big(\bigcup_{i=1}^{i=n} f^{-1}(y_i)\big) = \sum_{i=1}^{k} \#f^{-1}(y_i).$$

Si $\#f^{-1}(y_i) \leq m$ para todo i se tendría $\#X \leq nm$, lo que es absurdo. Luego existe algún y_i con $\#f^{-1}(y) \geq m+1$. $\square$

El corolario anterior a menudo se enuncia de la siguiente manera: Si se meten $nm+1$ palomas en n jaulas, entonces alguna de las jaulas tendrá al menos $m+1$ palomas.

4.2. Conjuntos numerables

Tomemos un conjunto infinito X, luego podemos construir por recurrencia la siguiente función $f : \mathbb{N} \to X$:

- $f(0)$ es algún elemento de X.
- Si f está definida en $\{0, \ldots, n\}$, entonces $f(n+1)$ es un elemento de $X \setminus f\big(\{0, \ldots, n\}\big)$ (como X es infinito, este conjunto es siempre no vacío).

Observamos que f es inyectiva, luego define una biyección entre $\mathbb{N}$ y $f(\mathbb{N})$. Esto nos dice que todo conjunto infinito contiene una copia de $\mathbb{N}$. Si además f fuese sobreyectiva podríamos escribir $X = \{x_0, \ldots, x_n, \ldots\}$, donde $x_n = f(n)$. Es decir que la función f es una numeración del conjunto X. En general, diremos que un conjunto X es **numerable** si es finito o es equipotente con $\mathbb{N}$.

Tenemos la siguiente versión de la Proposición 4.1.4 para conjuntos numerables:

Proposición 4.2.1. *Sea X un conjunto infinito numerable. Entonces*

1. *si $A \subset X$, entonces A es numerable.*

2. *si existe $f : Y \to X$ inyectiva, entonces Y es numerable.*

3. *si existe $f : X \to Y$ sobreyectiva, entonces Y es numerable.*

Demostración. 1. Escribimos $X = \{x_0, x_1, x_2, \ldots\}$ y definimos en X el orden dado por $x_0 < x_1 < x_2 < \cdots$. Suponemos que A es no vacío.

Definimos por recurrencia la función f:

- $f(0) = \min A$
- $f(n+1) = \min A \setminus \{f(0), \ldots, f(n)\}$.

Si este proceso termina quiere decir que $A = \{f(0), \ldots, f(n)\}$ para algún n y luego f es una función biyectiva entre $\{f(0), \ldots, f(n)\}$ y A, lo que muestra que A es finito. Si no termina queda definida una función biyectiva de $\mathbb{N}$ a X.

2. El conjunto Y es equipotente con $f(Y)$, que es numerable por la parte anterior.

3. Definimos $g : Y \to X$ por
$$g(y) = \min f^{-1}(y).$$
Puede verificarse que g es inyectiva, luego Y es numerable.

$\square$

Ejemplo 4.2.2. Veamos que $\mathbb{Z}$ es numerable. Para esto basta con considerar la función biyectiva $f : \mathbb{N} \to \mathbb{Z}$ definida por

$$f(n) = \begin{cases} \frac{n}{2} & \text{si } n \text{ es par} \\ -\frac{n+1}{2} & \text{si } n \text{ es impar} \end{cases}$$

Veamos ahora lo que pasa con la unión y el producto cartesiano de conjuntos infinitos numerables, es decir, qué forma toman el Principio de la Suma y el Principio del Producto cuando sacamos la hipótesis de finitud.

Proposición 4.2.3. *Sean X e Y dos conjuntos equipotentes con $\mathbb{N}$. Entonces $X \cup Y$ y $X \times Y$ son equipotentes con $\mathbb{N}$*

Demostración. 1. Procedemos como en el Ejemplo 4.2.2. Empezamos numerando ambos conjuntos:

$$X = \{x_0, x_1, x_2 \ldots\}; \quad Y = \{y_0, y_1, y_2, \ldots\}.$$

Luego definimos la función $f : \mathbb{N} \to X \cup Y$ de forma tal que $f(2n) = x_n$ y $f(2n+1) = y_n$. Es fácil encontrar una inversa de f por lo que esta debe ser biyectiva.

2. Es claro que $X \times Y$ es infinito pues contiene al conjunto $X \times \{y_0\}$, que es equipotente con $\mathbb{N}$. Definimos la función

$$f : X \times Y \to \mathbb{N}, \ f(x_n, y_m) = 2^n 3^m.$$

Esta función es inyectiva[1], luego $X \times Y$ es numerable. Por ser infinito debe ser equipotente con $\mathbb{N}$.

□

Ejemplo 4.2.4. Veamos que el conjunto de números racionales $\mathbb{Q}$ es numerable. Para esto primero observamos que $X = \mathbb{Z} \times \mathbb{Z}^*$ es numerable por la proposición anterior. Luego, como la proyección al cociente $\pi : X \to \mathbb{Q}$ es sobreyectiva, podemos utilizar el punto 3 la Poposición 4.2.1 para concluir que $\mathbb{Q}$ es numerable.

Ejercicio 4.2.5. Probar que si $\{X_n\}_{n\in\mathbb{N}}$ es una familia de conjuntos numerables, entonces

$$\bigcup_{n\in\mathbb{N}} X_n$$

es también un conjunto numerable. Es decir que la unión de una cantidad numerable de conjuntos numerables es a su vez numerable.

4.3. Conjuntos no numerables

Tenemos entonces que tanto $\mathbb{Z}$ como $\mathbb{Q}$, que son conjuntos que contienen estrictamente a $\mathbb{N}$, son numerables. Sin embargo existe una diferencia esencial entre estos conjuntos y $\mathbb{R}$, como vemos a continuación.[2]

Proposición 4.3.1. *El conjunto de los números reales $\mathbb{R}$ no es numerable.*

Demostración. La prueba que presentamos utiliza una idea conocida como *argumento diagonal de Cantor* (en honor al matemático ruso-alemán Georg Cantor).

Vamos a probar que existe un subconjunto de $\mathbb{R}$ que no es numerable. Esto implicará que $\mathbb{R}$ tampoco lo es (pues los subconjuntos de un conjunto numerable son a su vez numerables). Definimos entonces $S \subset [0, 1)$ como el conjunto de números reales que tienen una expresión decimal que solo utiliza ceros y unos. Queremos ver que no existe una función sobreyectiva de $\mathbb{N}$ a S.

Veamos que dada una función $f : \mathbb{N} \to S$, existe un elemento de S que no está en la imagen de f. Para esto tomamos un número $x \in S$ tal que en el lugar k después de la

[1] Asumimos que todo número natural positivo tiene una única descomposición en factores primos.

[2] No daremos aquí una definición formal del conjunto de números reales. Puede pensarse en ellos como los números que se expresan de forma decimal con una cantidad (posiblemente infinita) de cifras después de la coma.

coma tenga una cifra (0 o 1) diferente al lugar k después de la coma de $f(k)$. Podemos observar que este x no está en la imagen de f porque para cualquier $k \in \mathbb{N}$ el lugar k después de la coma de x difiere del lugar k después de la coma de $f(k)$.

Un ejemplo de lo anterior puede verse a continuación:

$$\begin{aligned} f(1) &= 0,01100010100111\ldots \\ f(2) &= 0,01001110010101\ldots \\ f(3) &= 0,10100010010101\ldots \\ f(4) &= 0,00011101010100\ldots \\ &\vdots \end{aligned}$$

Aquí tenemos que el primer lugar después de la coma de $f(1)$ es 0, el segundo lugar después de la coma de $f(2)$ es 1, etc. Luego $x = 0,1000\ldots$ no está en la imagen de f. □

Tenemos entonces que existen conjuntos infinitos de diferentes órdenes ($\mathbb{N}$ y $\mathbb{R}$ por ejemplo). Podríamos decir que desde el punto de vista de su cardinal, $\mathbb{R}$ es estrictamente más grande que $\mathbb{N}$. A partir de esto surge la siguiente pregunta: ¿Existen órdenes de infinito más grandes que el de $\mathbb{R}$? Es decir: ¿Existe un conjunto X que no sea equipotente con $\mathbb{R}$ y una función inyectiva $f : \mathbb{R} \to X$?

El siguiente teorama responde a esta pregunta.

Teorema 4.3.2 (Cantor)**.** *Sea X un conjunto cualquiera. Entonces no existe uan función sobreyectiva $f : X \to \mathcal{P}(X)$. En particular X no es equipotente con $\mathcal{P}(X)$.*

Demostración. Supongamos que $f : X \to \mathcal{P}(X)$ es sobreyectiva. Definimos

$$A = \{x \in X : x \notin f(x)\} \in \mathcal{P}(X).$$

Como f es sobreyectiva, existe $a \in X$ tal que $f(a) = A$. Nos preguntamos entonces si a pertenece o no a A. Estudiamos las dos opciones:

- Si $a \in A$, entonces por la definición de A se tiene que $a \notin f(a) = A$, lo que es absurdo.
- Si $a \notin A$, entonces $a \notin f(a)$ y por lo tanto $a \in A$, que también es absurdo.

Concluimos entonces que no puede existir dicha función f.

□

El Teorema de Cantor nos dice que existe una gran cantidad de ordenes diferentes de infinito pues puede construirse, por ejemplo, la sucesión de conjuntos

$$\mathbb{N},\ \mathcal{P}(\mathbb{N}),\ \mathcal{P}(\mathcal{P}(\mathbb{N})),\ \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N}))),\ \ldots$$

de forma tal que cada uno de ellos es estrictamente más grande que el anterior.

4.4. Apéndice

I. El hotel de Hilbert

Un viajero llegó a un hotel que se jactaba de tener infinitas habitaciones, cada una numerada con un número natural. Pero, lamentablemente, al solicitar una habitación el recepcionista le informó que el hotel estaba lleno. Entonces al viajero se le ocurrió una solución: que cada huesped se mudara al habitación siguiente, de esa forma la número 0 *quedaría libre para él.*

Luego de haberse instalado en la habitación número 0*, el viajero pasaba por la recepción cuando vio una gran muchedumbre. Al acercarse a ver que pasaba, se enteró de que había una excursión de infinitos viajeros (pero una cantidad numerable) solicitando habitaciones. Como le constaba que el hotel estaba lleno le propuso al recepcionista lo siguiente: que cada husped se mude a la habitación cuyo número sea el doble de la actual. Al hacerlo de esta forma hubo lugar para todos.*

(a) Reinterpretar este ejemplo en términos de conjuntos infinitos y equipotencia.

(b) Usar la parte anterior para dar una definición alternativa de conjunto infinito.

II. Teorema de Shröder-Bernstein

Si X e Y son dos conjuntos finitos, entonces la existencia de una función inyectiva $f : X \to Y$ implica que el cardinal de X es menor o igual al cardinal de Y, pues si se tienen dos funciones biyectivas $\alpha : X \to \{1, \dots, n\}$ y $\beta : Y \to \{1, \dots, m\}$, entonces la composición $\beta \circ f \circ \alpha^{-1} : \{1, \dots, n\} \to \{1, \dots, m\}$ es inyectiva. Por el Principio del Palomar la existencia de esta función implica $n \leq m$. Podemos concluir de aquí que si existen dos funciones inyectivas $f : X \to Y$ y $g : Y \to X$, entonces $X \simeq Y$ (en el caso de que X e Y sean finitos).

El caso infinito es un poco más difícil, sin embargo el resultado sigue siendo cierto. Lo enunciamos y demostramos a continuación:

Teorema 4.4.1 (Schröder-Bernstein)**.** *Sean X e Y dos conjuntos cualesquiera. Si existen dos funciones inyectivas $f : X \to Y$ y $g : Y \to X$, entonces X e Y son equipotentes.*

Demostración. Definimos la siguiente función $H : \mathcal{P}(X) \to \mathcal{P}(X)$ por

$$H(A) = X \setminus g(Y \setminus f(A)).$$

Vamos a probar que H tiene un punto fijo, es decir que existe $W \in \mathcal{P}(X)$ tal que $H(W) = W$. Para esto se considera

$$\mathcal{A} = \big\{A \in \mathcal{P}(X) : A \subset H(A)\big\},$$

luego ponemos

$$W = \bigcup_{A \in \mathcal{A}} A.$$

Por un lado se tiene

$$W = \bigcup_{A \in \mathcal{A}} A \subset \bigcup_{A \in \mathcal{A}} H(A) \subset H\left(\bigcup_{A \in \mathcal{A}} A\right) = H(W).$$

Por otro lado, lo anterior implica $H(W) \subset H(H(W))$, por lo que $H(W) \in \mathcal{A}$ y entonces se tiene $H(W) \subset W$.

Definimos ahora $h : X \to Y$ por

$$h(x) = \begin{cases} f(x) & \text{si } x \in W \\ g^{-1}(x) & \text{si } x \notin W \end{cases}$$

Observar que como $H(W) = W$, entonces $W^c = X \setminus W \subset g(Y)$, luego h está bien definida.

Como f y $g^{-1}|_{W^c}$ son inyectivas, para ver que h es inyectiva basta probar que si $x \in W$ y $x' \notin W$, entonces $f(x) \neq g^{-1}(x')$. Usando $H(W) = X \setminus g(Y \setminus f(W)) = W$ obtenemos $g(f(W)^c) = W^c$. Como g es inyectiva (ver Ejercicio 1.2.3), al aplicar g^{-1} de ambos lados de la igualdad tenemos

$$f(W)^c = g^{-1}(W^c),$$

es decir que los conjuntos $f(W)$ y $g^{-1}(W^c)$ son disjuntos. Luego $f(x) \neq g^{-1}(x')$. Además esto prueba la sobreyectividad, ya que si $y \in Y$ está en $f(W)$ luego está en $h(W)$, y si no es así $y \in g^{-1}(W^c)$ y por lo tanto $y \in h(W^c)$. $\square$

Capítulo 5

Combinatoria

En el capítulo anterior dijimos que un conjunto X es finito si para algún natural n existe una función biyectiva
$$f : \{1, \ldots, n\} \to X.$$
En ese caso decimos que n es el cardinal de X, o de forma más coloquial, que X tiene n elementos. Luego sabemos expresar de una forma precisa lo que significa *contar* un conjunto finito, que es en definitiva determinar su cardinal.

A lo largo de este capítulo trabajaremos sobre el problema de cómo contar, es decir, en desarrollar estrategias para determinar el cardinal de un conjunto finito.

Para ilustrar la complejidad que puede tener este problema planteemos dos preguntas:

1. ¿Cuál es el cardinal del siguiente conjunto de símbolos $\{*, 0, 35, +, a, k\}$?
2. ¿Cuántas palabras de cinco letras (no necesariamente pertenecientes al diccionario) no tienen dos vocales juntas?

El primer problema es muy sencillo, uno puede observar rápidamente que el conjunto tiene 6 elementos. Pero la resolución del segundo presenta cierta dificultad. Ya el conteo de todas las posibles palabras de largo 5 es un problema no trivial que equivale, por ejemplo, a contar funciones de la forma $f : \{1, \ldots, 5\} \to \mathcal{A}$ donde $\mathcal{A}$ es el abecedario. A esto se le suma la condición de que no puede haber dos vocales juntas, lo que agrega dificultad al problema.

5.1. Principios básicos de conteo

En el capítulo anterior probamos dos propiedades a las que llamamos *Principio de la Suma* y *Principio del Producto* (Ver Proposición 4.1.5). Estas serán el punto de partida de las estratégias de conteo que construiremos en el presente capítulo.

Una forma más coloquial de enunciar el Principio de la Suma es la siguiente:

Principio de la suma[1]**:** *Si una tarea puede ser realizada de m formas diferentes, una segunda tarea puede ser realizada en n formas diferentes y ambas no pueden realizarse simultáneamente, entonces hay $m + n$ formas de realizar una o la otra.*

A modo de ejemplo podríamos contemplar el siguiente problema:

Ejemplo 5.1.1. *En una esquina de la calle Cassinoni hay un bar llamado El Turco, atendido por su propio dueño (cuyo apodo le da el nombre al lugar). Sobre el mostrador el Turco tiene unos frascos de golosinas que suele dar a modo de cambio cuando no tiene monedas. Un día, para congraciarse con una niña que estaba sentada con su padre, el Turco le ofreció tomar una golosina de alguno de los dos frascos que tenía más a mano. En uno había 25 caramelos surtidos (todos diferentes), mientras que el otro contenía 10 chicles (también todos de diferente sabor). La niña calculó que tenía* $25 + 10 = 35$ *opciones para elegir su golosina.*

En el ejemplo anterior uno puede rápidamente interpretar cada frasco como un conjunto, y las opciones de escoger una golosina de un frasco como el cardinal de dicho conjunto. Por otro lado, la elección que se le ofrece a la niña es equivalente a juntar todas las golosinas en una bolsa y pedirle que saque de allí una unidad cualquiera. Este nuevo conjunto es la unión de los dos conjuntos anteriores. Luego si A es el conjunto de los caramelos y B es el conjunto de los chicles, el principio de la suma en este caso puede leerse como la igualdad $\#(A \cup B) = \#A + \#B$.

Por otro lado, el Principio del Producto puede enuncairse de la siguente forma:

Principio del producto[2]**:** *Si un procedimiento puede ser dividido en un primer paso para el cual hay m posibilidades y un segundo paso, y si para cada forma de realizar el primer paso hay luego n formas de realizar el segundo, entonces el procedimiento puede ser realizado de mn formas diferentes.*

Ejemplo 5.1.2. *Para darle un empuje al negocio, el Turco decide ofrecer para el almuerzo una fórmula consistente en plato principal y postre a un precio muy competitivo. Para el plato principal el bar dispone de siete opciones (tres de ellas son algún tipo de milanesa), mientras que tiene sólo cinco opciones de postre. ¿Cuantas fórmulas es posible armar?*

Reinterpretando lo anterior podemos llamar A al conjunto de platos principales y B al conjunto de postres. Luego podemos ver las diferentes formulas como el conjunto $A \times B$.

[1] Extraido textualmente de [G]
[2] También extraído de [G]

Sin embargo podemos observar que el Principio del Producto tal como lo hemos enunciado es más general que esto, ya que la Proposición 4.1.5 no contempla el siguiente ejemplo:

Ejemplo 5.1.3. *Un día el Turco decidió ofrecer otra promoción. Se trata de un plato principal entre las siguientes opciones: colita de cuadril al horno con puré, filete de merluza con ensalada o tarta de zapallitos. Con el plato principal se ofrece sin cargo la bebida con el siguiente criterio:*

- *La colita de cuadril (C) puede ir acompañada por vino tinto*[3]*, gaseosa sabor cola o agua con gas.*
- *El filete de merluza (M) puede ir acompañado con vino blanco, jugo de naranja o agua sin gas.*
- *La tarta de zapallitos (Z) puede ir con licuado de frutas, jugo de naranja o agua sin gas.*

Usando el principio del producto en el ejemplo anterior uno puede rápidamente concluir que las posibles combinaciones son $3 \cdot 3 = 9$. Podemos pensar que $A = \{C, M, Z\}$ es el conjunto de los platos principales, mientras que hay tres conjuntos diferentes de bebidas

- $B_C = \{\text{vino tinto}, \text{gaseosa cola}, \text{agua con gas}\}$
- $B_M = \{\text{vino blanco}, \text{jugo de naranja}, \text{agua sin gas}\}$
- $B_Z = \{\text{licuado de frutas}, \text{jugo de naranja}, \text{agua sin gas}\}$

El conjunto de opciones no puede codificarse por un producto cartesiano de una forma directa, sin embargo podemos ver que $\{B_C, B_M, B_Z\}$ es una familia de conjuntos indexada en A, y una opción admisible por *el Turco* es un par (x, y) donde $x \in A$ y $y \in B_x$. Generalizando esta observación podemos dar una versión del Principio del Producto:

Proposición 5.1.4. *Sean $A_1, \ldots, A_m$ conjuntos finitos con n elementos. Entonces el conjunto*

$$X = \{(i, a) : a \in A_i\}$$

tiene cardinal $m \cdot n$.

Demostración. Probaremos que X es equipotente con $\{1, \ldots, n\} \times \{1, \ldots, n\}$, luego por la Proposición 4.1.5 se obtiene lo buscado. Para esto escribimos para cada $i = 1, \ldots, m$, $A_i = \{a_1^i, \ldots, a_n^i\}$. Luego se define la función

$$f : \{1, \ldots, n\} \times \{1, \ldots, n\} \to X, \; f(i, j) = a_j^i.$$

Puede verse que f es biyectiva, lo que termina la prueba. □

[3]De caja, por supuesto.

5.1.1. Principio de Inclusión-Exclusión

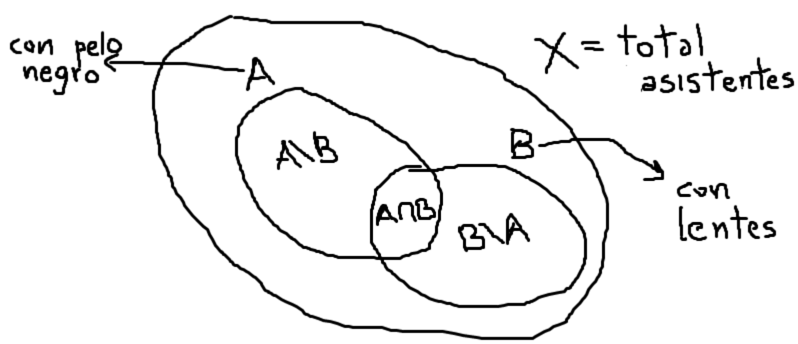
El Principio de la Suma resuelve el problema de contar los elementos de la unión de conjuntos disjuntos. Sin embargo este es un caso bastante particular y es natural preguntarse acerca de lo que sucede en caso de que los conjuntos que se están uniendo no sean disjuntos.

Ejemplo 5.1.5. *Noche de música en vivo en el bar El Turco. Se presentaba una banda de blues llamada La banda de Dieguito. Con el propósito de controlar que el número de asistentes no sobrepasara el límite habilitado por las autoridades, el Turco contrató al Comadreja, un hombre algo extraño que había llegado al bar unos días atrás pidiéndole una changa.*

Poco después de la medianoche el Turco se acercó a la puerta para preguntarle al Comadreja cuánta gente había entrado al local. Este le mostró una libreta donde tenía anotados algunos números. Según él, le había parecido aburrido contar una a una a todas las personas y prefirió hacerlo de forma indirecta. En su libreta aparecían los siguientes datos:

- 47 *tienen pelo negro.*
- 23 *usan lentes.*
- 17 *usan lentes y tienen el pelo negro.*
- 39 *no tienen el pelo negro ni usan lentes.*

Después de mostrarle estos números al Turco, el Comadreja sacó la lapicera que tenía apretada entre la oreja y el cráneo e hizo el siguiente dibujo:



Luego le explicó al Turco que había cuatro conjuntos disjuntos que considerar y que cada uno tenía su cardinal:

- $\#(A \cap B) = 17$
- $\#(A \setminus B) = \#A - \#(A \cap B) = 47 - 17 = 30$
- $\#(B \setminus A) = \#B - \#(A \cap B) = 23 - 17 = 6$
- $\#X \setminus (A \cup B) = \#(A \cup B)^c = 39$

Por el principio de la suma se tenía

$$\#X = \#(A \cup B)^c + \#(A \setminus B) + \#(B \setminus A) + \#(A \cap B) = 39 + 30 + 6 + 17 = 92.$$

Pero había otra forma de expresar esto:

$$\#X = \#(A \cup B)^c + \#A + \#B - \#(A \cap B). \tag{5.1}$$

Le explicó también que esta última igualdad se conocía como el principio de inclusión-exclusión.

– Fijate que al sumar los cardinales de A y B estás contando dos veces la intersección, por lo que tenés que restarle después el cardinal de esta para eliminar los repetidos, ¿entendés? - decía moviendo la lapicera sobre la hoja con entusiasmo.

Mientras el Comadreja conversaba de esto y se iba por las ramas entraron como 15 personas más sin que ninguno de los dos se diera cuenta. Adentro La banda de Dieguito tocaba The thrill is gone.

Lo anterior puede generalizarse para una cantidad finita arbitraria de conjuntos:

Teorema 5.1.6 (Principio de Inclusión-Exclusión)**.** *Consideremos $A_1, \dots, A_k$ una familia de conjuntos finitos. Luego*

$$\#\left(\bigcup_{1\le i\le k} A_i\right) = \left(\sum_{1\le i\le k} \#A_i\right) - \left(\sum_{1\le i<j\le k} \#(A_i \cap A_j)\right) + \cdots + (-1)^{k-1}\#\left(\bigcap_{1\le i\le k} A_i\right). \tag{5.2}$$

Demostración. Vamos a probarlo en por inducción en la cantidad de conjuntos $k \geq 2$. En el caso $k = 2$ tenemos

$$A_1 \cup A_2 = \big(A_1 \setminus (A_1 \cap A_2)\big) \cup \big(A_2 \setminus (A_1 \cap A_2)\big) \cup (A_1 \cap A_2).$$

Los tres conjuntos a la derecha de la igualdad son disjuntos dos a dos, por lo que la suma de sus cardinales es el cardinal de $A_1 \cup A_2$. Observamos (también por el Principio de la Suma) que además

$$\#\big(A_1 \setminus (A_1 \cap A_2)\big) = \#A_1 - \#(A_1 \cap A_2)$$

y que

$$\#\big(A_2 \setminus (A_1 \cap A_2)\big) = \#A_2 - \#(A_1 \cap A_2),$$

luego

$$\begin{aligned}\#(A_1 \cup A_2) &= \#A_1 - \#(A_1 \cap A_2) + \#A_2 - \#(A_1 \cap A_2) + \#(A_1 \cap A_2)\\ &= \#A_1 + \#A_2 - \#(A_1 \cap A_2).\end{aligned}$$

Supongamos ahora que el Principio de Inclusión-Exclusión se cumple para cierto k y consideremos una colección de conjuntos finitos $A_1, \ldots, A_{k+1}$. Aplicando la formula a los conjuntos $\bigcup_{1\le i\le k} A_i$ y A_{k+1} obtenemos

$$\#\left(\bigcup_{1\le i\le k+1} A_i\right) = \#\left(\bigcup_{1\le i\le k} A_i\right) + \#A_{k+1} - \#\left(\bigcup_{1\le i\le k} A_i \cap A_{k+1}\right). \tag{5.3}$$

Si desarrollamos el primer sumando del miembro derecho de (5.3) obtenemos exactamente (5.2), por otro lado, el tercer sumendo queda

$$\begin{aligned}\#\left(\bigcup_{1\le i\le k} A_i \cap A_{k+1}\right) = \left(\sum_{1\le i\le k} \#(A_i \cap A_{k+1})\right) - \left(\sum_{1\le i<j\le k} \#(A_i \cap A_j \cap A_{k+1})\right)\\ + \cdots + (-1)^{k-1}\#\left(\bigcap_{1\le i\le k+1} A_i\right).\end{aligned}$$

Sustituyendo ambos desarrollos en (5.3) obtebemos

$$\#\left(\bigcup_{1\le i\le k+1} A_i\right) = \left(\sum_{1\le i\le k+1} \#A_i\right) - \left(\sum_{1\le i<j\le k+1} \#(A_i \cap A_j)\right) + \cdots + (-1)^k \#\left(\bigcap_{1\le i\le k+1} A_i\right). \tag{5.4}$$

El Principio de Inducción prueba entonces el teorema. □

Ejemplo 5.1.7. Calculemos la cantidad de enteros positivos menores o iguales a 1000 que no son múltiplos ni de 2 ni de 3 ni de 5. Denotamos por A_2, A_3 y A_5 a los conjuntos de múltiplos de 2, 3 y 5 menores o iguales a 1000 respectivamente. Vemos que:

- $\#A_2 = \frac{1000}{2} = 500$
- $\#A_3 = \lfloor \frac{1000}{3} \rfloor = 333$
- $\#A_5 = \frac{1000}{5} = 200$
- $\#(A_2 \cap A_3) = \lfloor \frac{1000}{6} \rfloor = 166$

- $\#(A_2 \cap A_5) = \frac{1000}{10} = 100$
- $\#(A_3 \cap A_5) = \lfloor \frac{1000}{15} \rfloor = 66$
- $\#(A_2 \cap A_3 \cap A_5) = \lfloor \frac{1000}{30} \rfloor = 33.$

Por el Principio de Inclusión-Exclusión se tiene que la cantidad buscada es

$$1000 - 500 - 333 - 200 + 166 + 100 + 66 - 33 = 266.$$

5.2. Permutaciones

Consideremos el siguiente problema:

¿De cuántas formas se pueden ordenar las letras A,B,C,D,E y F?.

Observamos lo siguiente: Para ocupar el primer lugar tenemos 6 posibilidades. Luego de hacer la primera elección nos quedan 5 posibilidades para ocupar el siguiente lugar. Entonces por el principio del producto, tenemos $6 \cdot 5 = 30$ posibilidades para ocupar los dos primeros lugares. Siguiendo de este modo podemos concluir que la cantidad de formas de ordenar estas letras es $6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$. Esta cantidad puede verse también como la cantidad de palabras que pueden formarse con seis las letras dadas.

Como vemos en la siguiente proposición, el problema de ordenar símbolos diferentes es equivalente a otros problemas de formulación familiar.

Proposición 5.2.1. *Sean X e Y dos conjuntos con n elementos. Entonces los siguientes conjuntos son equipotentes dos a dos:*

- *El conjunto de todas las relaciones de orden total en X.*
- *El conjunto de todas las relaciones de orden total en $\{1, \ldots, n\}$.*
- *El conjunto de todas las funciones biyectivas de X a Y.*
- *El conjunto de todas las funciones biyectivas de $\{1, \ldots, n\}$ en si mismo.*

Demostración. La equipotencia entre los dos primeros conjuntos y el tercero con el cuarto salen de la existencia de funciones biyectivas $h_1 : \{1, \ldots, n\} \to X$ y $h_2 : \{1, \ldots, n\} \to Y$.

La equipotencia entre el segundo y el cuarto puede probarse definiendo una función que identifique una función $f : \{1, \ldots, n\} \to \{1, \ldots, n\}$ con la única relación de orden $<$ en el codominio $\{1, \ldots, n\}$ que hace que la función f sea creciente, es decir,

$$f(1) < f(2) < \cdots < f(n).$$

$\square$

El cardinal de los conjuntos mencionados en la proposición anterior se conoce como **número de permutaciones de n elementos**.

En el primer ejemplo vimos que $P_6 = 6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2$. Esto nos da una idea de lo que debe ser P_n para cualquier n, que se plasma en el siguiente resultado:

Teorema 5.2.2. *Para todo* $n \in \mathbb{N}$ *se tiene* $P_n = n! = n(n-1)\cdots 2 \cdot 1$.

Demostración. Vamos a probar la igualdad por inducción en n. Es claro que $P_1 = 1$ ya que existe una única función $f : \{1\} \to \{1\}$, o que existe una única relación de orden en el conjunto $\{1\}$.

Supongamos que $P_n = n!$. Esto quiere decir que existen $n!$ formas de ordenar un conjunto de n elementos. Luego observamos que ordenar el conjunto $\{1, \ldots, n+1\}$ es un proceso que se puede hacer en dos pasos:

- Se coloca primero un elemento en el lugar $n+1$. Para esto se tienen $n+1$ posibilidades.

- Se ordenan los restantes n elementos en los primeros n lugares. Para esto se tienen $P_n = n!$ posibilidades.

Por el principio del producto se tiene $P_{n+1} = (n+1) \cdot n! = (n+1)!$. $\square$

Observar que puede ponerse $P_0 = 1$, que es la cantidad de funciones de la forma $f : \emptyset \to \emptyset$.

Ejercicio 5.2.3. *Una cantidad n de personas se sentaron alrededor de una de las mesas circulares del bar El Turco para jugar un juego de cartas. La silla ocupada por cada persona no tenía ninguna injerencia en el juego, sin embargo la persona que cada jugador tuviera a la derecha o a la izquierda sí que la tenía. A algunos metros de la mesa, el Comadreja se vio interesado por saber cuál sería el número de configuraciones posibles. Como no tenía papel dejó escrito el número en la mesa después de hacer algunos cálculos mentales. ¿Cuál es este número?*

El número hallado en el ejercicio anterior es llamado **permutaciones circulares de n elementos**, al que podemos notar por PC_n. En el apéndice de este capítulo puede encontrarse un estudio más detallado de este número.

5.3. Arreglos

En la sección anterior consideramos las formas de reordenar n símbolos diferentes, lo que es igual al cardinal del conjunto de funciones biyectivas de $\{1, \ldots, n\}$ en sí mismo. Variemos un poco esto y consideremos para dos números naturales fijos k y n el siguiente conjunto:

$$\big\{f : \{1, \ldots, k\} \to \{1, \ldots, n\} : f \text{ es inyectiva}\big\}. \tag{5.5}$$

Observamos que si $k > n$, entonces el conjuto anterior se vacío por el Principio del Palomar, luego podemos considerar $k \leq n$.

El cardinal de (5.5) es llamado **arreglos de n elementos de largo k**. Este número también puede interpretarse como la cantidad de posibilidades de formar palabras de largo k usando n símbolos diferentes sin repetirlos.[4] La identificación de las funciones inyectivas con dichas palabras se obtiene por medio de la regla

$$f \mapsto f(1)f(2)\ldots f(k).$$

Es claro que en (5.5) puede cambiarse $\{1, \ldots, k\}$ y $\{1, \ldots, n\}$ por dos conjuntos arbitrarios de cardinales k y n respectivamente.

Teorema 5.3.1. *Para todo $n \in \mathbb{N}$ y $k \in \{0, \ldots, n\}$ se tiene*

$$A_k^n = \frac{n!}{(n-k)!}.$$

Demostración. Lo hacemos por inducción en n. Si $n = 0$, entonces $k = 0$ y existe una única función inyectiva de la forma $f : \emptyset \to \emptyset$, luego

$$A_0^0 = 1 = \frac{0!}{0!}.$$

Más en general, en el caso $k = 0$ se tiene claramente $A_0^{n+1} = 1 = \frac{(n+1)!}{(n+1)!}$.

Suponemos que la fórmula es cierta para n y todo $k \in \{1, \ldots, n\}$. Observemos que definir una función inyectiva $f : \{1, \ldots, k\} \to \{1, \ldots, n+1\}$ (con $1 \leq k \leq n+1$) puede hacerse en dos pasos:

1. Se elige $f(1)$, para lo cual se tienen $n + 1$ posibilidades.
2. Se completan las imágenes de los restantes números $2, \ldots, k$. Para esto se tienen A_{k-1}^n posibilidades.

Luego el Principio del Producto implica que la cantidad de formas de elegir f es

$$A_k^{n+1} = (n+1)A_{k-1}^n = \frac{(n+1)n!}{(n-(k-1))!} = \frac{(n+1)!}{((n+1)-k)!}.$$

El Principio de Inducción permite concluir la tesis. $\square$

[4] En la bibliografía la notación para los arreglos puede variar. Por ejemplo el cardinal de $\mathcal{A}(n, k)$ puede notarse A_n^k. Este número también puede encontrarse nombrado por "arreglos de k en n".

5.3.1. Arreglos con repetición

Supongamos ahora que permitimos repeticiones en el caso anterior, es decir, consideramos palabras de largo k escritas en un abecedario de n letras. La cantidad de formas de hacerlo se denotará por AR_k^n. Estos son los **arreglos con repetición de n elementos de largo k**. En este caso no es necesario que k sea menor o igual a n. Observar que este número es el cardinal del conjunto

$$\{1,\ldots,n\}^{\{1,\ldots,k\}} = \big\{f : \{1,\ldots,k\} \to \{1,\ldots,n\} : f \text{ función}\big\}.$$

Este es el producto cartesiano de $\{1,\ldots,n\}$ por si mismo k veces, luego por la regla del producto tenemos $\#AR_k^n = n^k$.

Observación 5.3.2. Veamos que $\{0,1\}^{\{1,\ldots,k\}}$, es equipotente con $\mathcal{P}(\{1,\ldots,k\})$. Observamos que dar un subconjunto de $\{1,\ldots,k\}$ equivale a revisar uno a uno sus elementos eligiendo en cada caso si incluirlo o no en el subconjunto. Esto es asignarle a cada uno un 1 (si lo incluimos) o un 0 (si no lo incluimos). Luego ponemos

$$F : \{0,1\}^{\{1,\ldots,k\}} \to \mathcal{P}(\{1,\ldots,k\}),\ F(f) = f^{-1}(\{1\}).$$

Para ver que esta función es biyectiva alcanza con verificar que $G : \mathcal{P}(\{1,\ldots,k\}) \to \{0,1\}^{\{1,\ldots,k\}}$, definida por

$$G(A)(x) = \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{si } x \notin A \end{cases}$$

es su inversa. Como conclusión tenemos que el cardinal de $\mathcal{P}(\{1,\ldots,k\})$ es $AR_k^2 = 2^k$. En particular se tiene que si X es un conjunto finito, entonces

$$\#\mathcal{P}(X) = 2^{\#X}.$$

5.3.2. Cantidad de relaciones

Consideremos un conjunto finito $X = \{x_1,\ldots,x_n\}$. ¿Cuantas relaciones pueden definirse en X?

Para responder esta pregunta recordemos que el conjunto de las relaciones en X es equipotente con el conjunto de las matrices de $n \times n$ de ceros y unos (ver Sección 3.3). Luego es este último conjunto el que tenemos que contar. Observamos que una matriz de ceros y unos te tamaño $n \times n$ es un arreglo con repetición de dos elementos de largo n^2. Concluimos que existen 2^{n^2} relaciones en X.

Si ahora queremos contar la cantidad de relaciones en X que cumplan con cierta propiedad podemos mirar la caracterización de estas relaciones en términos de sus matrices asociadas (Ejercicio 3.3.2).

1. **Relaciones reflexivas:** Las relaciones reflexivas corresponden a las matrices que tienen 1 en todas las entradas de la diagonal. Luego los espacios que quedan libres son $n^2 - n$, por lo que concluimos que la cantidad de relaciones reflexivas es $2^{n^2-n} = 2^{n(n-1)}$.

2. **Relaciones simétricas:** Las relaciones simétricas se corresponden con las matrices simétricas, es decir que quedan determinadas por las entradas que están por encima de la diagonal (incluyendo la diagonal). La cantidad de estas entradas es
$$n + (n-1) + \cdots + 1 = \frac{n(n+1)}{2}.$$
Luego la cantidad de relaciones simétricas en X es $2^{\frac{n(n+1)}{2}}$.

3. **Relaciones antisimétricas:** Las relaciones antisimétricas corresponden a matrices (a_{ij}) que cumplen la condición
$$\text{Si } i \neq j \Rightarrow (a_{ij}, a_{ji}) \in \{(0,0), (0,1), (1,0)\}. \tag{5.6}$$
Contar la cantidad de relaciones antisimétricas en X consiste entonces en contar las formas de:

   1 Poner un 0 o un 1 en cada lugar de la diagonal de una matriz de $n \times n$. Para esto tenemos 2^n posibilidades.

   2 Elegir para cada par (a_{ij}, a_{ji}), con $i < j$, alguno de los tres valores posibles. Aquí tenemos $3^{\frac{n(n-1)}{2}}$ posibilidades, puesto que hay $\frac{n(n-1)}{2}$ de estos pares (correspondientes a las entradas de la matriz por encima de la diagonal).

   Por el principio del producto tenemos que existen $2^n \cdot 3^{\frac{n(n-1)}{2}}$ relaciones antisimétricas en X.

4. **Relaciones asimétricas:** Se deja como ejercicio.

Si comenzamos a combinar propiedades tenemos más familias de relaciones que contar. Por ejemplo uno podría preguntarse cuantas relaciones de orden o de equivalencia pueden definirse en cierto conjunto finito.

5.4. Combinaciones

Nos interesa ahora estudiar una familia de problemas que consisten en elegir subconjuntos de un conjunto dado sin tener en cuenta el orden. Miremos el siguiente ejemplo:

Ejemplo 5.4.1. *Una persona entra a la heladería que queda frente al bar El Turco para comprar un cucurucho de tres sabores. Cuando llega al mostrador se encuentra con que tiene 20 diferentes sabores para elegir. ¿Qué posibilidades tiene de armar su helado?*[5]

En general notaremos por C_k^n al número de formas de tomar k elementos de un conjunto de cardinal n y lo llamamos **combinaciones de n tomadas de a k**.[6] De esta forma el problema planteado en el ejemplo anterior consiste en calcular C_3^{20}.

Dicho de otra forma, C_k^n es el número de subconjuntos de cardinal k de un conjunto de cardinal n. Para ser más precisos podemos escribirlo como el cardinal de

$$\big\{A \subset \{1, \dots, n\} : \#A = k\big\}.$$

Observación 5.4.2.

1. Hay algunos números combinatorios (así le llamaremos a los números C_k^n) que son muy fáciles de determinar. Por ejemplo es claro que $C_0^n = C_n^n = 1$, pues hay un solo subconjunto de $\{1, \dots, n\}$ con 0 elementos y uno solo con n elementos. También puede verse que $C_1^n = n$, esto es, la cantidad de formas de tomar un subconjunto unitario de $\{1, \dots, n\}$.
2. Observar que $C_k^n = C_{n-k}^n$, ya que elegir un subconjunto de $\{1, \dots, n\}$ es equivalente a elegir su complemento.

El siguiente teorema da una relación entre números combinatorios que permite conocerlos a todos, aunque no de la forma más eficiente.

Teorema 5.4.3. *(Fórmula de Stiefel) Para $k \leq n$ se tiene la siguiente igualdad*

$$C_k^{n+1} = C_k^n + C_{k-1}^n.$$

Demostración. Existen dos tipos de subconjuntos de k elementos de $\{1, \dots, n+1\}$:

- Conjuntos que contienen el elemento $n+1$. Estos son C_{k-1}^n, porque para completarlos se necesitan tomar otros $k-1$ elementos de entre los restantes n.
- Conjuntos que no contienen al $n+1$. Estos son C_k^n, ya que se deben elegir k elementos del conjunto $\{1, \dots, n\}$.

Luego la tesis del teorema sale directamente del Principio de la Suma. □

[5] Suponemos que al cliente no le importa el orden en que se sirven los sabores, cosa que es a las claras un error, puesto que los sabores tienen diferente densidad y firmeza, y la discriminación en este sentido permite armar un helado más estable a fin de evitar eventos desafortunados.

[6] También puede encontrarse en la literatura la notación C_n^k o $\binom{n}{k}$, y la nomenclatura "combinaciones de n en k" o "combinaciones de k en n".

$$
\begin{array}{ccccccccc}
 & & & & C^0_0 & & & & \\
 & & & C^1_0 & & C^1_1 & & & \\
 & & C^2_0 & & C^2_1 & & C^2_2 & & \\
 & C^3_0 & & C^3_1 & & C^3_2 & & C^3_3 & \\
C^4_0 & & C^4_1 & & C^4_2 & & C^4_3 & & C^4_4
\end{array}
\qquad
\begin{array}{ccccccccc}
 & & & & 1 & & & & \\
 & & & 1 & & 1 & & & \\
 & & 1 & & 2 & & 1 & & \\
 & 1 & & 3 & & 3 & & 1 & \\
1 & & 4 & & 6 & & 4 & & 1
\end{array}
$$

La figura anterior es conocida como **Triangulo de Pascal**. Cada fila se construye sumando dos números de la fila precedente y escribiendo el resultado debajo de estos; luego se agregan unos en los extremos. Puede seguirse de esta forma de manera de obtener cualquier número combinatorio que se quiera conocer.

La siguiente proposición relaciona las combinaciones con los arreglos y las permutaciones. Esto nos dará una fórmula expícita para los números combinatorios.

Proposición 5.4.4. *Tomemos $k \leq n$. Luego se cumple la igualdad*

$$A^n_k = C^n_k \cdot P_k. \tag{5.7}$$

Demostración. Aquí podemos usar el principio del producto y dividir la tarea de elegir una función inyectiva $f : \{1, \dots, k\} \to \{1, \dots, n\}$ en dos pasos:

1º Se elige la imagen de f, para lo que se tienen C^n_k posibilidades.

2º Se ordenan los elementos elegidos. Para esto tenemos P_k posibilidades.

De lo anterior obtenermos (5.7). □

A partir de la igualdad (5.7) y las fórmulas de arreglos y permutaciones obtenemos la fórmula para las combinaciones:

$$C^n_k = \frac{n!}{(n-k)!k!} \tag{5.8}$$

De esta forma podemos terminar el Ejemplo 5.4.1 concluyendo que el cliente tiene

$$C^{20}_3 = \frac{20!}{3!17!} = \frac{20 \cdot 19 \cdot 18}{3 \cdot 2} = 1140.$$

posibilidades de armar su helado.

Ejercicio 5.4.5. Probar la fórmula de Stiefel usando (5.8).

5.4.1. Teorema del binomio

Nos enfocamos ahora en el problema de calcular la n-ésima potencia de un binomio $x + y$. Veamos los primeros ejemplos:

- $(x + y)^0 = 1$
- $(x + y)^1 = x + y$
- $(x + y)^2 = x^2 + 2xy + y^2$
- $(x + y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$
- $(x + y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4$

Observamos que los coeficientes se corresponden con las primeras filas del Triángulo de Pascal. Así por ejemplo podemos escribir

$$(x + y)^4 = \sum_{k=0}^{4} C_k^4 x^{4-k} y^k.$$

La formula anterior puede generalizarse para cualquier exponente, como muestra el siguiente resultado.

Teorema 5.4.6 (Teorema del binomio)**.**

$$(x + y)^n = \sum_{k=0}^{n} C_k^n x^{n-k} y^k. \tag{5.9}$$

Daremos dos pruebas del Teorema del binomio. La primera será por inducción mientras que para la segunda usaremos un argumento puramente combinatorio.

Primera prueba del Teorema del binomio. Como vimos en los ejemplos, el caso para $n = 1$ ya está probado. Supongamos entonces que la fórmula (5.9) se cumple para cierto n. Luego

$$
\begin{aligned}
(x+y)^{n+1} &= (x+y)\left(\sum_{k=0}^{n} C_k^n x^{n-k} y^k\right) \\
&= \sum_{k=0}^{n} C_k^n x^{n-k} y^k (x+y) \\
&= \sum_{k=0}^{n} \left(C_k^n x^{n+1-k} y^k + C_k^n x^{n-k} y^{k+1}\right) \\
&= \sum_{k=0}^{n} C_k^n x^{n+1-k} y^k + \sum_{k=1}^{n+1} C_{k-1}^n x^{n+1-k} y^k \\
&= C_0^n x^{n+1} + \sum_{k=1}^{n} \left(C_k^n + C_{k-1}^n\right) x^{n+1-k} y^k + C_n^n y^{n+1}
\end{aligned}
$$

Usando la fórmula de Stiefel en el sumando del medio y las igualdades $C_0^n = C_0^{n+1} = C_n^n = C_{n+1}^{n+1} = 1$ en los otros, obtenemos

$$
(x+y)^{n+1} = \sum_{k=0}^{n+1} C_k^{n+1} x^{n+1-k} y^k.
$$

La prueba termina usando el principio de inducción. □

Antes de dar la segunda prueba veamos, a modo de ejemplo, lo que sucede en le caso $n = 3$. Desarrollamos entonces $(x+y)^3$ de la siguiente manera:

1º. Del producto $(x+y)(x+y)(x+y)$ elegimos x en los tres factores, obteniendo x^3.

2º. Elegimos x en los dos primeros e y en el tercero. Obtenemos x^2y.

3º Elegimos x en el primero y el tercero e y en el segundo. Obtenemos x^2y

4º Elegimos y en el primero y x en los otros dos. Obtenemos x^2y.

Siguiendo de esta manera, los pasos 5, 6 y 7 corresponden a elegir dos y y un x, y el octavo a elegir y en todos los factores. Finalmente tenemos:

$$
(x+y)^3 = x^3 + x^2y + x^2y + x^2y + xy^2 + xy^2 + xy^2 + y^3 = x^3 + 3x^2y + 3xy^2 + y^3.
$$

Segunda prueba del Teorema del binomio. Generalizado la idea anterior vemos que elegir de cada uno de los n factores $(x+y)$ una variable x o y se corresponde con elegir una función $f : \{1, \dots, n\} \to \{x, y\}$. De esta forma por ejemplo $f(k) = x$ significa que estamos tomando x en el k-ésimo factor. Se tiene entonces

$$(x+y)^n = \sum_{f \in \mathcal{X}} f(1) \cdots f(n),$$

donde $\mathcal{X} = \{x, y\}^{\{1,\dots,n\}}$ es el conjunto de todas las funciones de $\{1, \dots, n\}$ a $\{x, y\}$.

El coeficiente de $x^{n-k}y^k$ en el desarrollo es exactamente la cantidad de funciones f que cumplen $f(1) \dots f(n) = x^{n-k}y^k$, es decir, el cardinal del conjunto

$$\big\{f \in X : \#f^{-1}(y) = k\big\}.$$

Este es equipotente con $\big\{A \subset \{1, \dots, n\} : \#A = k\big\}$, luego el coeficiente que estamos buscando es C^n_k. $\square$

Ejercicio 5.4.7. Escribir el desarrollo de $(x - y)^n$.

5.4.2. Combinaciones con repetición

Supongamos ahora que tenemos X un conjunto con n elementos y queremos tomar k de ellos permitiendo repeticiones. A la cantidad de posibilidades que se tienen de hacer esto la llamamos **número de combinaciones con repetición de n tomadas de a k** y lo notamos por CR^n_k. Al igual que sucede en los casos estudiados anteriormente, CR^n_k sólo depende del cardinal de X, por lo que siempre puede suponerse $X = \{1, \dots, n\}$.

Notar que CR^n_k puede interpretarse como la cantidad de posibles soluciones de la ecuación

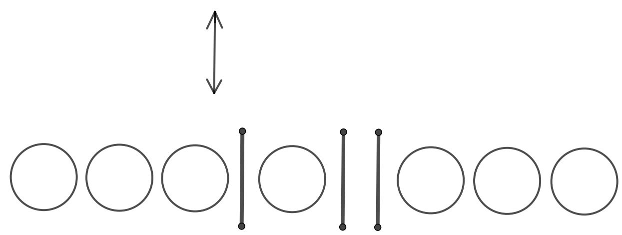
$$x_1 + \cdots + x_n = k,$$

con variables $x_1, \dots, x_n \in \mathbb{N}$. Aquí x_i corresponde al número de veces que se elije el elemento i. Luego podemos escribir

$$CR^n_k = \#\big\{(x_1, \dots, x_n) \in \mathbb{N}^n : x_1 + \cdots + x_n = k\big\}.$$

El número CR^n_k también puede verse como la cantidad de formas que se tienen de meter k pelotas iguales en n cajas distintas. Aquí x_i indica la cantidad de pelotas que se colocan en la i-ésima caja. Este proceso es equivalente a colocar las n pelotas en fila y poner entre ellas $n - 1$ separaciones. De forma tal que las pelotas que quedan antes de la primer separación se asignan a la primera caja, las que quedan entre la primera y la segunda separación se asignan a la segunda caja y así sucesivamente. Puede interpretarse esto como una secuencia formada por dos símbolos, tanto pueden ser pelotas y separaciones como unos y ceros. Un ejemplo de esto se ve en la siguiente figura.

$$\{1,1,1,0,1,0,0,1,1,1\} \sim 3+1+0+3=7$$



Expresamos esto más formalmente en el siguiente resultado:

Proposición 5.4.8. *Existe una función biyectiva entre el conjunto de soluciones naturales de $x_1 + \cdots + x_k = n$ y el conjunto de todas las $(n+k-1)$-uplas formadas por k unos y $n-1$ ceros.*

Demostración. Llamamos X al segundo conjunto e Y al segundo y definimos una función biyectiva $f : X \to Y$ de la siguiente forma:

- Los lugares de $f(x_1, \ldots, x_n)$ de la forma $x_1 + \cdots + x_h + h$ para $h = 1, \ldots, n-1$ tienen ceros.

- El resto de los lugares tienen unos.

Se deja como ejercicio probar que la función descrita es biyectiva. □

De la Proposición 5.4.8 se puede deducir la fórmula

$$CR_k^n = C_k^{n+k-1} = \frac{(n+k-1)!}{k!(n-1)!},$$

que es la cantidad de elecciones posibles de los k lugares en donde se pondrán los unos en la $(n+k-1)$-upla.

Resumiendo, el número CR_k^n puede verse como cantidad de:

- formas de elegir k elementos de un conjunto de n permitiendo repeticiones.

- soluciones de la ecuación $x_1 + \cdots + x_n = k$ con $x_1, \ldots, x_n \in \mathbb{N}$.

- maneras de distribuir k objetos iguales en n recipientes distintos.
- Palabras de largo $n+k-1$ que se pueden formar con dos símbolos repitiendo k veces uno de ellos y $n-1$ veces el otro.

Ejemplos 5.4.9. Para terminar esta sección vamos a ver algunas variantes del problema estudiado.

1. ¿De cuántas formas se pueden distribuir k pelotas iguales en n cajas distintas sin que queden cajas vacías?

   Observamos primero que si k es menor a n no hay ninguna posibilidad, por lo que tienen sentido suponer $k \geq n$. Luego, en ese caso, podemos ver que una distribución tal puede hacerse poniendo primero una pelota en cada caja y distribuyendo luego sin restricciones las restantes $k-n$. Entonces la respuesta a esta pregunta es $CR^n_{k-n} = C^{k-1}_{k-n}$.

   Este problema es equivalente a contar la cantidad de soluciones naturales de
$$\begin{cases} x_1 + \cdots + x_n = k \\ x_1, \ldots, x_n \geq 1. \end{cases}$$

2. Variamos un poco el problema anterior y planteamos, por ejemplo, el problema de contar soluciones naturales de
$$\begin{cases} x_1 + x_2 + x_3 + x_4 = 10 \\ x_1 \geq 1 \\ x_2 \geq 2 \\ x_3 \geq 3. \end{cases}$$

   Podemos pensar que esto equivale a distribuir 10 pelotas iguales en 4 cajas numeradas de forma tal que la primera tenga al menos una pelota, la segunda al menos 2 y la tercera al menos 3. Este proceso puede hacerse distribuyendo primero las 6 pelotas que obligatoriamente deben ir en las primeras tres cajas y después las 4 restantes. Para esto tenemos CR^4_4 posibilidades.

   Otra forma de resolver este problema es haciendo los cambios de variables $y_1 = x_1 - 1$, $y_2 = x_1 - 2$, $y_3 = x_3 - 3$, $y_4 = x_4$. Luego el problema anterior es equivalente a resolver
$$\begin{cases} y_1 + y_2 + y_3 + y_4 = 4 \\ y_1, y_2, y_3, y_4 \geq 0. \end{cases}$$

3. Por último, consideremos el problema
$$\begin{cases} x_1 + x_2 + x_3 + x_4 = 20 \\ 1 \leq x_1 \leq 3 \\ 2 \leq x_2 \leq 5 \\ 3 \leq x_3 \leq 7 \\ 0 \leq x_4 \leq 8. \end{cases} \tag{5.10}$$

Procediendo como en el ejemplo anterior podemos obtener el siguiente problema equivalente:

$$\begin{cases} y_1 + y_2 + y_3 + y_4 = 14 \\ 0 \leq y_1 \leq 2 \\ 0 \leq y_2 \leq 3 \\ 0 \leq y_3 \leq 4 \\ 0 \leq y_4 \leq 8. \end{cases}$$

Lidiar con las cotas superiores de las variables es bastante más difícil que lidiar con las cotas inferiores. Sin embargo, es posible transformar el problema anterior en un conjunto de problemas de restricciones con cotas inferiores. Para esto llamemos X al conjunto de soluciones naturales de la ecuación $y_1 + y_2 + y_3 + y_4 = 14$, A_1 al conjunto de soluciones con $y_1 \geq 3$, A_2 al conjunto de soluciones con $y_2 \geq 4$, A_3 al conjunto de soluciones con $y_3 \geq 5$ y A_4 al conjunto de soluciones con $y_4 \geq 9$. Luego el número buscado es, por el Principio de Inclusión-Exclusión,

$$\begin{aligned} \#\big(X \setminus (A_1 \cup A_2 \cup A_3 \cup A_4)\big) = \#X - \sum_{1\leq i\leq 4} \#A_1 + \sum_{1\leq i<j\leq 4} \#(A_i \cap A_j) \\ - \sum_{1\leq i<j<k\leq 4} \#(A_i \cap A_j \cap A_k) + \#(A_1 \cap A_2 \cap A_3 \cap A_4). \end{aligned}$$

Observar que determinar cada uno de estos cardinales es contar soluciones de un problema con restricciones con cotas inferiores para las variables.

Observación 5.4.10. En el último ejemplo puede verse que el problema (5.10) es equivalente con encontrar el coeficiente de grado 20 en el desarrollo

$$(x+x^2+x^3)(x^2+x^3+x^4+x^5)(x^3+x^4+x^5+x^6+x^7)(1+x+x^2+x^3+\cdots+x^8). \quad (5.11)$$

Esto puede verse de la siguiente forma: elegir el valor de x_1 corresponde a elegir en el primer factor de (5.11) x^{x_1}, elegir el valor de x_2 corresponde a elegir en el segundo factor x^{x_2} y así sucesivamente; siempre de forma tal que $x^{x_1}x^{x_2}x^{x_3}x^{x_4} = x^{20}$. Luego todas las formas de hacer las elecciones de x_1, x_2, x_3 y x_4 se corresponden con el coeficiente de x^{20}.

El ejemplo abre la puerta a problemas con otro tipo de restricciones, por ejemplo que algunas variables sean pares, multiplos de 3, etc.

5.5. Otras cantidades interesantes

5.5.1. Permutaciones con repetición

Ejemplo 5.5.1. *El Turco estaba sentado detrás del mostrador con un frasco en la mano izquierda y la vista fija en la etiqueta. La otra mano alternaba tareas, de a ratos* *rascaba su pelada y de a ratos ahuyentaba una mosca que volaba cerca del frasco atraída por el azucarado contenido.*

"MERMELADA" leyó en la etiqueta como por centésima vez, y lo leyó con mayúsculas, sobreactuando la pronunciación como quién le enseña a un niño una palabra difícil.

Desde que el Comadreja le había enseñado el asunto de las permutaciones no había parado de contar ordenaciones: de los borrachos acodados a lo largo del mostrador, de las botellas en el tercer estante o los trofeos de campeonatos de truco y escoba de quince en el último. Pero se había topado con un problema nuevo con la palabra MERMELADA, pues la repetición de la M, la E y la A hacía que al aplicar la fórmula que el otro le había enseñado estuviera contando siempre de más.

Podemos imaginarnos una gran familia de ejemplos que consisten, en esencia, en el problema del ejemplo anterior: contar las formas de ordenar n símbolos sabiendo que estos se repiten con frecuencias $n_1, \ldots, n_k$ (suponemos aquí que $n_1 + \cdots + n_k = n$). La cantidad descrita es llamada **permutaciones de $\boldsymbol{n}$ elementos con repeticiones de frecuencias $\mathbf{n_1}, \ldots, \mathbf{n_k}$**, y se denota por $P_{n;n_1,\ldots,n_k}$. Este número puede verse como el cardinal del conjunto

$$\big\{f : \{1, \ldots, n\} \to \{1, \ldots, k\} : \#f^{-1}(i) = n_i \text{ para todo } i = 1, \ldots, k\big\}, \tag{5.12}$$

donde $n = n_1 + \cdots + n_k$.

Vamos a obtener una fórmula para $P_{n;n_1,\ldots,n_k}$ usando el principio del producto. Para esto observemos que el proceso de ordenar k símbolos $A_1, \ldots, A_k$ con repeticiones $n_1, \ldots, n_k$ puede hacerse en los siguientes pasos:

1. Elegimos los lugares que ocuparán los n_1 símbolos A_1 entre los n lugares disponibles. Para esto tenemos $C^n_{n_1}$ posibilidades.

2. Colocamos los símbolos $A_2, \ldots, A_k$ en los $\tilde{n}_1 = n_2 + \ldots + n_k$ lugares restantes. Para esto tenemos $P_{\tilde{n}_1;n_2,\ldots,n_k}$ posibilidades.

Luego el principio del producto nos da la igualdad

$$P_{n;n_1,\ldots,n_k} = C^n_{n_1} \cdot P_{\tilde{n}_1;n_2,\ldots,n_k} \tag{5.13}$$

Notando $\tilde{n}_i = n_{i+1} + \cdots + n_k$ y usando (5.13) obtenemos

$$\begin{aligned} P_{n;n_1,\ldots,n_k} &= C^n_{n_k} \cdot P_{\tilde{n}_1;n_2,\ldots,n_k} = C^n_{n_1} \cdot C^{\tilde{n}_1}_{n_2} \cdot P_{\tilde{n}_2;n_3,\ldots,n_k} = \cdots = C^n_{n_1} \cdot C^{\tilde{n}_1}_{n_2} \cdots C^{\tilde{n}_{k-1}}_{n_k} \\ &= \frac{n!}{\tilde{n}_1! n_1!} \cdot \frac{\tilde{n}_1!}{\tilde{n}_2! n_2!} \cdot \frac{\tilde{n}_2!}{\tilde{n}_3! n_3!} \cdots \frac{\tilde{n}_{k-1}!}{\tilde{n}_k! n_k!} = \frac{n!}{n_1! \cdots n_k!}. \end{aligned}$$ [7]

Usando esta fórmula podemos rápidamente resolver el problema planteado en el Ejemplo 5.5.1. Observar que las repeticiones correspondientes a las letras M, E, R, L,

A y D son $n_1 = 2$, $n_2 = 2$, $n_3 = 1$, $n_4 = 1$, $n_5 = 2$ y $n_6 = 1$, luego la cantidad buscada es

$$P_{9;2,2,1,1,2,1} = \frac{9!}{2!2!1!1!2!1!} = \frac{362880}{8} = 45360.$$

Usemos ahora las permutaciones con repetición para generalizar el Teorema del Binomio (Teorema 5.4.6).

Teorema 5.5.2 (Teorema Multinomial)**.** *El coeficiente del monomio* $x_1^{n_1} \dots x_k^{n_k}$ *en el desarrollo* $(x_1 + \cdots + x_k)^n$ *es*

$$P_{n;n_1,\dots,n_k} = \frac{n!}{n_1! \cdots n_k!}.$$

Observar que si $k = 2$, entonces $C^n_{n_1} = P_{n;n_1,n_2}$, de donde sale la fórmula dada por el Teorema del Binomio.

Demostración. Siguiendo la idea de la prueba combinatoria del Teorema 5.4.6 observamos que

$$(x_1 + \cdots + x_k)^n = \sum_{f \in \mathcal{X}} f(1) \cdots f(n),$$

donde $\mathcal{X} = \{x_1, \dots, x_k\}^{\{1,\dots,n\}}$. Tenemos entonces que el coeficiente de $x_1^{n_1} \dots x_k^{n_k}$ en el desarrollo es el cardinal del conjunto

$$\{f \in X : \#f^{-1}(x_i) = n_i \text{ para todo } i = 1, \dots, k\},$$

que es $P_{n;n_1,\dots,n_k}$ ya que el conjunto descrito es claramente equipotente con el conjunto (5.12). □

Para ilustrar la demostración anterior supongamos que $n = 5$, $k = 3$, $n_1 = 2$, $n_2 = 1$ y $n_3 = 2$ y que queremos formar $x_1^2 x_2 x_3^2$. Una manera de obtener este monomio es haciendo la siguiente elección (marcada en negrita):

$$(x_1+x_2+x_3)^5 = (x_1+x_2+\mathbf{x_3}).(x_1+\mathbf{x_2}+x_3).(\mathbf{x_1}+x_2+x_3).(\mathbf{x_1}+x_2+x_3).(x_1+x_2+\mathbf{x_3}).$$

Esto se identifica con la palabra $x_3x_2x_1x_1x_3$. Luego las formas de obtener dicho monomio en el desarrollo están en biyección con el conjunto de las palabras de largo cinco que se pueden formar con tres variables repitiendo dos veces x_1 y x_3. Esta cantidad es, como ya vimos, $P_{5;2,1,2}$.

Ejercicio 5.5.3. Escribir una prueba por inducción del Teorema Multinomial.

5.5.2. Desordenes

Consideramos aquí el siguiente problema: dada una palabra formada por n símbolos diferentes, ¿cuántas palabras se pueden formar reordenando las letras de forma tal que ninguna quede en su lugar original? Llamaremos a este número **desordenes de n elementos** y lo notaremos por D_n. Observamos que este número es el cardinal del conjunto

$$\mathcal{D}_n = \big\{f : \{1, \ldots, n\} \to \{1, \ldots, n\} : f \text{ biyctiva, } f(i) \neq i \text{ para todo } i\big\}$$

Una forma de hallar D_n es usando el Principio de Inclusión-Exclusión. Para esto definimos

$$A_i = \big\{f : \{1, \ldots, n\} \to \{1, \ldots, n\} : f \text{ biyectiva, } f(i) = i\big\}.$$

Entonces $\mathcal{D}_n = \left(\bigcup_{i=1}^n A_i\right)^c$, donde el complemento se toma en el conjunto de todas las funciones. Observamos que $\#(A_{i_1} \cap \cdots \cap A_{i_k}) = P_{n-k}$ y que hay C_k^n intersecciones de esta forma, luego

$$D_n = P_n - nP_{n-1} + C_2^n P_{n-2} - \ldots + (-1)^n C_n^n P_0 = \sum_{i=0}^{n} (-1)^i C_i^n P_{n-i}.$$

5.5.3. Cantidad de funciones sobreyectivas y número de Stirling de segunda especie

Nos preguntamos ahora cuantas funciones sobreyectivas pueden definirse de un conjunto de n elementos a un conjunto de k elementos ($k \leq n$), es decir, cuál es el cardinal de

$$\big\{f : \{1, \ldots, n\} \to \{1, \ldots, k\} : f \text{ sobreyectiva}\big\},$$

al que notamos por $Sob(n, k)$.

Para encontrar una fórmula para este número usaremos el Principio de Inclusión-Exclusión. Consideramos entonces $Z = \{1, \ldots, k\}^{\{1,\ldots,n\}}$ el conjunto de todas las funciones de $\{1, \ldots, n\}$ en $\{1, \ldots, k\}$, que tiene cardinal k^n, y los subconjuntos

$$A_i = \big\{f \in Z : i \notin f(\{1, \ldots, n\})\big\}.$$

Es claro que el conjunto de funciones sobreyectivas es $\left(\bigcup_{i=1}^k A_i\right)^c$. Observamos que $\#(A_{i_1} \cap \cdots \cap A_{i_\ell}) = (k - \ell)^n$ y que hay C_ℓ^k intersecciones de esta forma. Luego tenemos

$$\begin{aligned} Sob(n, k) &= k^n - C_1^k (k-1)^n + C_2^k (k-2)^n - \ldots + (-1)^{k-1} C_{k-1}^k 1^n \\ &= \sum_{i=0}^{k} (-1)^i C_i^k (k-i)^n. \end{aligned}$$

El número
$$S(n,k) = \frac{1}{k!} Sob(n,k)$$
se llama **número de Stirling de segunda especie** y denota la cantidad de particiones en k subconjuntos que pueden hacerse en un conjunto de n elementos. El número total de particiones se conoce como el n-ésimo **número de Bell** y se denota por
$$B(n) = \sum_{k=1}^{n} S(n,k).$$
Este puede interpretarse también como el número de relaciones de equivalencia que es posible definir en un conjunto con n elementos.

5.5.4. Más problemas con cajas y pelotas

En la Sección 5.4.2 abordamos el problema de colocar k pelotas distintas en n cajas diferentes, y vimos que la solución era el número CR_k^n. Variando este problema podemos plantearnos las siguientes preguntas: ¿que sucede si las pelotas son distintas y las cajas también? ¿y si las pelotas son distintas y las cajas iguales? ¿y si las pelotas son iguales y las cajas también?

La respuesta a la primera pregunta es sencilla: toda distribución de k pelotas distintas en n cajas distintas corresponde a una función $f : \{1, \ldots, k\} \to \{1, \ldots, n\}$ (puede pensarse que tanto las cajas como las pelotas están numeradas); luego la cantidad de posibilidades de hacerlo es $AR_k^n = n^k$. Si además pedimos que no queden cajas vacías, entonces la respuesta es la cantidad de funciones sobreyectivas, es decir, $Sob(k,n)$.

Por otro lado, si las pelotas son distintas y las cajas iguales, cada distribución corresponde a una partición del conjunto $\{1, \ldots, k\}$. Si pedimos que no queden cajas vacías, entonces estamos haciendo particiones en n subconjuntos, para lo que tenemos $S(k,n)$ posibilidades. Si quitamos la condición de que no deben quedar cajas vacías, entonces estamos contando particiones en no más de n conjuntos. Para esto tenemos
$$\sum_{i=1}^{n} S(k,n)$$
posibilidades.

Nos queda entonces una pregunta por responder: ¿De cuantas formas se pueden distribuir k pelotas iguales en n cajas iguales?

Intentaremos dar una respuesta (aunque quizá no del todo satisfactoria) en dos instancias. Primero supondremos que $n \geq k$, es decir que hay más cajas que pelotas. En este caso podemos olvidarnos el número n ya que el problema equivale a contar la cantidad de formas de particionar el conjunto de las k pelotas iguales. También podemos enunciar este problema de la siguiente forma: ¿De cuántas formas se puede escribir k como una suma de naturales positivos? Llamaremos a este número **particiones de k** y lo escribiremos $p(k)$. Por ejemplo, en el caso $k = 5$ tenemos las siguientes formas:

$$\begin{aligned}
5 &= 1+1+1+1+1\\
5 &= 1+1+1+2\\
5 &= 1+1+3\\
5 &= 1+2+2\\
5 &= 1+4\\
5 &= 2+3\\
5 &= 5
\end{aligned}$$

Entonces concluimos $p(5) = 7$. Es esperable que a medida que el número k crezca la lista que hemos hecho crezca también y de forma más rápida. Luego sería bueno buscar una equivalencia para este problema que pueda resolverse de otro modo.

Recordar la Observación 5.4.10 puede darnos una pista de cómo reinterpretar este problema. Consideremos el siguiente producto:

$$(1+x+x^2+x^3+x^4+x^5)(1+x^2+x^4)(1+x^3)(1+x^4)(1+x^5). \tag{5.14}$$

Si aplicamos la propiedad distributiva podemos ver que el término x^5 aparece 7 veces en el desarrollo. Expresemoslo manteniendo el órden de los factores en (5.14):

$$\begin{aligned}
x^5 &= x^5\cdot 1\cdot 1\cdot 1\cdot 1\\
x^5 &= x^3\cdot x^2\cdot 1\cdot 1\cdot 1\\
x^5 &= x^2\cdot 1\cdot x^2\cdot 1\cdot 1\\
x^5 &= x\cdot x^4\cdot 1\cdot 1\cdot 1\\
x^5 &= x\cdot 1\cdot 1\cdot x^4\cdot 1\\
x^5 &= 1\cdot x^2\cdot x^3\cdot 1\cdot 1\\
x^5 &= 1\cdot 1\cdot 1\cdot 1\cdot 1\cdot x^5
\end{aligned}$$

Observamos que los ítems de esta lista se corresponden uno a uno con los de la lista anterior. Así por ejemplo elegir x^5 en el primer factor y 1 en los otros cuatro corresponde a elegir cinco veces el 1 para sumar 5, y elegir x en el primero, $x^4 = (x^2)^2$ en el segundo y 1 en el resto corresponde a elegir una vez el 1 y dos veces el 2 para sumar 5.

En conclusión, $p(k)$ es el coeficiente de x^k en el desarrollo

$$(1+x+\cdots)(1+x^2+\cdots)(1+x^3+\cdots)\cdots(1+x^k+\cdots).$$

Donde en cada factor puede colocarse una suma hasta un término de grado mayor o igual k o directamente considerar que cada factor es una serie de potencias de x.

Asumiendo que $\sum_{i=0}^{\infty} r^i = \frac{1}{1-r}$ (si $r < 1$) podemos escribir

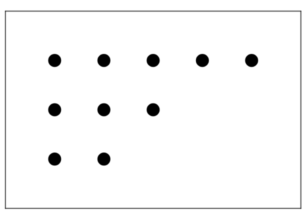
$$(1 + x^{\ell} + x^{2\ell} + \cdots) = \frac{1}{1 - x^{\ell}},^{8}$$

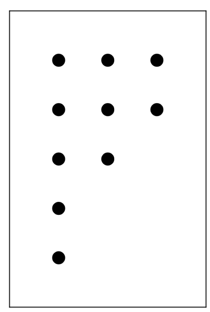
luego determinar $p(k)$ corresponde a encontrar el coeficiente de grado k en el desarrollo en serie de potencias de la función

$$f(x) = \frac{1}{1-x} \cdot \frac{1}{1-x^2} \cdots \frac{1}{1-x^k} = \frac{1}{(1-x)(1-x^2)\cdots(1-x^k)}.$$

Este tipo de problemas excede los objetivos de este curso, sin embargo parece bueno en este punto mostrar en qué derivan algunos problemas de conteo de formulación elemental.

Para terminar consideremos el problema para $n < k$. Una distribución de k pelotas en n cajas (pudiendo dejar algunas vacías) verse como una forma de poner las pelotas en n filas ordenadas desde la fila con más pelotas a la fila con menos pelotas. En el siguiente dibujo, a la izquierda, se ve una forma de distribuir 10 pelotas en 3 cajas. Si lo rotamos obtenemos la figuro de la derecha, que corresponde a una distribución de las 10 pelotas en cajas con la restricción de que cada caja no puede contener más de 3 pelotas.





Como estas formas de distribuir las pelotas se corresponden 1 a 1 se tiene que el número buscado es el coeficiente de x^{10} en el desarrollo

$$(1 + x + \cdots)(1 + x^2 + \cdots)(1 + x^3 + \cdots).$$

En general, la forma de distribuir k pelotas iguales en n cajas diferentes corresponde al coeficiente de x^k en el desarrollo

$$(1 + x + \cdots)(1 + x^2 + \cdots)\cdots(1 + x^n + \ldots) = \frac{1}{(1-x)(1-x^2)\cdots(1-x^n)}.$$

[8] Aquí debemos asumir $|x| < 1$ para asegurarnos la convergencia de las series.

Observar que esta fórmula también funciona en el caso $n \geq k$.

Determinar este coeficiente requiere técnicas que escapan a este curso, sin embargo daremos algunas ideas en el Apéndice **V**. Se sugiere también la lectura de [G, Capítulo 9] para un estudio más completo del tema.

Ejercicio 5.5.4. Buscar una correspondencia como la establecida anteriormente para el problema de colocar k pelotas iguales en n cajas iguales de forma tal que ninguna caja quede vacía.

5.6. Apéndice

I. Recordemos el problema dado al principio del capítulo: ¿Cuántas palabras de cinco letras no tienen dos vocales juntas?

Para resolver este problema podemos dividir en cuatro casos:

Palabras con tres vocales: Tenemos en este caso que todos los lugares impares de la palabra tienen vocal, luego tenemos 5^3 formas de llenar estos lugares con vocales y 22^2 de llenar los restantes con consonantes.

Palabras con dos vocales: Aquí primero debemos elegir dos lugares de entre los cinco donde colocar las vocales, tenemos 5 formas para hacerlo. Después de hecho esto, tenemos 5^2 formas de llenar estos lugares y 22^3 de llenar el resto.

Palabras con una vocal: Tenemos 5 formas de elegir el lugar donde irá la vocal y 5 formas de llenarlo. Luego hay 22^4 formas de llenar los lugares restantes.

Palabras sin vocales: Aquí tenemos 22^5 palabras posibles.

En conclusión, la cantidad buscada es

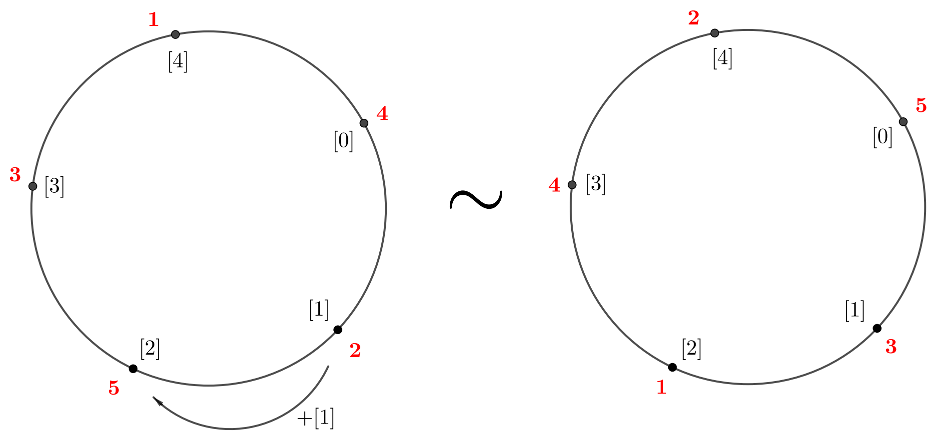
$$5^3 \cdot 22^2 + 5 \cdot 5^2 \cdot 22^2 + 5 \cdot 5 \cdot 22^4 + 22^5 = 12401532.$$

II. Permutaciones circulares

Vamos a aprovechar lo que sabemos de relaciones de equivalencia para expresar PC_n como el cardinal de un conjunto.

Observemos que la diferencia entre el proceso descrito en el Ejercicio 5.2.3 y las permutaciones es que los n elementos se ordenan de forma circular en lugar de ordenarse de forma lineal, por lo que se corresponde con una función con el mismo codominio (el conjunto $\{1, \ldots, n\}$ correspondiente a los elementos a ordenar) pero con un dominio diferente (correspondiente a los lugares a ocupar).

Para emular un dominio circular de n elementos consideramos el conjunto $\mathbb{Z}_n$, es decir, el cociente de $\mathbb{Z}$ por la relación de congruencia módulo n.



Observamos que sumar $[1]$ en $\mathbb{Z}_n$ corresponde a hacer un giro de ángulo $\frac{2\pi}{n}$ (por lo que sumar $[k]$ es hacer un giro de $\frac{2\pi k}{n}$). Vamos a querer que una distribución de los números $\{1, \ldots, n\}$ en dicho círculo sea equivalente a una rotación de la misma, tal como se ve en la figura.

Teniendo en cuenta estas observaciones definimos en el conjunto

$$X = \{f : \mathbb{Z}_n \to \{1, \ldots, n\} : f \text{ es biyectiva}\}$$

la relación de equivalencia $\sim$ por

$$f \sim g \iff \text{existe } k \in \mathbb{N} \text{ tal que } f([x]) = g([x+k]) \text{ para todo } [x] \in \mathbb{Z}_n.$$

Luego PC_n es el cardinal del conjunto $X/\sim$.

Observar que si $\sim$ es una relación de equivalencia cualquiera en un conjunto finito X, entonces $\#X$ es igual a la suma de los cardinales de todas las clases de equivalencia. Justificar la fórmula de permutaciones circulares a partir de este hecho.

Dejamos como ejercicio definir y dar una fórmula para los **arreglos circulares de n elementos de largo k**.

III. Números de Stirling de primera especie

Tomemos una permutación de n elementos $f : \{1, \ldots, n\} \to \{1, \ldots, n\}$. Un **ciclo** en f es una ℓ-upla $(x_1, \ldots, x_\ell)$ de forma tal que $f(x_i) = x_{i+1}$ para $i = 1, \ldots, \ell - 1$

y $f(x_\ell) = x_1$. Puede probarse que toda permutación f se descompone en ciclos, es decir, existen ciclos

$$(x_1, \dots, x_{\ell_1}), \dots, (x_{\ell_{k-1}+1}, \dots, x_{\ell_k})$$

tal que $\ell_k = n$ y todos los x_i son distintos. En este caso puede escribirse

$$f = (x_1, \dots, x_{\ell_1}) \cdots (x_{\ell_{k-1}+1}, \dots, x_{\ell_k})$$

El **número de Stirling de primera especie sin signo** para el par (n, k) es la cantidad de permutaciones de n elementos que tienen exactamente k ciclos. Notamos este número por $z(n, k)$. Aquí es importante tener en cuenta que las ℓ-uplas $(x_1, \dots, x_\ell)$ y $(x_2, \dots, x_\ell, x_1)$ cuentan como un único cíclo.

Hagamos algunas observaciones inmediatas:

- $\sum_{k=1}^{n} z(n, k) = P_n = n!$
- $z(n, n) = 1$
- $z(n, 1) = PC_n = (n-1)!$

Proposición 5.6.1. *Los números de Stirling de primera especie sin signo satisfacen la siguiente relación de recurrencia:*

$$z(n, k) = (n-1)z(n-1, k) + z(n-1, k-1) \text{ para } k < n. \tag{5.15}$$

Demostración. Dividimos las permutaciones de n elementos con k ciclos en dos tipos disjuntos:

- Permutaciones que tienen el ciclo (n), es decir, que fijan el elemento n. Cada una de estas puede verse como una permutación de $n-1$ elementos con $k-1$ ciclos, y sabemos que hay $z(n-1, k-1)$ de ellas.
- Permutaciones que tienen el elemento n en un ciclo de largo $\ell \geq 2$. En este caso observamos que si retiramos el elemento n obtenemos una permutación de $n-1$ elementos con k ciclos. Este proceso construye una función sobreyectiva entre la primer y la segunda familia de permutaciones de forma tal que cada elemento del codominio tiene exactamente $(n-1)$ preimágenes. De aquí deducimos que esta cantidad es $(n-1)z(n-1, k)$.

A partir de esto y el principio de la suma se concluye (5.15). $\square$

Observar que a partir de (5.15) se pueden determinar todos los números de Stirling de primera especie sin signo.

El **número de Stirling de primera especie (con signo)** es la cantidad $s(n, k) = (-1)^{n-k} z(n, k)$.

IV. Ejercicio: Probar las siguientes identidades en las que intervienen los números de Stirling:

a) $x^n = \sum_{k=0}^{n} S(n,k)x(x-1)\cdots(x-k+1)$

b) $x(x-1)\cdots(x-k+1) = \sum_{k=0}^{n} s(n,k)x^k$

V. Vamos a intentar mostrar una posible técnica para resolver el problema de contar distribuciones de k pelotas iguales en k cajas iguales.

Como vimos en la Sección 5.5.4, este número coincide con el coeficiente de x^k en el desarrollo en serie de potencias de la función

$$f(x) = (1+x+\cdots)(1+x^2+\cdots)\cdots(1+x^n+\ldots) = \frac{1}{(1-x)(1-x^2)\cdots(1-x^n)}.$$

Es decir que debemos intentar escribir

$$f(x) = \sum_{i=0}^{\infty} a_i x^i$$

y encontrar el coeficiente a_k. En este caso se dice que f es la *función generatriz* de la sucesión $\{a_i\}_{i\in\mathbb{N}}$.

Una posible aproximación a esto puede hacerse escribiendo la serie de Taylor de f en $x=0$:

$$f(x) = \sum_{i=0}^{\infty} \frac{f^{(i)}(0)}{i!} x^i.$$

Aquí tenemos entonces $a_k = f^{(k)}(0)/k!$. Sin embargo, si k es muy grande este número podría ser difícil de hallar, ya que se debe derivar k veces la función f.

Una opción tal vez más amigable viene de usar la descomposición en fracciones simples. Para ilustrar esta técnica concentremonos en un ejemplo sencillo: supongamos $n=2$. Si bien el problema en este caso puede resolverse rápidamente de forma elemental, nos interesará seguir el camino que ya hemos comenzado para dar una idea de cómo resolver el problema en el caso general.

Queremos en este caso escribir la función

$$f(x) = \frac{1}{(1-x)(1-x^2)} = \sum_{i=0}^{\infty} a_i x^i.$$

Para esto podemos aplicar la descomposición en fracciones simples y escribir

$$f(x) = \frac{1}{(1-x)^2(1+x)} = \frac{1/4}{1-x} + \frac{1/2}{(1-x)^2} + \frac{1/4}{1+x}.$$

Ahora, si podemos expresar como series de potencias cada sumando, entonces nuestro problema estará resuelto.

El primer sumando lo podemos escribir como

$$\frac{1/4}{1-x} = \frac{1}{4}\bigl(1 + x + x^2 + x^3 + \cdots\bigr)$$

y el tercero como

$$\frac{1/4}{1+x} = \frac{1}{4} \cdot \frac{1}{1-(-x)} = \frac{1}{4} \cdot \bigl(1 - x + x^2 - x^3 + \cdots\bigr).$$

Para desarrollar el segundo sumando podemos observar que

$$\frac{1/2}{(1-x)^2} = \frac{1}{2} \cdot \left(\frac{1}{1-x}\right)^2 = \frac{1}{2}\bigl(1 + x + x^2 + x^3 + \cdots\bigr)^2.$$

Al desarrollar el cuadrado anterior existen exactamente $\ell + 1$ formas de escribir el término x^ℓ:

$$x^\ell = 1 \cdot x^\ell = x \cdot x^{\ell-1} = \cdots = x^\ell \cdot 1,$$

luego

$$\frac{1/2}{(1-x)^2} = \frac{1}{2}\bigl(1 + 2x + 3x^2 + 4x^3 + \cdots\bigr).$$

De acá concluimos

$$a_k = \frac{1}{4} + \frac{(k+1)}{2} + \frac{(-1)^k}{4}.$$

Es claro que cuanto más grande sea n más complejo será el problema, sin embargo siempre podrá resolverse mediante la descomposición en fracciones simples.[9] Por otro lado, este método tiene la ventaja de dar una fórmula para todo k sin importar qué tan grande sea este número.

Una alternativa a este método es obtener una relación de recursión. Observar que si denotamos por $\pi(k, n)$ al número de formas de distribuir k peotas idénticas en n cajas idénticas, entonces podemos observar que

$$\pi(n, k) = \pi(k, n-1) + \pi(k-n, n), \tag{5.16}$$

donde se entiende que $\pi(k, n) = 0$ si k es negativo. Esto se prueba de la siguiente forma: si $k \geq n$, entonces hay dos tipos de distribuciones: las que dejan alguna caja vacía (estas son $\pi(k, n-1)$) y las que no dejan cajas vacías (que son $\pi(k-n, n)$ ya que una tal distribución puede hacerse poniendo una pelota en cada caja y

[9]En general puede ser conveniente descomponer en fracciones simples de polinomios con coeficientes complejos.

luego distribuyendo las $k-n$ restantes sin restricciones). Si $k < n$ necesariamente se deben dejar cajas vacías, por lo que tentemos

$$\pi(k, n) = \pi(k, n-1) = \pi(k, n-1) + \pi(k-n, n).$$

Por otro lado, observamos que $\pi(k, 1) = 1$ y $\pi(0, n) = \pi(1, n) = 1$. Esto nos permite, dado un par de números naturales k y n, aplicar la igualdad (5.16) las veces que sea necesario hasta obtener el valor de $\pi(k, n)$. Veamos esto con un ejemplo: supongamos $k = 7$, $n = 4$. Luego

$$\begin{aligned}
\pi(7,4) &= \pi(7,3) + \pi(3,4) = \pi(7,2) + \pi(4,3) + \pi(3,3) \\
&= \pi(7,1) + \pi(5,2) + \pi(4,2) + \pi(1,3) + \pi(3,2) + \pi(0,3) \\
&= \pi(7,1) + \pi(5,1) + \pi(3,2) + \pi(4,1) + \pi(2,2) + \pi(1,3) \\
&\qquad + \pi(3,1) + \pi(1,2) + \pi(0,3) = 11.
\end{aligned}$$

Es cierto que resolver el problema con la función generatriz podría costarnos más en este caso, sin embargo el número de operaciones hechas en este proceso crece con k.

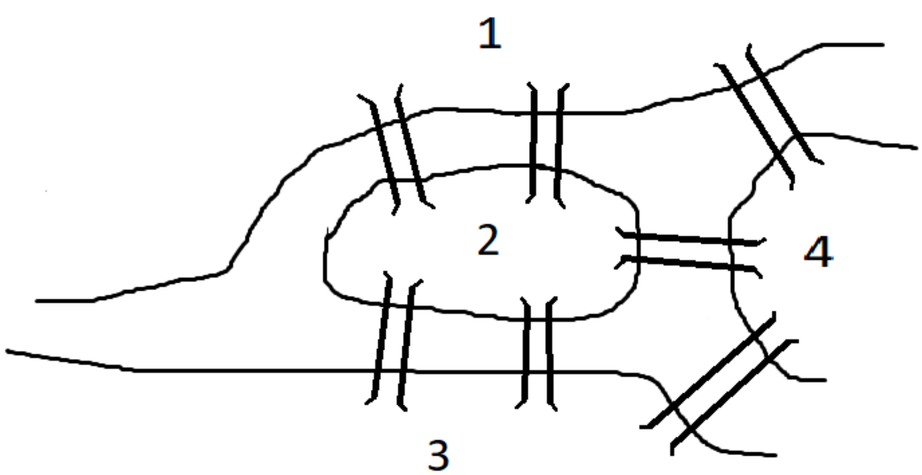
Capítulo 6

Grafos

Para motivar este capítulo presentaremos dos problemas. El primero es un problema célebre que data del siglo XVI y que, según se considera, da origen a la teoría de grafos. El segundo es un problema lúdico que circula entre los escolares (o circulaba en alguna época y alguna escuela).

1. Problema de los puentes de Königsberg

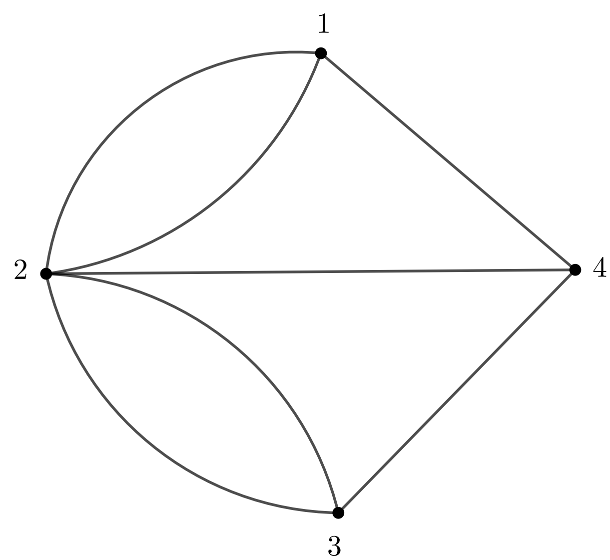
La ciudad de Königsberg (antigua capital de Prusia Oriental, hoy llamada Kaliningrado) estaba atravesada por el río Pregel, sobre el que se disponían siete puentes como se muestra a continuación:



En este escenario se plantea el siguiente problema: ¿Es posible recorrer todos los puentes pasando por cada uno una única vez y terminando el recorrido en el punto de partida?

Es posible resolver el problema por fuerza bruta, es decir, listando todos los posibles recorridos que no repitan puentes y verificando si entre ellos hay uno que cumpla las condiciones. Sin embargo, el matemático suizo Leonard Euler dio una solución en el año 1736 (en una publicación titulada *Solutio problematis ad geometriam situs pertinentis*) que puede generalizarse a toda una familia de problemas similares a este.

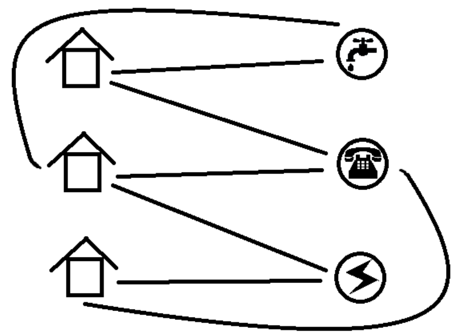
El primer paso en el análisis del problema consiste en simplificar el contexto hasta quedarse con los elementos escenciales del mismo. Observamos entonces que hay dos tipos de objetos en el problema: las regiones y los puentes. Se puede entonces representar el mapa anterior por medio de la siguiente figura, donde las regiones son representadas por puntos y los puentes por aristas. A los efectos del problema que estamos considerando no hay diferencia entre el mapa y esta figura (a la que vamos a denominar *grafo*, o más especificamente en este caso, *multigrafo*).



En la actualidad la disposición de los puentes es diferente a la descrita, por lo que el problema ha cambiado. El lector puede plantearse entonces, además del propuesto, el problema de los puentes de Kaliningrado.

2. Problema de la conexión de servicios básicos en el plano

Se disponen en un territorio plano tres casas y tres usinas de servicios públicos: agua, telefonía y electricidad. El problema consiste en conectar las tres casas a los tres servicios mediante conectores independientes (cables o ductos) que no se corten entre sí. (Como nos encontramos en un mundo plano, no es posible pasar un conector por encima de otro.)



Hay una diferencia escencial entre el primer problema y el segundo. Mientras el primero depende solamente de la estructura del grafo, es decir, de como están conectados los puntos con aristas, en el segundo se agrega una nueva circunstancia: el hecho de que el grafo está contenido en el plano. Veremos más adelante que estos corresponden a dos tipos diferentes de problemas más generales y mostraremos sus soluciones.

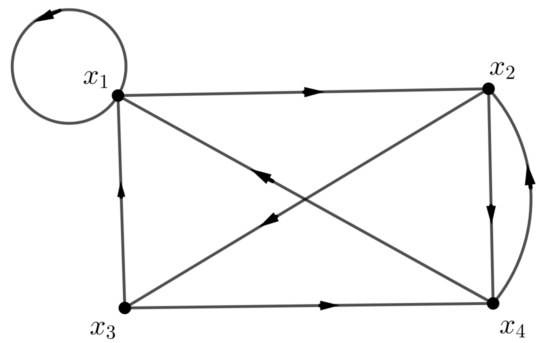
6.1. Primeras definiciones y ejemplos

Un **grafo dirigido** es un par (V, E) donde V es un conjunto finito al que llamamos conjunto de **vértices** y E es un subconjunto de $V \times V$ al que llamamos conjunto de **aristas**.

El conjunto de aristas no es otra cosa que una relación en el conjunto de vértices, luego tenemos una nueva representación (esta vez geométrica) de las relaciones definidas en un conjunto. Por ejemplo, para el conjunto $X = \{x_1, x_2, x_3, x_4\}$ podemos representar la relación

$$\mathcal{R} = \big\{(x_1, x_1), (x_1, x_2), (x_2, x_3), (x_2, x_4), (x_3, x_1), (x_3, x_4), (x_4, x_1), (x_4, x_2)\big\}$$

como sigue:



Nos interesa también definir grafos no dirigidos, es decir, que tengan aristas no orientadas. Para esto debemos reemplazar los pares ordenados por pares no ordenados.

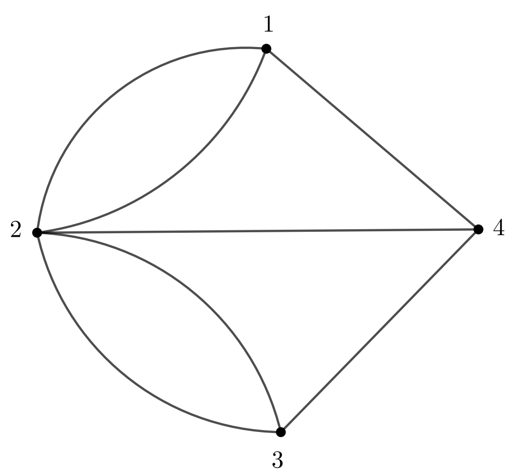
Un **grafo no dirigido** (también llamado simplemente **grafo**) es un par (V, E) donde V es un conjunto finito y

$$E \subset \big\{\{x, y\} : x, y \in V\big\}.$$

Las aristas de la forma $\{x, x\} = \{x\}$ se denominan **lazos**. Decimos que dos vértices x y y de un grafo G (no dirigido) son **adyacentes** si $\{x, y\}$ es una arista del grafo.

Observar que de forma similar al caso de los grafos dirigidos, un grafo no dirigido puede definirse como un conjunto de vértices V junto con una relación simétrica E en V. Esta relación no es otra cosa que la relación de adyacencia.

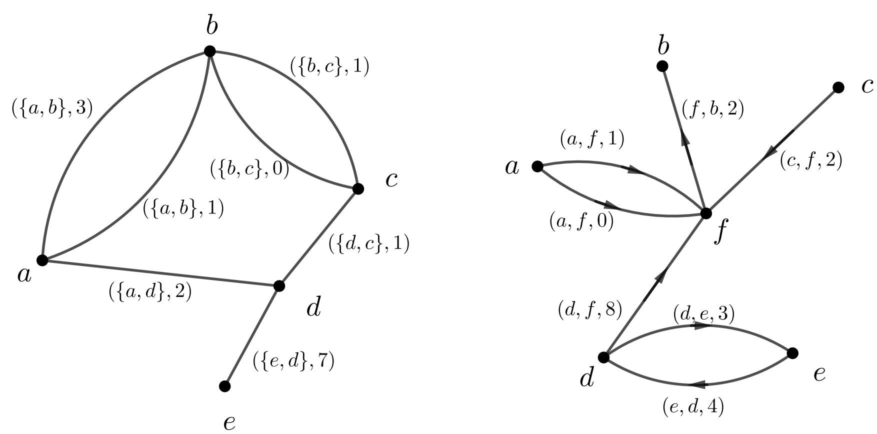
Volvamos al problema de los puentes de Königsberg y a la forma de modelarlo.



Como podemos ver en la figura, hay dos aristas entre 1 y 2 y dos aristas entre 2 y 3, luego el modelo no se ajusta a nuestra definición de grafo. Haremos entonces las siguientes definiciones:

Un **multigrafo** es un par $G = (V, E)$, donde V es un conjunto finito y E es un subconjunto finito de
$$\big\{\{x, y\} : x, y \in V\big\} \times \mathbb{N}.$$
Dados dos vértices $x, y \in V$, las aristas que los unen son los elementos de la forma $(\{x, y\}, n) \in E$. De esta forma podría representarse la figura de arriba mediante el par (V, E), donde $V = \{1, 2, 3, 4\}$ y
$$E = \big\{(\{1,2\},1), (\{1,2\},1), (\{1,4\},1), (\{2,3\},1), (\{2,3\},2), (\{2,4\},1), (\{3,4\},1)\big\}.$$

Un **multigrafo dirigido** es un par $G = (V, E)$, donde V es un conjunto finito y E es un subconjunto finito de $(V \times V) \times \mathbb{N}$. En este caso las aristas que unen dos vértices $x, y \in V$ son de la forma $(x, y, n) \in E$.



En general usaremos la notación $G = (V, E)$ tanto para grafos, grafos dirigidos, multigrafos o multigrafos dirigidos. Escribimos también en este caso $V(G) = V$ y $E(G) = E$.

6.1.1. Isomorfismos de grafos

Sean $G_1 = (V_1, E_1)$ y $G_2 = (V_2, E_2)$ dos grafos. Una función $f : V_1 \to V_2$ es un **isomorfismo de grafos** si

(i) f es biyectiva, y

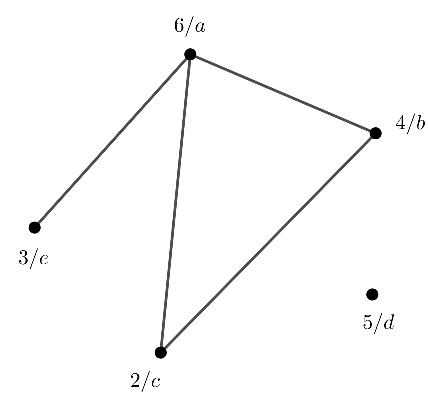
(ii) $\{x, y\} \in E_1$ si y sólo si $\{f(x), f(y)\} \in E_2$. Es decir, dos vértices son adyacentes si y sólo si sus imágenes por f lo son.

Observar que si $f : V_1 \to V_2$ es un isomorfismo de grafos, entonces queda definida automaticamente una función biyectiva $f : E_1 \to E_2$ (usamos la misma notación que para la función en los vértices). También notamos al isomorfismo por $f : G_1 \to G_2$ entendiendo esto como una correspondencia tanto entre los vértices como entre las aristas de ambos grafos. Emplearemos la notación $G_1 \cong G_2$ para indicar que G_1 y G_2 son **isomorfos**, es decir, que existe un isomorfismo entre ellos.

Ejemplo 6.1.1. Consideramos los siguientes grafos:

- $V_1 = \{2, 3, 4, 5, 6\}$ y E_1 definido por: x e y son adyacentes si x e y tienen algún divisor primo en común.
- $V_2 = \{a, b, c, d, e\}$ y $E_2 = \{\{a, b\}, \{a, c\}, \{a, e\}, \{b, c\}\}$.

Definimos $f : V_1 \to V_2$ por $f(2) = c$, $f(3) = e$, $f(4) = b, f(5) = d$ y $f(6) = a$. Puede verse que f es un isomorfismo entre los grafos $G_1 = (V_1, E_1)$ y $G_2 = (V_2, E_2)$.



Observar que f no es el único isomorfismo entre ambos grafos. Por ejemplo, uno puede considerar $g : V_1 \to V_2$ por $g(2) = b$, $g(3) = e$, $g(4) = c$, $g(5) = d$ y $g(6) = a$. ¿Hay algún otro isomorfismo?

En general nos interesarán, más que los grafos, las clases de isomorfismos de grafos. Por ejemplo, al mirar los grafos del Ejemplo 6.1.1, veremos los números y las letras simplemente como puntos que están unidos de a pares. Adoptaremos entonces la mirada que se plantea al principio del capítulo con el problema de los puentes de Königsberg, en el cual uno se olvida de que está trabajando con regiones y puentes y ve sólo un conjunto de vértices unidos por un conjunto de aristas.

Ejercicio 6.1.2. Observar que el isomorfismo de grafos define una relación de equivalencia en cualquier familia de grafos o grafos dirigidos.

En el caso de grafos dirigidos la definición de isomorfismo es análoga a la hecha anteriormente. La única modificación que hay que hacer es cambiar los pares en (ii) por pares ordenados.

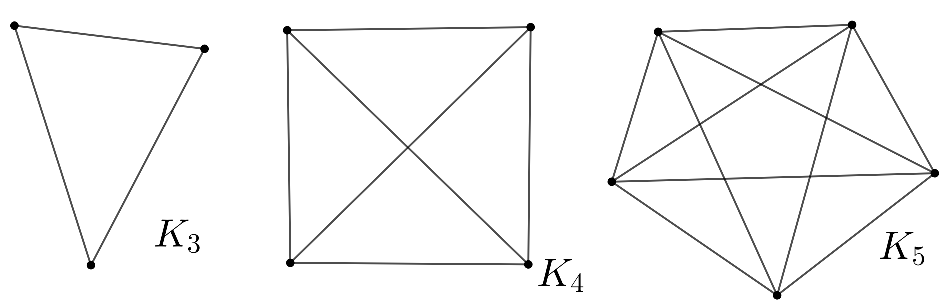
Para definir isomorfismo de multigrafos vamos a introducir la siguiente notación: si $G = (V, E)$ es un multigrafo y $x, y \in V$, denotamos por $E(x, y)$ al conjunto de las aristas entre x e y. Luego si $G_1 = (V_1, E_1)$ y $G_2 = (V_2, E_2)$ son dos multigrafos, decimos que una función $f : V_1 \to V_2$ es un **isomorfismo** si se cumple $\#E_1(x, y) = \#E_2(f(x), f(y))$ para todo par de vértices $x, y \in E_1$. De forma similar se define isomorfismo de multigrafo dirigido.

Ejemplos 6.1.3.

1. Un grafo $G = (V, E)$ se dice **completo** si

$$E = \big\{\{x, y\} : x, y \in V, x \neq y\big\}.$$

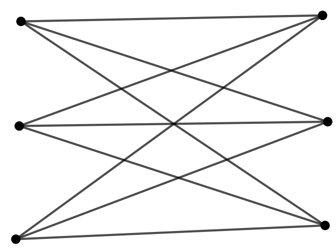
   Es decir que es el grafo sin lazos de vértices V con el máximo número de aristas. Podemos observar que la clase de isomorfismo de un grafo completo sólo depende del número de vértices, es decir, para cada $n \geq 1$ todos los grafos completos con n vértices son isomorfos. Luego notamos por K_n a cualquiera de ellos (o a todos ellos).



   Observar que si $G = (V, E)$ es un grafo completo, entonces toda función biyectiva $f : V \to V$ es un isomorfismo. Tenemos entonces que si G tiene n vértices, existen $P_n = n!$ isomorfismos de la forma $f : G \to G$.

2. Un grafo $G = (V, E)$ es **bipartito** si $V = V_1 \cup V_2$ con $V_1 \cap V_2 = \emptyset$ y $E = \big\{\{x, y\} : x \in V_1, y \in V_2\big\}$. Haciendo la misma consideración que para el grafo

completo, ponemos la notación $K_{n,m}$ para referirnos al grafo bipartito con vértices $V = V_1 \cup V_2$ con $\#V_1 = n$ y $\#V_2 = m$.



$K_{3,3}$

3. Un grafo $G = (V, E)$ es un **ciclo de largo n** si existe una numeración de sus vértices $V = \{x_1, \ldots, x_n\}$ de forma tal que

$$E = \big\{\{x_1, x_2\}, \{x_2, x_3\}, \ldots, \{x_{n-1}, x_n\}, \{x_n, x_1\}\big\}.$$

Es claro que todos los ciclos de largo n son isomorfos. Luego adoptamos la notación C_n para referirse a cualquiera de ellos (o a su clase de isomorfismo).

Ejercicio 6.1.4. Contar la cantidad de isomorfismos de la forma $f : G \to G$ en los casos $G = K_{n,m}$ y $G = C_n$.

6.1.2. Subgrafos

Aquí consideraremos grafos (no dirigidos), pero lo mismo puede hacerse para grafos dirigidos, multigrafos o multigrafos dirigidos.

Sea $G = (V, E)$ un grafo. Decimos que un grafo $G' = (V', E')$ es un **subgrafo** de G si $V' \subset V$ y $E' \subset E$. Para simplificar la notación notaremos $G' \leq G$ si G' es subgrafo de G.

Observar que $\leq$ induce una relación de orden en cualquier familia de grafos, en particular en la familia de todos los subgrafos de un grafo dado G, que notaremos por $\mathcal{S}(G)$. En adelante, cuando consideremos el máximo/mínimo subgrafo de G que cumpla determinada propiedad P, lo haremos siempre con respecto a esta relación en el subconjunto

$$\mathcal{S}(G, P) = \{G' \in \mathcal{S}(G) : G' \text{ satisface } P\}.$$

Un **encaje** de un grafo $G_1 = (V_1, E_1)$ en otro grafo $G_2 = (V_2, E_2)$ es una función inyectiva $f : V_1 \to V_2$ tal que si $x, y \in V_1$ son adyacentes, entonces $f(x), f(y) \in V_2$ son adyacentes. Denotamos también al encaje por $f : G_1 \to G_2$, y por $f : E_1 \to E_2$ a la función inducida en las aristas. De forma similar se define la noción encaje para grafos dirigidos.

Dados dos grafos (o grafos dirigidos) G_1 y G_2 escribimos

$$G_1 \preceq G_2 \Leftrightarrow \text{existe un encaje de } G_1 \text{ en } G_2.$$

Observar que esta definición no da una relación de orden dado que no se satisface la propiedad antisimétrica. De hecho, $G_1 \preceq G_2$ y $G_2 \preceq G_1$ implica que G_1 y G_2 son isomorfos. Sin embargo, si consideramos la relación de isomorfismo en una familia de grafos $\mathcal{G}$, entonces $\preceq$ define una relación de orden en el cociente $\mathcal{G}/\cong$, donde $\cong$ es la relación de isomorfismo.

Proposición 6.1.5. *Se tiene que $G_1 \preceq G_2$ si y sólo si existe G_1' un subgrafo de G_2 que es isomorfo a G_1.*

Demostración. ($\Rightarrow$) Supongamos que tenemos $G_1 = (V_1, E_1)$ y $G_2 = (V_2, E_2)$, y que $f : G_1 \to G_2$ es un encaje. Luego definimos el subgrafo $G_1' = (f(V_1), f(E_1))$. Es claro por la definición de encaje que f define un isomorfismo entre G_1 y G_1'.

($\Leftarrow$) Un isomorfismo $f : G_1 \to G_1'$ (con $G_1' \leq G_2$) se extiende de forma obvia a un encaje $f : G_1 \to G_2$. $\square$

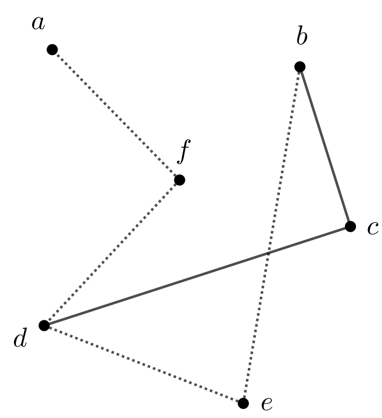
Como en realidad nos interesa trabajar con las clases de isomorfismo de grafos, diremos también que G_1 es subgrafo de G_2 si $G_1 \preceq G_2$.

Dado un grafo $G = (V, E)$ y $V' \subset V$ un subconjunto cualquiera. El **subgrafo generado** por V' es el máximo subgrafo de G que tiene a V' como conjunto de vértices.

En la siguiente figura puede verse el grafo generado por los vértices b, c y d de un grafo $G = (V, E)$ con

$$V = \{a, b, c, d, e, f\} \text{ y } E = \{\{a, f\}, \{b, c\}, \{b, e\}, \{c, d\}, \{d, e\}, \{d, f\}\}.$$

Las líneas punteadas indican las aristas de G que no están en el subgrafo generado.

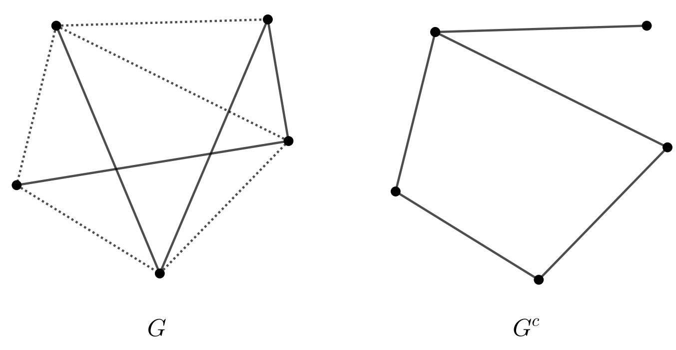


Definimos el **complemento** de un grafo sin lazos $G = (V, E)$ como el grafo $G^c = (V, E')$

$$E' = \big\{\{x, y\} : x \neq y, \{x, y\} \notin E\big\}.$$

Es decir que es el grafo que resulta de sacarle a K_n las aristas de G, donde $n = \#V$.

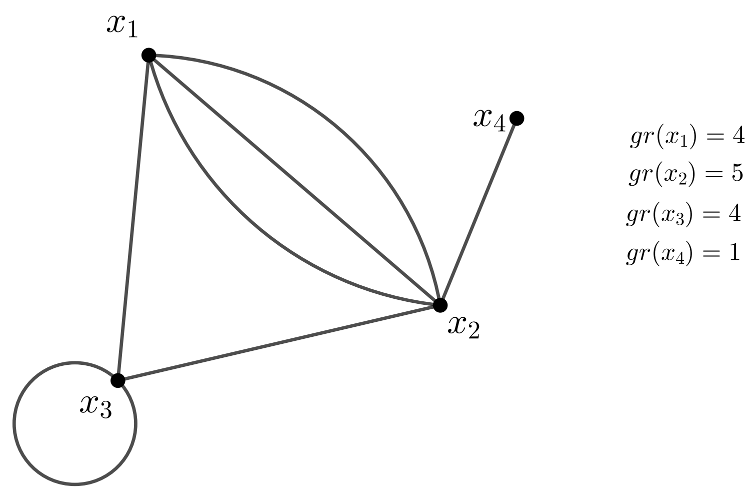
En la siguiente figura podemos ver el grafo G y su complemento G^c. Las líneas punteadas a la izquierda indican las aristas que están en K_5 pero no en G.



Ejercicio 6.1.6. Probar que si G_1 y G_2 son dos grafos tales que $V(G_1) = V(G_2)$, entonces $G_1 \leq G_2$ implica $G_2^c \leq G_1^c$. Concluir que si G_1 y G_2 tienen la misma cantidad de vértices, entonces $G_1 \preceq G_2$ implica $G_2^c \preceq G_1^c$.

6.1.3. Grado de un vértice

El **grado** de un vértice x en un grafo multigrafo G, notado por $gr(x)$, es el número de aristas que inciden en el vértice. Un lazo en x cuenta doble.



Una observación importante sobre el grado es que es invariante por isomorfismos. Es decir que si $f : G_1 \to G_2$ es un isomorfismo de grafos, entonces para todo vértice x de G_1 se tiene $gr(x) = gr(f(x))$. Esto da una herramienta fundamental a la hora de determinar si existen isomorfirmos entre dos grafos y en ese caso cúantos de ellos hay.

Lema 6.1.7. *Si $G = (V, E)$ es un grafo o multigrafo, entonces*

$$\sum_{x \in V} gr(x) = 2\#E.$$

Demostración. Simplemente observamos que cada lazo contribuye a sumar dos al grado de un vértice y cada arista que une dos vértices suma uno en el grado de cada uno de ellos. □

El lema anterior se conoce como *Handshaking lemma* debido a la siguiente consecuencia: si en una fiesta los invitados saludan a otros invitados (no necesariamente todos) dandose un apretón de manos, entonces el número de personas que da una cantidad impar de apretones de manos debe ser par.

Para el caso de un multigrafo dirigido $G = (V, E)$ podemos hacer la siguientes definiciones:

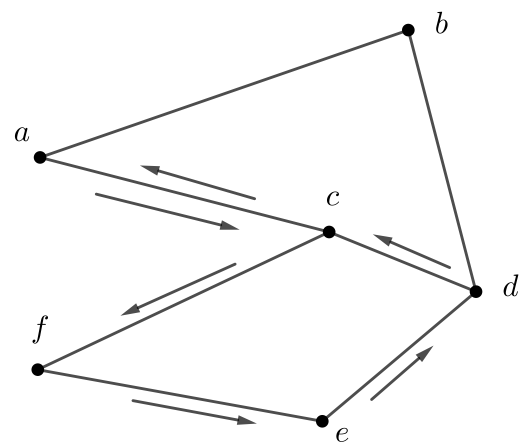
- El **grado entrante** de x es la cantidad de aristas entrantes en x (de la forma $(y, x, n) \in V \times V \times \mathbb{N}$). Lo notamos por $gr_-(x)$.
- El **grado saliente** de x es la cantidad de aristas salientes en x (de la forma $(x, y, n) \in V \times V \times \mathbb{N}$). Lo notamos por $gr_+(x)$.

Aquí también tenemos que tanto el grado entrante como el grado saliente son invariantes por isomorfismos. Además se cumple

$$\sum_{x\in V} gr_+(x) = \sum_{x\in V} gr_-(x) = \#E.$$

6.2. Caminatas en grafos

Un **camino** en un grafo $G = (V, E)$ es una secuencia de vértices $c = (x_0, x_1, \ldots, x_n)$ tal que x_{i-1} es adyacente a x_i para todo $i = 1, \ldots, n$. En este caso decimos que el camino une x_0 con x_n. Si $x_0 = x_n$ el camino se dice **cerrado**. La **longitud** del camino c es $long(c) = n$, es decir, la cantidad de aristas (contadas con repetición) por las que pasa el camino. Un camino cerrado de la forma (x_0) se denomina **trivial** y su longitud es 0.



(a, c, f, e, d, c, a)

Decimos que un camino es un **recorrido** si no repite aristas, y que es un **camino simple** si no repite vértices. Llamaremos **circuito** a un recorrido cerrado y **ciclo** a un camino simple cerrado. Observar que un camino simple es un recorrido, salvo que se trate de un ciclo de longitud 2. También sucede que un ciclo de longitud mayor o igual a tres es un circuito.

Proposición 6.2.1. *Sea $G = (V, E)$ un grafo y $x, y \in V$. Si existe un camino que une x con y, entonces existe un camino simple que une ambos vértices.*

Demostración. Supongamos que tenemos un camino de longitud n desde x a y. Consideramos entonces el conjunto de todos los caminos de x a y con longitud menor o igual a n, al que notamos por $\mathcal{C}_n$. Es claro que este conjunto es no vacío, además es finito porque V es finito. Luego existe un camino $c = (x = x_0, x_1, \ldots, x_k = y)$ que minimiza la longitud de todos los elementos de $\mathcal{C}_n$.

Si c no es un camino simple, entonces existen dos índices diferentes $i, j \in \{0, \ldots, k\}$ tal que $x_i = x_j$. Suponiendo que $i < j$ podemos observar que

$$c' = (x_0, \ldots, x_i, x_{j+1}, \ldots, x_k)$$

es un camino en $\mathcal{C}_n$ de longitud estrictamente menor a k, lo que contradice el hecho de que k es el mínimo de las longitudes de los caminos en $\mathcal{C}_n$. Concluimos entonces que c debe ser un camino simple. $\square$

Ejercicio 6.2.2. Probar que un grafo bipartito no puede tener ciclos de largo impar.

Diremos que un grafo $G = (V, E)$ es **conexo** si para todo par de vértices $x, y \in V$ existe un camino que los une. Por otro lado, dado un grafo $G = (V, E)$, podemos definir la relación $\mathcal{R}$ en el conjunto de los vértices de la siguiente manera:

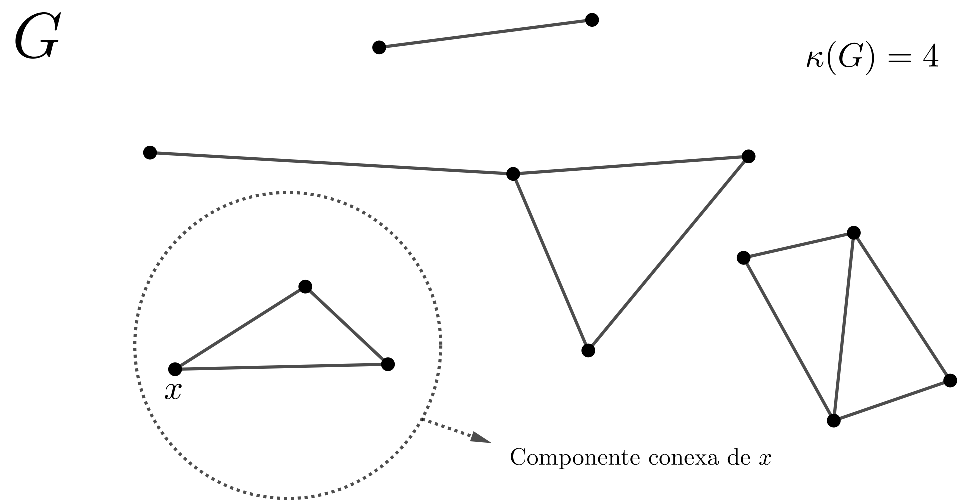
$$x\mathcal{R}y \Leftrightarrow \text{ existe un camino que une } x \text{ con } y.$$

Se deja como ejercicio probar que $\mathcal{R}$ es una relación de equivalencia.

La **componente conexa** de un vértice $x \in V$ es el subgrafo de G generado por la clase de equivalencia $[x] \subset V$.

Ejercicio 6.2.3. Probar que la componente conexa de un vértice x de un grafo es el máximo subgrafo conexo que contiene a x.

Usaremos la notación $\kappa(G)$ para indicar el número de componentes conexas del grafo G, que coincide con el cardinal del cociente $V/\mathcal{R}$. Observar que G es conexo si y sólo si $\kappa(G) = 1$.



Hay una noción natural de distancia en los grafos conexos que está relacionada con la longitud: Para un par de vértices $x, y \in V$ tomamos $\mathcal{C}(x, y)$ el conjunto de los caminos que unen a x con y, luego definimos

$$dist(x, y) = \text{mín}\{long(c) : c \in \mathcal{C}(x, y)\}.$$

Observación 6.2.4. En general, una **distancia** o **métrica** en un conjunto X es una función $d : X \times X \to [0, +\infty)$ que cumple:

- $d(x, y) = 0$ si y sólo si $x = y$.
- $d(x, y) = d(y, x)$ para todo par de puntos $x, y \in X$.
- Desigualdad triangular: dados tres puntos x, y, z, se cumple $d(x, z) \leq d(x, y) + d(y, z)$.

Luego $dist : V \times V \to \mathbb{N}$ es efectivamente una distancia.

El diámetro de un grafo conexo $G = (V, E)$ es

$$\text{Diam}(G) = \text{máx}\big\{dist(x, y) : x, y \in V\big\}.$$

Si $G = (V, E)$ es un grafo dirigido también se pueden considerar en él caminos, recorridos y caminos simples. Sin embargo en este caso $dist$ no resulta una verdadera distancia en los vértices ya que no se cumple la segunda condición de la Observación 6.2.4.

Para dar un camino en un multigrafo debemos especificar cuál de las aristas se toma al unir dos vértices adyacentes. Teniendo esto en cuenta definimos un **camino** en un multigrafo $G = (V, E)$ como una secuencia

$$(x_0, e_0, x_1, e_1, \ldots, e_{n-1}, x_n)$$

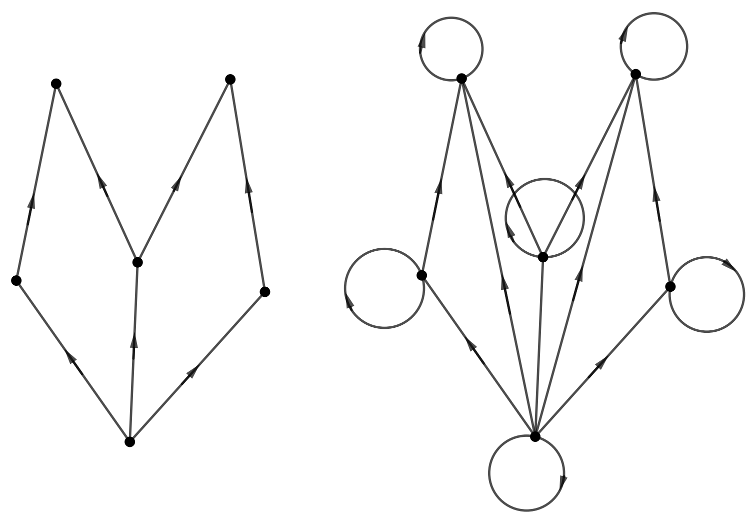
donde $x_1, \ldots, x_n \in V$ y para cada $i = 0, \ldots, n-1$, e_i es una arista que une x_i con x_{i+1}. Para multigrafos dirigidos la definición es análoga.

Luego de tener esta definición se hacen de forma obvia las definiciones de **camino cerrado**, **recorrido**, **circuito, camino simple** y **ciclo** en un multigrafo o multigrafo dirigido.

Observación 6.2.5. Si $G = (V, E)$ es un grafo dirigido sin ciclos que no sean lazos, entonces puede definirse una relación de orden en V de la siguiente forma:

$$x \leq y \Leftrightarrow \text{existe un camino de } x \text{ a } y. \tag{6.1}$$

Por otro lado un conjunto ordenado puede verse como un grafo dirigido sin ciclos (diferentes de lazos). Sin embargo, si $\leq$ es una relación de orden en V, entonces existe más de un grafo que genera $\leq$ mediante (6.1).



En la figura anterior pueden verse grafos dirigidos que generan la misma relación de orden $\mathcal{R}$.

6.2.1. Recorridos y circuitos Eulerianos

Diremos que un recorrido o un circuito en un multigrafo no dirigido G es **Euleriano** si pasa por todas las aristas del multigrafo. Observar que, en particular, el problema de los puentes de Königsberg consiste en encontrar o probar la inexistencia de un circuito Euleriano. Una generalización de dicho problema puede enunciarse de la siguiente forma:

Problema 6.2.6. *Sea $G = (V, E)$ un multigrafo conexo. ¿Existe un recorrido Euleriano en G? ¿Y un circuito Euleriano?*

El siguiente teorema resuelve parte del Problema 6.2.6.

Teorema 6.2.7. *Un multigrafo conexo $G = (V, E)$ admite un circuito Euleriano si y solo si el grado de todos sus vértices es par.*

Demostración. ($\Rightarrow$) Asumimos que existe un circuito euleriano y sea $x \in V$. Notamos por E_x al conjunto de aristas que inciden en x. Podemos suponer aquí que G no tiene lazos, puesto que si los tuviera esto no alteraría la existencia de un recorrido Euleriano ni la paridad de las aristas.

Escribimos el circuito Euleriano empezando de x:

$$(x = x_0, e_1, \ldots, e_{n-1}, x_n = x).$$

Si en el circuito se tiene $x_{i_1} = x_{i_2} = \cdots = x_{i_k} = x$ (con $i_1 = 0$ e $i_k = n$), entonces

$$E_x = \{e_{i_1}, e_{i_2-1}, e_{i_2}, \ldots, e_{i_{k-1}-1}, e_{i_{k-1}}\}.$$

Concluimos que $gr(x) = \#E_x$ es par.

($\Leftarrow$) Suponemos ahora que todos los vértices de G tienen grado par. Consideramos $\mathcal{C}$ la familia de todos los recorridos en G. Como la longitud de todos los elementos de $\mathcal{C}$ está acotada por $\#E$ podemos tomar un recorrido C con longitud máxima. Vamos a probar que C es un circuito Euleriano.

Veamos primero que C es un circuito. Para esto escribimos

$$C = (x_0, e_1, x_1, \ldots, e_n, x_n).$$

Si $x_0 \neq x_n$, entonces las aristas que inciden en $x_n = x_{i_1} = \cdots = x_{i_k}$ (con $i_1 < \cdots < i_k < n$) son $e_{i_1}, e_{i_1+1}, \ldots, e_{i_k}, e_{i_k+1}, e_n$. Como $gr(x_n)$ es impar existe $e_{n+1} \in E$ que incide en x_n y no es ninguna de las anteriores. Luego

$$(x_0, e_1, x_1, \ldots, e_n, x_n, e_{n+1}, x_{n+1})$$

es un recorrido cuya longitud es estrictamente mayor que la de C, lo que es absurdo.

Supongamos ahora que el circuito C no recorre todas las aristas. En este caso vemos que existe una arista $\tilde{e}$ de G que no está en C y que incide en un vértice $\tilde{x}$ de C. Para esto podemos tomar una arista que no está en C, si ninguno de sus extremos está en C existe un camino de uno de ellos a un vértice de C. Escribimos

$$(y_0, \tilde{e}_1, y_1, \ldots, \tilde{e}_\ell, y_\ell),$$

donde y_0 no es un vértice de C mientras que y_ℓ si lo es. Si r es el primer índice tal que y_r está en C, entonces $\tilde{e}_r$ no está en C. Escribimos entonces $\tilde{x} = y_r$, $y = y_{r-1}$ y $\tilde{e} = \tilde{e}_r$.

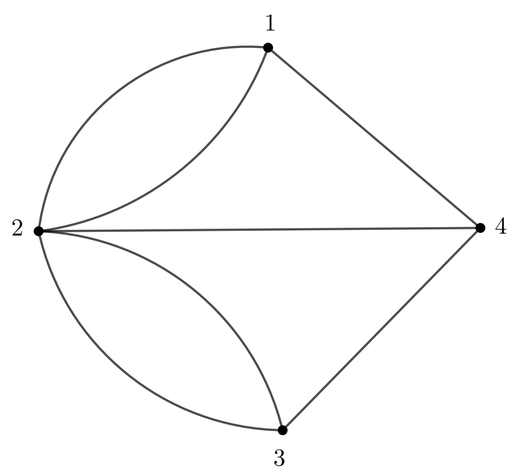
Como C es un circuito podemos suponer $x_0 = x_n = \tilde{x}$, luego el recorrido

$$(x_0, e_1, \ldots, e_n, x_n, \tilde{e}, y)$$

es un recorrido de longitud estrictamente mayor a la longitud de C, lo que es absurdo.

Concluimos entonces que C es un circuito Euleriano. □

Utilizando el Teorema 6.2.7 podemos rápidamente concluir la solución del problema de los puentes de Königsberg.



Vemos que $gr(1) = gr(3) = gr(4) = 3$ y $gr(2) = 5$, por lo que no puede haber un circuito Euleriano. Como se ve en el siguiente corolario tampoco puede haber un recorrido Euleriano abierto (es decir, que no sea circuito).

Corolario 6.2.8. *Un multigrafo conexo G admite un recorrido Euleriano abierto si y sólo si dos de sus vértices tienen grado impar y el resto tienen grado par.*

Demostración. (⇒) Supongamos que existe un recorrido Euleriano $(x_0, e_0, \ldots, e_{n-1}, x_n)$. Luego si agregamos al grafo G una arista que une x_0 con x_n tenemos que existe un circuito Euleriano. Por el Teorema 6.2.7 se tiene que el grado de todas las aristas de este nuevo grafo es par. Por lo tanto el grado de todos los vértices del grafo original G es par, salvo para x_0 y x_n, que tienen grado impar.

(⇐) Supongamos que x e y son los vértices que tienen grado impar. Se considera G' el grafo que resulta de agregarle una arista a G uniendo x con y. Luego los vértices de G' tienen todos grado par, por lo que existe un circuito Euleriano en G'. Es claro entonces que existe un recorrido Euleriano en G que une x con y. □

Para el caso dirigido tenemos un resultado similar. Consideraremos que un multigrafo dirigido G es **conexo** si lo es el multigrafo no dirigido que resulta de quitarle la dirección a las aristas de G.

Teorema 6.2.9. *Sea $G = (V, E)$ un multigrafo dirigido conexo. Entonces:*

1. *G admite un circuito Euleriano si y solo si el grado entrante de cada vértice es igual a su grado saliente.*

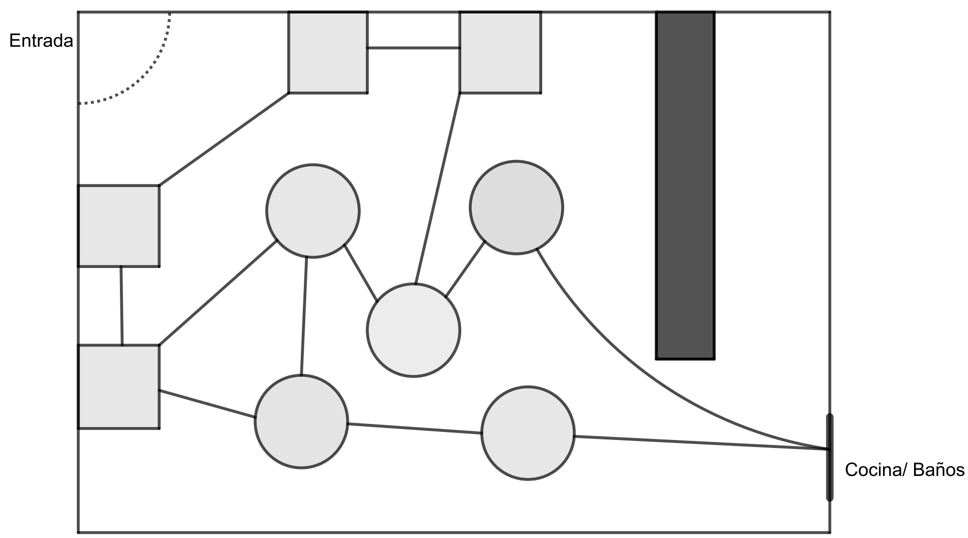
2. *G admite un recorrido Euleriano abierto si y solo si existen dos vértices x_0 y x_1 tales que:*

   - $gr_+(x_0) = gr_-(x_0) - 1$.
   - $gr_-(x_1) = gr_+(x_1) - 1$.
   - *Si $x \neq x_0, x_1$, entonces $gr(x)_+ = gr(x)_-$.*

Las pruebas del Teorema 6.2.7 y el Corolario 6.2.8 pueden adaptarse al caso dirigido para probar el Teorema 6.2.9. Se deja como ejercicio verificarlo.

6.2.2. Caminos y ciclos Hamiltonianos

Ejemplo 6.2.10. *Influido por lo que le contaba el Comadreja (que para ese tiempo hasta dormía en el bar), el Turco se había obsesionado con los grafos. Tanto era así que una mañana se puso a dibujar líneas sobre el piso uniendo pares de mesas. Ese día le pidió al único mozo del bar que siempre que se moviera entre las mesas lo hiciera respetando las aristas que había marcado. Después de negociar una subida de sueldo a cambio del nuevo capricho, el mozo aceptó. Se muestra a continuación el plano del bar incluyendo los caminos que dibujó el Turco entre las mesas.*



Un día, ya tomado por completo por el delirio, el Turco le pidió al mozo que cambiara todos los manteles de las mesas con la condición de no pasar dos veces por la misma mesa. Le dijo además que si en un momento se quedaba sin posibilidades de continuar tendría que volver a la cocina y empezar de nuevo. Totalmente fastidiado, el mozo reboleó los manteles por el aire y se fue pateando mesas para nunca volver.

Al otro día el Turco contrató al Comadreja para cubrir el puesto, confiado en que él sí entendería sus excentricidades.

La sociedad de ambos personajes abrió la puerta a una etapa dorada del bar. Por desgracia esta duró poco. Pronto los clientes dejaron de ir. Quizá tenga que ver el hecho de que se les haya ocurrido conectar, con una línea dibujada en el suelo, la puerta de entrada con una de las mesas y exigirle a los clientes que también ellos respetaran las aristas al moverse.

Del ejemplo anterior podemos extraer el siguiente problema: Dado un grafo G, ¿existe un camino simple que pasa por todos los vértices? Un tal camino se denomina **camino Hamiltoniano**. Por otro lado, un **ciclo Hamiltoniano** es un ciclo que pasa por todos los vértices.

Consideraremos en esta sección grafos y no multigrafos por una sencilla razón: un camino o ciclo Hamiltoniano solo puede pasar por una arista que une dos vértices dados, luego un multigrafo admite un camino o ciclo Hamiltoniano si y sólo si lo admite el grafo que resulta de sacarle al multigrafo original las aristas que repiten pares de vértices adyacentes.

Determinar cuáles son exactamente los grafos que admiten caminos o ciclos Hamiltonianos es más difícil que para recorridos y circuitos Eulerianos. Daremos sin embargo algunos condiciones suficientes. Una idea general que engloba a estas condiciones es la siguiente: cuanto más aristas haya en el grafo más probable será que admita un camino o ciclo Hamiltoniano.

Teorema 6.2.11. *Sea G un grafo sin lazos con n vértices.*

1. *Si para todo par de vértices x e y se tiene $gr(x) + gr(y) \geq n - 1$, entonces G admite un camino Hamiltoniano.*
2. *Si para todo par de vértices x e y se tiene $gr(x) + gr(y) \geq n$, entonces G admite un ciclo Hamiltoniano.*

Demostración. Empecemos probando la primera parte. Para esto veamos primero que G es conexo. Si no lo fuera tomamos dos componentes conexas G_1 y G_2 y dos vértices x e y, uno en cada una de estas componentes conexas. Si G_1 tiene n_1 vértices y G_2 tiene n_2 vértices, tenemos

$$gr(x) + gr(y) \leq n_1 + n_2 - 2 \leq n - 2,$$

lo que contradice la hipótesis.

Tomamos ahora $c = (x_1, \ldots, x_m)$ un camino simple abierto de longitud máxima, suponemos que no es un camino Hamiltoniano, es decir que $m < n$.

Afirmación: Existe un ciclo que pasa por todos los vértices de c.

Si x_1 y x_m son adyacentes o si alguno de estos vértices es adyacente a otro vértice fuera del camino c, entonces c puede prolongarse por alguno de los extremos, lo que contradice el hecho de que tiene longitud máxima.

En el otro caso todos los vértices adyacentes a los vértices x_1 y x_m están en el conjunto $\{x_2, \ldots, x_{m-1}\}$. Vamos a definir los siguientes conjuntos de índices:

$$S_1 = \{k \in \{3, \ldots, m-1\} : x_1 \text{ es adyacente a } x_k\}$$

$$S_m = \{k \in \{3, \ldots, m-1\} : x_m \text{ es adyacente a } x_{k-1}\}.$$

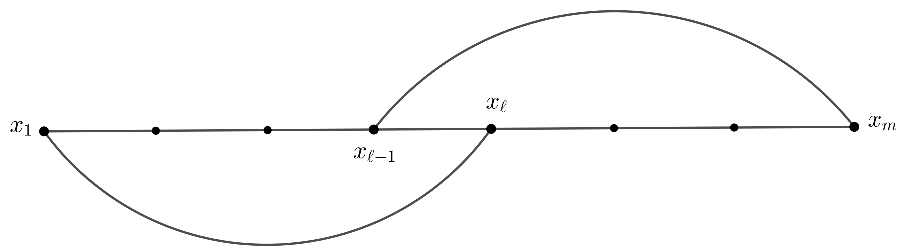
Como $gr(x_1) + gr(x_m) \geq n - 1$, entonces

$$\#S_1 + \#S_m \geq n - 3 > m - 3 = \#\{3, \ldots, m-1\},$$

lo que implica que $S_1 \cap S_m \neq \emptyset$. Tomamos $\ell \in S_1 \cap S_m$, luego x_ℓ es adyacente a x_1 y $x_{\ell-1}$ es adyacente a x_m. Obtenermos así el ciclo

$$(x_1, \ldots, x_{\ell-1}, x_m, x_{m+1} \ldots, x_\ell, x_1).$$

Esto prueba la afirmación.



Ahora reescribimos el ciclo de largo m obtenido en la afirmación de la forma $(y_1, \ldots, y_m, y_1)$. Como $m < n$ y G es conexo, existe un vértice del ciclo y_k que es adyacente a un vértice x fuera del ciclo. Entonces existe un camino simple

$$(x, y_k, y_{k+1}, \ldots, y_m, y_1, \ldots, y_{k-1})$$

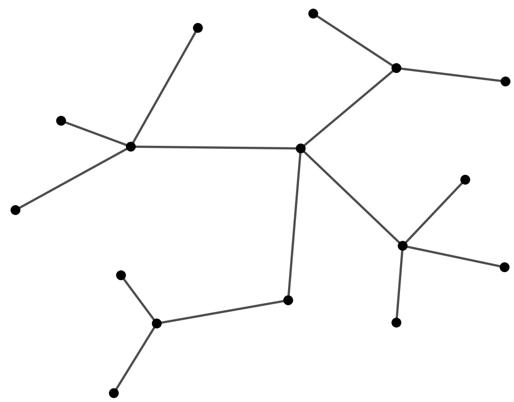
que es más largo que el camino c tomado al principio. Esto es absurdo porque c tiene longitud máxima. Concluimos entonces que $m = n$ y por lo tanto c es un camino Hamiltoniano.

Para probar la segunda parte observamos que por lo anterior el grafo G admite un camino Hamiltoniano. Repitiendo el argumento utilizado para probar la afirmación puede construirse un ciclo que pase por los mismos vértices de este camino, quedando así un ciclo Hamiltoniano. $\square$

Ejercicio 6.2.12. Probar que si $G = (V, E)$ es un grafo sin lazos con $\#V \geq 3$ y $\#E \geq C_2^{n-1} + 2$, entones G admite un ciclo Hamiltoniano.

6.3. Árboles

Decimos que un grafo no dirigido G es un **árbol** si es conexo y no tiene ciclos (en particular no tiene lazos).



Dado un grafo cualquiera $G = (V, E)$ decimos que un subgrafo $A \leq G$ es un **árbol recubridor** si es un árbol y cumple $V(A) = V$.

Teorema 6.3.1. *Todo grafo conexo tiene un árbol recubridor.*

En la prueba del teorema usaremos el siguiente lema:

Lema 6.3.2. *Todo conjunto ordenado finito no vacío* $(X, \leq)$ *tiene un elemento maximal.*

Demostración. Lo haremos por inducción en $n = \#X \geq 1$. Es claro que si $X = \{x\}$, entonces x es un elemento maximal, luego el caso $n = 1$ está probado.

Supongamos que la afirmación es cierta para conjuntos ordenados de cardinal n y tomemos $(X, \leq)$ con $\#X = n + 1$. Si $x_0 \in X$ es un elemento cualquiera el conjunto ordenado $\big(X \setminus \{x_0\}, \leq\big)$ tiene un elemento maximal m. Si este no es maximal en X, luego $m \leq x_0$, lo que implica que x_0 es maximal. □

Demostración del Teorema 6.3.1. Consideramos $\mathcal{A}$ el conjunto de árboles que son subgrafos de $G = (V, E)$, lo ordenamos por:

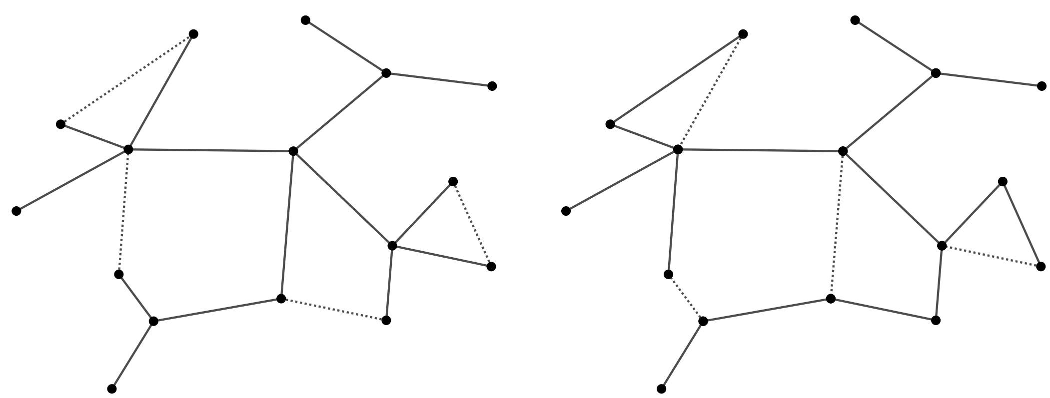
$$A_1 \leq A_2 \Leftrightarrow A_1 \textit{ es subgrafo de } A_2.$$

El conjunto $\mathcal{A}$ es finito y no vacío, luego por el Lema 6.3.2 existe elemento maximal $A_M \in \mathcal{A}$. Vamos a probar que A_M es un árbol recubridor de G.

Si existe un vértice $x_0 \in V \setminus V(A_M)$, entonces existen vértices $x_1 \in V \setminus V(A_M)$ y $x_2 \in V(A_M)$ que son adyacentes en G. Esto lo vemos tomando $x \in V(A_M)$ y un camino $(x_0 = y_0, \ldots, y_n = x)$. Si consideramos $k = \text{máx}\{i : y_i \notin V(A_M)\}$, entonces podemos tomar $x_1 = y_k$ y $x_2 = y_{k+1}$.

Tenemos entonces que si A_M no es un árbol recubridor, entonces existe un árbol más grande, que resulta de agregar a A_M el vértice x_1 y la arista $\{x_1, x_2\}$, lo que es absurdo. $\square$

En general el árbol recubridor de un grafo no es único. En la siguiente figura pueden verse dos diferentes árboles recubridores de un mismo grafo G. Las líneas punteadas indican las aristas de G que no están en el árbol recubridor correspondiente.

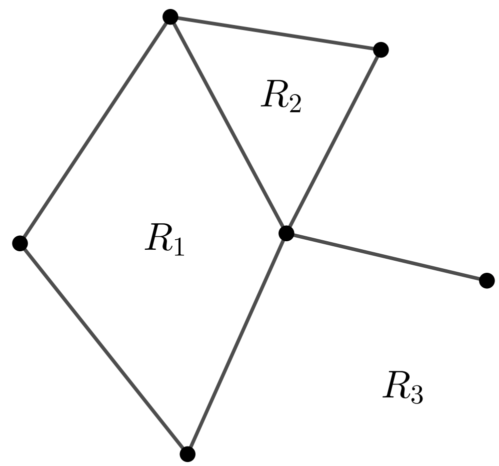


6.4. Planaridad

El segundo problema dado al principio del capítulo (conexión de servicios básicos) puede interpretarse de la siguiente manera: ¿Es posible dibujar en el plano el grafo bipartito $K_{3,3}$ de forma tal de no intersectar sus aristas?

Podemos preguntarnos más en general si un grafo puede dibujarse en el plano sin intersectar aristas. Diremos en este caso que el grafo (o multigrafo) es **plano** o **planar**, y que su dibujo en el plano es una **representación plana** del grafo.

Fijado un grafo planar junto con su representación plana, observamos que los puntos del plano que no son vértices y no pertenecen a ninguna arista se distribuyen en lo que llamamos **regiones**. Podemos definir el **grado** de una región como la cantidad de aristas que la delimitan.



$gr(R_1) = 4$

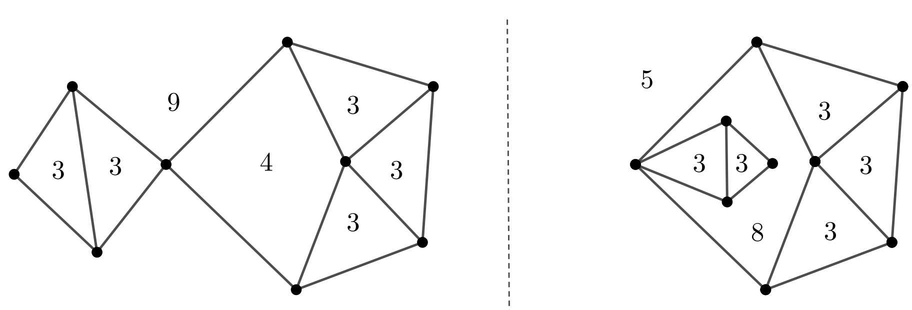
$gr(R_2) = 3$

$gr(R_3) = 7$

Hay dos cosas importantes a tener en cuenta en la definición del grado de una región:

1. Si una región está delimitada por un vértice de grado 1 que no es aislado, entonces la arista que incide en ese vértice cuenta como dos lados de la región. Esto es lo que sucede con la región no acotada R_3 de la figura anterior.

2. La definición de grado de una región no es intrínseca del grafo si no que depende de la representación plana. Podemos ver esto con el siguiente ejemplo, en el que tenemos dos representaciones planas del mismo grafo. El grado de cada región es indicado en su interior.



Notamos por $v(G)$ a la cantidad de vértices de G, por $a(G)$ a la cantidad de aristas de G y por $r(G)$ a la cantidad de regiones de G (esta última puede depender a priori de la representación plana).

El siguiente teorema de Euler relaciona las cantidades anteriores en el caso de grafos conexos.

Teorema 6.4.1. *Sea G un grafo planar conexo sin lazos junto con una representación plana fijada. Entonces*

$$v(G) - a(G) + r(G) = 2. \tag{6.2}$$

Demostración. Lo hacemos por inducción en la cantidad de aristas $n = a(G)$. Los casos $n = 0$ y $n = 1$ es claro. Supongamos entonces que es cierto para cierto n y tomemos G con $a(G) = n + 1$.

Tomamos e una arista de G y G' el grafo que resulta de quitarle e a G con la representación plana inducida por la de G. Si G' es conexo, entonces al quitar e dos regiones de G se unificaron en una de G', luego tenemos

$$v(G) - a(G) + r(G) = v(G') - \big(a(G') + 1\big) + \big(r(G') + 1\big) = v(G') - a(G')r(G') = 2.$$

Por otro lado, si G' es disconexo debe tener dos componentes conexas G_1 y G_2 que cumplen $v(G) = v(G_1) + v(G_2)$, $a(G) = a(G_1) + a(G_2) + 1$ y $r(G) = r(G_1) + r(G_2) - 1$. Luego

$$\begin{aligned} v(G) - a(G) + r(G) &= v(G_1) + v(G_2) - a(G_1) - a(G_2) - 1 + r(G_1) + r(G_2) - 1 \\ &= \big(v(G_1) - a(G_1) + r(G_1)\big) + \big(v(G_2) - a(G_2) + r(G_2)\big) - 2 = 2. \end{aligned}$$

□

Observación 6.4.2.

1. El teorema anterior muestra que la cantidad de regiones no depende de la representación plana si no sólo del grafo G.

2. Un grafo planar puede verse como un grafo en la esfera. Se observa fácilmente que un grafo es plano si y sólo si admite una representación en la esfera (por lo que podemos llamarlos también **grafos esféricos**).

3. El número $v-a+r$ se denomina **característica de Euler**. Tenemos entonces que tanto la característica de Euler del plano como la de la esfera es 2. Sin embargo hay superficies con característica de Euler diferente.

4. Si permitimos lazos la fórmula (6.2) sigue siendo cierta. También es cierta para multigrafos (se deja como ejercicio).

Ejercicio 6.4.3. Generalizar el Teorema 6.4.1 para grafos no conexos.

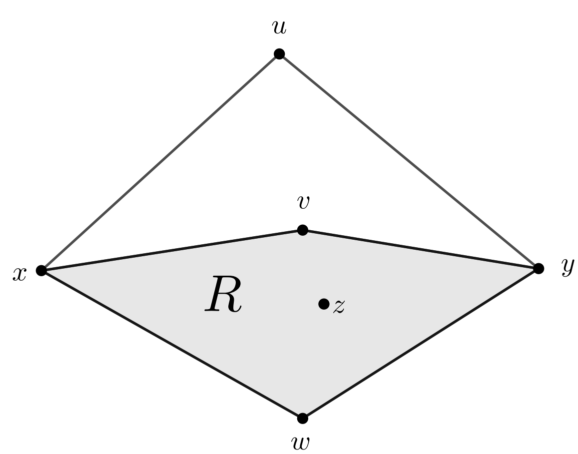
6.4.1. Grafos no planares

En este punto volvemos al segundo de los problemas presentados al principio del capítulo. La siguiente proposición responde a la pregunta planteada.

Proposición 6.4.4. *Los grafos $K_{3,3}$ y K_5 no son planares.*

Demostración. Veamos que $K_{3,3}$ no es plano. El caso de K_5 puede probarse usando un argumento similar.

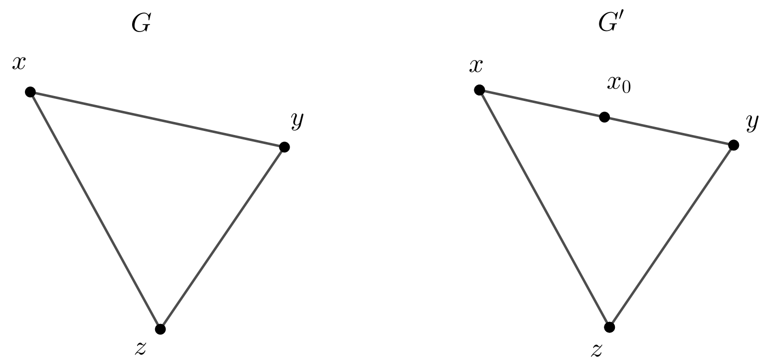
Supongamos que $K_{3,3}$ es planar y notemos por $\{u, v, w, x, y, z\}$ a sus vértices, de forma tal que u, v y w son adyacentes a x, y y z. El subgrafo generado por los vértices u, v, w, x e y es $K_{3,2}$. Usando la característica de Euler podemos deducir que este subgrafo planar tiene 3 regiones. Como un grafo bipartito no tiene ciclos de longitud impar (Ejercicio 6.2.2) concluimos que las tres regiones del subgrafo tienen grado cuatro.



Llamemos R a la región (de $K_{3,2}$) que contiene al sexto vértice z. En el borde de dicha región sólo pueden aparecer dos de los tres vértices u, v y w, por lo que uno de ellos no puede conectarse con z. Esto muestra que no existe una representación plana de $K_{3,3}$. $\square$

En realidad la proposición anterior es parte de un resultado más general que enunciaremos sin demostrar. Para esto necesitamos hacer primero algunas definiciones.

Sea $G = (V, E)$ un grafo. Decimos que el grafo $G' = (V', E')$ es una **subdivisión elemental** de G si $V' = V \cup \{x_0\}$ y existe un par de vértices adyacentes $x, y \in V$ tal que $E' = (E \setminus \{\{x, y\}\}) \cup \{\{x, x_0\}, \{x_0, y\}\}$. Dicho de otro modo, G' se obtiene al dividir en dos una arista de G poniendo en esta un nevo vértice. De forma similar puede hacerse la definición para multigrafos.



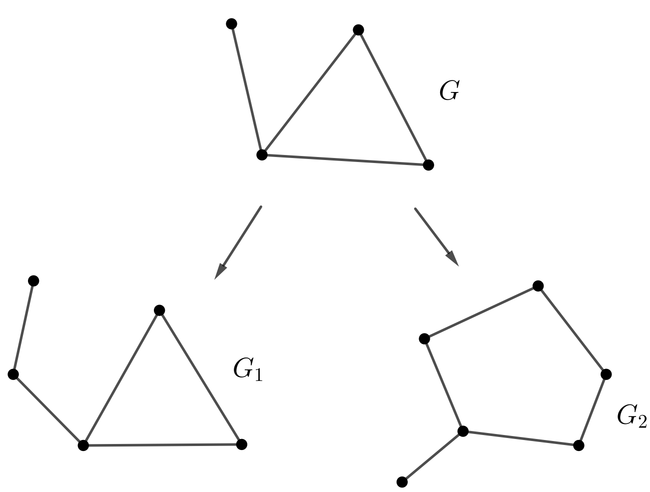
Un grafo G' es una **subdivisión** de otro grafo G si existe una secuencia finita de grafos

$$G_0 = G, G_1, \ldots, G_{k-1}, G_k = G'$$

tal que G_i es una subdivisión elemental de G_{i-1} para todo $i = 1, \ldots, k$.

Diremos que G_1 y G_2 son grafos (o multigrafos) **homeomorfos** si existen tres grafos G, G_1' y G_2' tales que

- G_1' y G_2' son subdivisiones de G,
- G_1 es isomorfo a G_1' y G_2 es isomorfo a G_2'.



Observación 6.4.5.

- La relación de homeomorfismo define una relación de equivalencia en cualquier familia de grafos o multigrafos $\mathcal{G}$.
- La condición de planaridad se preserva por homeomorfismo, es decir que si G_1 y G_2 son homeomorfos, entonces G_1 es plano si y sólo si G_2 lo es.
- Todo multigrafo es homeomorfo a un grafo. Más precisamente todo multigrafo tiene una subdivisión que es un grafo. Luego el problema de la planaridad de multigrafos se reduce al caso de los grafos.

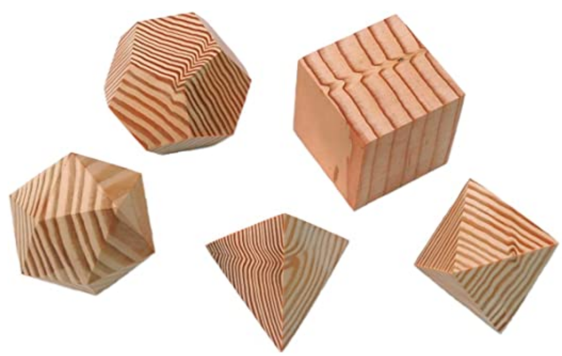
Habiendo definido estas nociones estamos listos para enunciar el siguiente teorema:

Teorema 6.4.6 (Kuratowski)**.** *Un grafo G es plano si y sólo si no tiene un subgrafo homeomorfo a K_5 ni a $K_{3,3}$.*

La prueba del teorema anterior puede encontrarse en [L] o [W].

6.4.2. Solidos platónicos

Para su cumpleaños número cincuenta y dos el Turco recibió una caja de madera con cinco solidos:



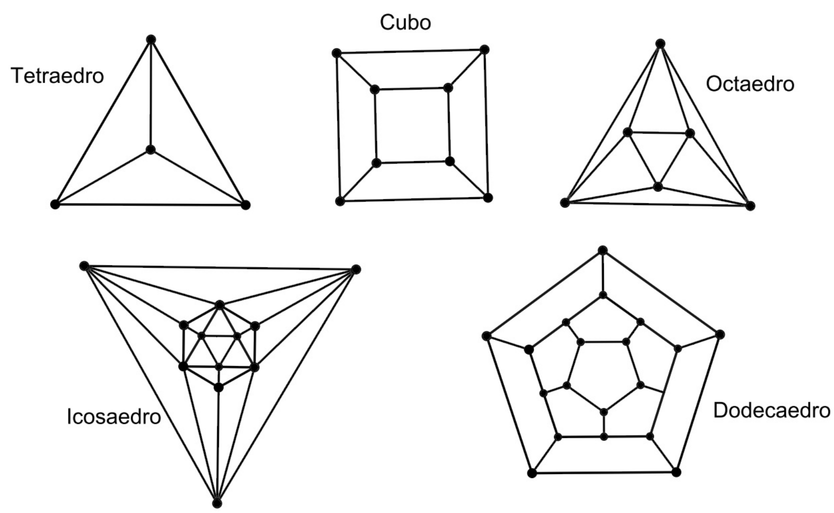
Nunca supo de quién era el regalo, había encontrado la caja sobre la barra al llegar al bar con una tarjeta que decía "Solidos platónicos. Feliz cumpleaños".

Entrenado como estaba en el asunto de los grafos reconoció rápidamente que lo que tenía delante eran cinco grafos esféricos que cumplían dos condiciones:

(i) *Todos los vértices tenían el mismo grado, siendo este mayor o igual a* 3.

(ii) *Todas las regiones tenían el mismo grado. También mayor o igual a* 3.

Supuso (de forma acertada) que estas eran las condiciones que definen a los solidos platónicos. Se preguntó si habría más que cinco solidos como estos. Rápidamente tomó papel y lápiz y se puso a hacer algunas cuentas. También dibujó dichos grafos en el plano:



Más tarde llegó el Comadreja al bar, y al verlo con dificultades para resolver su problema le contó el siguiente teorema:

Teorema 6.4.7. *Existen sólo cinco solidos platónicos.*

En la prueba de este teorema usaremos el siguiente resultado:

Lema 6.4.8. *Sea G un grafo planar conexo sin lazos con $a = a(G) > 2$ (notamos también $v = v(G)$ y $r = r(G)$). Luego*

(1) $3r \leq 2a$

(2) $a \leq 3v - 6$

Demostración. El grado de cada región es al menos tres (porque G no es un multigrafo y no tiene lazos). Observamos que cada arista es borde o bien de dos regiones o bien es dos veces borde de una región, luego

$$2a = \sum_{R \text{ región}} gr(R) \geq 3r.$$

Esto prueba (1).

Por el Teorema 6.4.1 y la parte (1),

$$2 = v - a + r \leq v - a + \frac{2}{3}a = v - \frac{1}{3}a,$$

lo que implica (2). $\square$

Demostración del Teorema 6.4.7. Supongamos que G es un grafo planar que representa a un sólido platónico. Notamos entonces por m al grado de los vértices y por n al grado de las regiones. Ponemos también $v = v(G)$ y $a = a(G)$ y $r = (G)$. Tenemos

$$2a = \sum_{x \in V} gr(x) = mv \text{ y } 2a = \sum_{R \text{ región}} gr(R) = nr. \tag{6.3}$$

Usando la fórmula de la característica de Euler se tiene

$$0 < 2 = v - a + r = \frac{2a}{n} - a + \frac{2a}{m} = a\left(\frac{2m - mn + 2n}{mn}\right). \tag{6.4}$$

Lo que implica $2m - mn + 2n > 0$, que es equivalente a

$$(m-2)(n-2) = mn - 2m - 2n + 4 < 4.$$

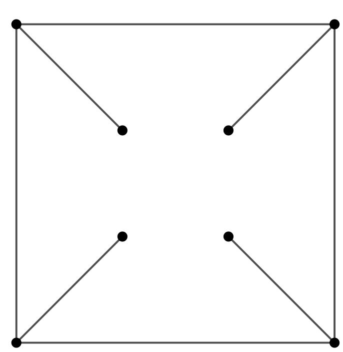
Si sumamos a esto la condición $m, n \geq 3$ tenemos las siguientes soluciones:

- $\underline{m = n = 3}$: Sustituyendo en la ecuación (6.4) tenemos $2 = \frac{a}{3}$ y por lo tanto $a = 6$. Por último las ecuaciones (6.3) nos dan $v = 4$ y $r = 4$. Esto determina que el grafo es completo de cuatro vértices, es decir que el solido es el tetraedro.

- $\underline{m = 3 \text{ y } n = 4}$: Usando nuevamente las ecuaciones (6.3) y (6.4) obtenemos $a = 12$, $v = 8$ y $r = 6$. Para ver que en este caso G es el cubo hagamos algunas observaciones:

  (1) El borde de la región no acotada de G es un cuadrilátero. El resto de las aristas y vértices de G están en el interior de dicho cuadrilátero.

  (2) Como el grado de cada vértice del cuadrilátero en G es 3, entonces el siguiente es un subgrafo de G:



Debemos usar aquí también que no hay regiones triangulares. Observar que ya están representados los ocho vértices de G.

(3) Como cada arista del cuadrilátero está en el borde de dos regiones de grado cuatro, la única forma de agregar las cuatro aristas restantes da como resultado el cubo.

- $\underline{m = 3 \text{ y } n = 5}$: En este caso tenemos $a = 30$, $v = 20$ y $r = 12$. Aquí podemos usar un argumento similar al del caso anterior para ver que G es el dodecaedro. Con los dos casos restantes se puede proceder de la misma manera.
- $\underline{m = 4 \text{ y } n = 3}$: Luego $a = 12$, $v = 6$ y $r = 8$. Lo que determina el octaedro.
- $\underline{m = 5 \text{ y } n = 3}$: Aquí tenemos $e = 30$, $v = 12$ y $r = 20$. Luego G es el icosaedro.

□

6.4.3. Coloración de grafos planares

Consideramos ahora el siguiente problema:

¿Cuántos colores se necesitan para colorear un mapa de forma tal que dos regiones limítrofes tengan colores diferentes?

Observamos que como lo único que importa en el problema es cuándo dos regiones son limítrofes, el problema puede modelarse con un grafo cuyos vértices son las regiones y las adyacencias están dadas por la existencia de una frontera común. Por otro lado, asignar un color a una región puede verse como asignar una etiqueta a un vértice.

Una **coloración** en un grafo sin lazos $G = (V, E)$ es una función $f : V \to \{1, \ldots, k\}$ de forma tal que si $\{x, y\} \in E$, entonces $f(x) \neq f(y)$.

Ejemplo 6.4.9.

1. En el grafo completo K_n los vértices son adyacentes dos a dos, luego se necesitan al menos n colores para colorearlo.
2. Para colorear un grafo bipartito son suficiente dos colores.
3. El ciclo C_n puede colorearse con dos colores si n es par pero se necesitan al menos tres si n es impar.

Observar que el grafo construido a partir de un mapa es necesariamente planar. Luego nuestro problema se puede enunciar de la siguiente manera:

Dado un grafo planar sin lazos $G = (V, E)$, ¿cuál es el mínimo k tal que existe una coloración $f : V \to \{1, \ldots, k\}$ de G?

Daremos la siguiente respuesta parcial a este problema:

Teorema 6.4.10 (Teorema de los cinco colores)**.** *Todo grafo planar (sin lazos) puede colorearse con cinco colores.*

En la prueba del teorema usaremos el siguiente lema:

Lema 6.4.11. *Sea G un grafo planar sin lazos. Entonces existe un vértice de G con grado a lo sumo* 5.

Demostración. Si todos los vértices tienen grado mayor o igual a 6 se tiene, por el Handshaking lemma,

$$2a = \sum_{x \in V} gr(x) \geq 6v,$$

donde a es la cantidad de aristas y v es la cantidad de vértices de G. Por otro lado, por el Lema 6.4.8 tenemos $3v \geq a + 6$. Concluimos entonces que se debe cumplir $2a \geq 2a + 12$, lo que es absurdo. □

Demostración del Teorema 6.4.10. Lo probamos por inducción en la cantidad de vértices n. Para $n = 1$ la afirmación es clara. Suponemos entonces que todo grafo planar con n vértices puede colorearse con 5 colores y tomamos un grafo planar $G = (V, E)$ con $n + 1$ vértices.

Sea x un vértice de G con grado menor o igual a 5 y consideremos G' el grafo que resulta de quitarle a G el vértice x y todas las aristas que inciden en él. Supongamos además que está dada una coloración $f : V \setminus \{x\} \to \{1, \ldots, 5\}$ del grafo G'.

Si $gr(x) < 5$, entonces f puede extenderse a una coloración de G poniendo $f(x)$ diferente a $f(y)$ para todo y adyacente a x.

Si $gr(x) = 5$ llamamos $x_1, \ldots, x_5$ a los vértices adyacentes a x. Podemos además suponer que $f(x_i) = i$ para todo $i = 1, \ldots, 5$ (si dos de estos vértices están coloreados con el mismo color, entonces la coloración se puede extender de forma evidente a x) y que si trazamos el polígono formado por estos vértices, entonces sus índices están ordenados en sentido horario. Tomamos ahora los subgrafos $G_{i,j} \leq G'$ $(i, j = 1, \ldots, 5)$, generados por los vértices coloreados con i y j. A partir de esto estudiamos dos casos:

- Si para un par i, j los vértices x_i y x_j están en componentes conexas distintas de G', entonces puede intercambiarse los colores de los vértices en una de estas dos componentes (el i por el j y viceversa) quedando libre uno de estos colores que pueden asignarse luego a x.

- En el otro caso tomamos un camino simple de x_1 a x_4 en $G_{1,4}$ y de x_3 a x_5 en $G_{3,5}$. Si a este último camino le agregamos las aristas $\{x_5, x\}$ y $\{x, x_3\}$ obtenemos un ciclo cuyo complemento en el plano tiene una componente conexa no acotada que contiene a x_1 y una componente conexa acotada que contiene a x_4.[1] El camino que une x_1 con x_2 debe entonces intersectar dicho ciclo, y como no pasa por x debe hacerlo en un vértice de $G_{3,5}$. Esto es absurdo porque todos los vértices de dicho camino están en $G1, 4$ y estos subgrafos no comparten vértices.

□

El resultado anterior no es óptimo, si lo es el siguiente (que no demostraremos):

Teorema 6.4.12 (Teorema de los cuatro colores)**.** *Todo grafo planar sin lazos puede colorearse con cuatro colores.*

6.5. Apéndice

I. Las definiciones de grafo planar y representación plana dadas en la Sección 6.4 son poco precisas. Para ofrecer una opción más formal consideramos la siguiente alternativa:

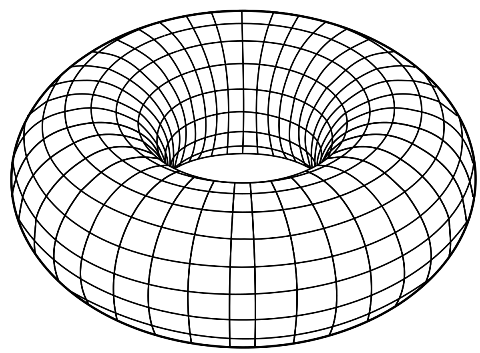
- Una **curva plana** es una función continua $\alpha : [0, 1] \to \mathbb{R}^2$. Esto quiere decir que se escribe $\alpha(t) = (f(t), g(t))$ donde las funciones $f, g : [0, 1] \to \mathbb{R}^2$ son continuas. Diremos en este caso que α **une** $x = \alpha(0)$ con $y = \alpha(1)$.
- Para un par de puntos $x, y \in \mathbb{R}^2$ denotamos por $\mathcal{C}(x, y)$ al conjunto de curvas planas que unen x con y. El conjunto de todas las curvas planas será notado $\mathcal{C}(\mathbb{R}^2)$. Una **representación plana** de un grafo (o multigrafo) $G = (V, E)$ es un par de funciones inyectivas $F : V \to \mathbb{R}^2$ y $H : E \to \mathcal{C}(\mathbb{R}^2)$ tales que:
  - $H(\{x, y\}) \in \mathcal{C}(F(x), F(y))$
  - Si $e \in E$ y $\alpha = H(e)$, entonces $\alpha(t_1) = \alpha(t_2)$ con $t_1 < t_2$ implica $t_1 = 0$ y $t_2 = 1$. (Se eliminan las auto-intersecciones).
  - Si e_1 y e_2 son dos aristas distintas en E y $\alpha_1 = H(e_1)$ y $\alpha_2 = H(e_2)$, entonces $\alpha_1(t_1) = \alpha_2(t_2)$ implica $t_1, t_2 \in \{0, 1\}$. (Se eliminan las intersecciones de aristas distintas que no sean en los extremos.)
- Decimos entonces que el grafo G es **plano** (o **planar**) si admite una representación plana.

II. Ejercicio: El toro es la superficie que se obtiene al rotar el círculo

$$C = \left\{ (x, y, z) \in \mathbb{R}^3 : x = 0,\ (y - 1)^2 + z^2 = \frac{1}{4} \right\} \subset \mathbb{R}^3$$

[1] Aquí se usa el Teorema de la curva de Jordan: una curva simple en el plano divide a este en dos componentes conexas.

alrededor del eje z.



Decimos que un grafo es **tórico** si admite una representación en el toro.

a) Mostrar que $K_{3,3}$ y K_5 son grafos tóricos.

b) Calcular en algunos ejemplos la cantidad $v(G) - a(G) + r(G)$. Conjueturar un enunciado del Teorema de la característica de Euler para el toro.

c) Investigar:

1) Si existen grafos que no sean tóricos.
2) Si dado un grafo cualquiera G, existe una superficie S tal que G admite una representación en S.

III. Pelotas de fútbol

El problema de determinar cuáles son todos los sólidos platónicos es equivalente a este otro: ¿de cuántas formas se puede hacer una pelota de fútbol cosiendo cascos de cuero iguales con forma poligonal?

Ejercicio 6.5.1. Dibujar en el plano el grafo determinado por los cascos hexagonales y pentagonales en una pelota de fútbol clásica. ¿Qué otras pelotas cuyos cascos sean polígonos regulares es posible fabricar?

IV. Ejercicio: Para cada sólido plátonico G determinar cuántos isomorfismos de la forma $f : G \to G$ existen.

Bibliografía

[G] Ralph Grimaldi; *Matemática discreta y combinatoria: Una introducción con aplicaciones.*

[H] Paul Halmos; *Teoría intuitiva de conjuntos.*

[L] Chung Laung Liu; *Introduction to combinatorial mathematics.*

[W] Dougles West; *Introduction to graph theory.*