Lógica y Matemática Discreta

Curso 2023-24

Enrique Ferres López
Área de Ingeniería
Centro Universitario de Tecnología y Arte Digital
enrique.ferres@u-tad.com

Índice general

Agradecimientos **1**

Introducción **3**

1. Lógica **5**

1.1. Introducción 5

1.2. Lógica proposicional 5

1.2.1. Introducción 5

1.2.2. Proposiciones y conectivas 6

1.2.3. Equivalencia, consistencia, tautología y contradicción 9

1.3. Lógica de predicados 11

1.3.1. Introducción 11

1.3.2. Predicados 12

1.4. Álgebra de Boole 14

1.4.1. Introducción 14

1.4.2. Estructuras algebraicas. Álgebras de Boole 15

1.5. Demostraciones 17

1.5.1. Introducción 17

1.5.2. Tipos de demostraciones 17

1.6. Cuestionario 19

2. Conjuntos **23**

2.1. Introducción . . . 23

2.2. Teoría ingenua de conjuntos . . . 23

2.2.1. Introducción . . . 23

2.2.2. Conceptos básicos . . . 24

2.2.3. Más sobre conjuntos . . . 28

2.3. Conjuntos numéricos . . . 37

2.3.1. Introducción . . . 37

2.3.2. Números naturales . . . 37

2.3.3. Números enteros . . . 42

2.3.4. Números racionales . . . 43

2.3.5. Números reales . . . 43

2.4. Bases de numeración . . . 44

2.4.1. Introducción . . . 44

2.4.2. Conceptos básicos . . . 44

2.4.3. El sistema binario. Números no negativos . . . 45

2.4.4. Números negativos. Complemento a dos . . . 48

2.5. Cuestionario . . . 49

3. Combinatoria y Recursividad **51**

3.1. Introducción . . . 51

3.2. Principios básicos del conteo . . . 52

3.2.1. Introducción . . . 52

3.2.2. Reglas de la suma y el producto . . . 52

3.2.3. Principio del palomar . . . 53

3.3. Variaciones, permutaciones y combinaciones . . . 55

3.3.1. Introducción . . . 55

3.3.2. Sin repetición . . . 55
3.3.3. Con repetición . . . 58
3.4. Números combinatorios . . . 62
3.4.1. Introducción . . . 62
3.4.2. El binomio de Newton . . . 62
3.4.3. El Triángulo de Pascal-Tartaglia . . . 65
3.5. Relaciones de recurrencia . . . 66
3.5.1. Introducción . . . 66
3.5.2. Recursividad . . . 66
3.5.3. Relaciones de recurrencia homogéneas . . . 67
3.5.4. Relaciones de recurrencia no homogéneas . . . 70
3.6. Cuestionario . . . 71

4. Relaciones **75**

4.1. Introducción . . . 75
4.2. Relaciones binarias . . . 75
4.2.1. Introducción . . . 75
4.2.2. Conceptos elementales . . . 75
4.2.3. Representaciones de relaciones binarias finitas . . . 76
4.3. Relaciones de equivalencia . . . 78
4.3.1. Introducción . . . 78
4.3.2. Conceptos elementales . . . 79
4.3.3. Relaciones de equivalencia, grafos y particiones . . . 83
4.4. Relaciones de orden . . . 85
4.4.1. Introducción . . . 85
4.4.2. Órdenes parciales y orden total . . . 86
4.4.3. Cotas superiores e inferiores . . . 88

4.4.4. Diagramas de Hasse . . . 90

4.5. Cuestionario . . . 91

5. Aritmética modular **95**

5.1. Introducción . . . 95

5.2. Divisivilidad en los números enteros . . . 95

5.2.1. Introducción . . . 95

5.2.2. Cuestiones fundamentales de aritmética . . . 96

5.3. Relaciones de congruencia . . . 100

5.3.1. Introducción . . . 100

5.3.2. Congruencias . . . 100

5.3.3. Congruencias lineales . . . 102

5.4. Ejercicios . . . 104

6. Grafos **107**

6.1. Introducción . . . 107

6.2. Tipos de grafos . . . 107

6.2.1. Introducción . . . 107

6.2.2. Conceptos básicos. Representación gráfica de grafos . . . 107

6.2.3. Representación matricial de grafos . . . 114

6.3. Más sobre grafos . . . 115

6.3.1. Introducción . . . 115

6.3.2. Aridad . . . 115

6.3.3. Grafos bipartitos . . . 118

6.3.4. Coloración de grafos . . . 119

6.4. Caminos . . . 123

6.4.1. Introducción . . . 123

6.4.2. Caminos, circuitos y ciclos . . . 123
6.4.3. Grafos eulerianos . . . 129
6.4.4. Grafos hamiltonianos . . . 135
6.5. Cuestionario . . . 136

7. Árboles. Algoritmos en grafos **141**

7.1. Introducción . . . 141
7.2. Algoritmos para comprobar la conexión . . . 141
7.2.1. Introducción . . . 141
7.2.2. Árboles . . . 142
7.2.3. Algoritmo DFS . . . 143
7.2.4. Algoritmo BFS . . . 145
7.3. Algoritmos para encontrar el árbol generador mínimo . . . 147
7.3.1. Introducción . . . 147
7.3.2. Conceptos preliminares . . . 147
7.3.3. Algoritmo de Kruskal . . . 148
7.3.4. Algoritmo de Prim . . . 150
7.4. Algoritmo de búsqueda del camino más corto . . . 152
7.4.1. Introducción . . . 152
7.4.2. Algoritmo de Dijkstra . . . 152
7.5. Cuestionario . . . 156

Agradecimientos

Estos apuntes los desarollé como contenido de la asignatura de Lógica y Matemática Discreta del recién nacido grado en Ingeniería del Software Online de U-tad el curso 2022-23. El trabajo durante el verano fue muy intenso y, aunque tuve como base las diapositivas que había preparado el curso anterior, el desarrollo que requiere un curso completo para un estudio a distancia no tiene nada que ver. Como consecuencia de ello, numerosas erratas y errores aparecen a lo largo del texto. Los más flagrantes fueron corregidos durante el curso 22-23, gracias a la revisión del profesor Marino Araque, que también los utilizó, y al cuál le agradezco enormemente su inestimable ayuda. Agradezco de igual manera la detección de errores y erratas a los grupos 1ºA de INSD y 1ºB y 1ºC de INSO, que se mostraron muy atentos y dedicados a la mejora de unos apuntes que servirán a futuros cursos para el estudio de la asignatura. El resto de fallos los detecté yo mismo mientras preparaba las clases. No obstante, esto no quiere decir que el texto se encuentre carente de erratas o fallos, por lo que humildemente solicito al lector que, si encontrase alguno me lo comunique para seguir mejorando los apuntes.

Cuando iba a comenzar el segundo cuatrimestre, decidí ampliar el temario con un tema dedicado en exclusiva a la Aritmética Modular para el grupo de 1º de MAIS. Agradezco también a este grupo y a 1º de FIIS su ayuda y perspicacia en la detección de fallos en el documento.

Finalmente, quiero agradecer a la profesora Mar Angulo su ayuda ofreciéndome su propio material cuando comencé a impartir esta asignatura y realizando importantes sugerencias en el contenido de la misma.

La bibliografía utilizada se halla en la guía de la asignatura, por lo que no he visto necesidad de incluirla en el texto.

Introducción

La Matemática Discreta forma parte de todo primer curso de grados relacionados con la Ingeniería del Software y las Ciencias de la Computación. Esta sirve como aproximación a las matemáticas que subyacen a la informática en sus diferentes aspectos, como las estructuras de datos, el diseño de algoritmos, el *machine learning* o la IA, por poner algunos ejemplos. El estudio de la misma proporcionará un conocimiento más profundo de los distintos campos de especialización así como un mayor rigor en el pensamiento abstracto, esencial en esta disciplina. La palabra *discreta* hace referencia a finitud o, como mucho, numerabilidad. Es decir, la Matemática Discreta es un área de las Matemáticas dedicada al estudio de estructuras matemáticas con una cantidad de elementos no mayor que la de los números naturales.

La asignatura toca temas muy diversos (aunque relacionados todos ellos entre sí), por lo que resulta muy habitual que a un estudiante se le dé muy bien un tema y no tan bien otro. Este es un aspecto que se debe tomar con cautela. Como profesor, es complicado organizar el contenido de la asignatura de manera coherente y cohesionada. Cursos previos me han dado la experiencia necesaria para decidir que la mejor forma de comenzar el curso es con la unidad de Lógica por un motivo principal: las matemáticas requieren de los conocimientos esenciales de la Lógica para resolver problemas, entender teoremas y realizar demostraciones. Además, se necesita saber escribir matemáticas de forma rigurosa para expresar adecuadamente las ideas, y en esta unidad se hace especial énfasis en ello.

A lo largo de las unidades, se proponen una serie de ejemplos y ejercicios con solución. Mi recomendación es que, antes de mirar las soluciones, se intenten resolver para comprobar que de verdad se han comprendido todos los conceptos.

Capítulo 1

Lógica

1.1. Introducción

En este tema estudiaremos dos modelos de Lógica: la lógica proposicional en la sección 2 y la lógica de predicados en la sección 3. La lógica proposicional nos proporcionará las bases del razonamiento matemático, la introducción de las conectivas lógicas y el uso de tablas de verdad para dilucidar si una expresión es cierta o falsa. Además, estudiaremos en qué consiste un lenguaje formal y aprenderemos a traducir afirmaciones del lenguaje natural al lenguaje de la lógica proposicional. La lógica de predicados, o de primer orden, es una extensión de la lógica proposicional en la que se diferencian los sujetos que realizan las acciones. Es más rica expresivamente que la primera, pero también más complicada de trabajar. En lógica de predicados introduciremos los cuantificadores, que nos permiten expresar la cantidad de elementos que satisfacen determinada propiedad.

Dedicamos la sección 4 al álgebra booleana. En esta sección estudiaremos de manera algebraica las operaciones de la lógica proposicional (las conectivas) y aprenderemos a simplificar expresiones y hallar sus resultados en función de los valores de las variables. Del mismo modo, como veremos en la próxima unidad, el álgebra booleana también modeliza las operaciones de la teoría de conjuntos. Es un apartado bastante teórico, pero muy interesante y necesario.

Para finalizar la unidad, daremos unas pinceladas a los tipos más frecuentes de demostraciones que encontramos en Matemáticas en la sección 5.

1.2. Lógica proposicional

1.2.1. Introducción

Por ahora nos vamos a conformar con entender la lógica como una teoría que nos permite simbolizar expresiones de un lenguaje y razonar sobre su veracidad. A modo de ejemplo, podemos razonar sobre afirmaciones de la forma:

(i) Los lunes tengo que ir a trabajar.

(ii) Una función $f : \mathbb{R} \to \mathbb{R}$ derivable es continua.

Hay muchos tipos de lógica en función de su *expresividad* y del nivel sobre el que se trabaja. Lo que distingue a la lógica proposicional es su limitación a cantidades finitas de información y el no distinguir al sujeto en la expresión; no se preocupa por la estructura interna de la misma. La lógica proposicional admite la expresión "el 2 puede escribirse como $2 \cdot 1$" o "el 4 puede escribirse como $2 \cdot 2$". Pero no admite "todo número par puede escribirse como $2k$ para algún número k".

Debemos tener en cuenta que la lógica proposicional es un lenguaje, y todo lenguaje se compone de un alfabeto y una gramática (esto es la sintaxis, nos ayuda a saber qué fórmulas pueden escribirse en nuestro lenguaje) y una semántica (qué fórmulas son ciertas o falsas). A lo largo de esta sección vamos a desarrollar la lógica proposicional exponiendo cada una de estas facetas.

1.2.2. Proposiciones y conectivas

Definición 1.2.2.1. Un alfabeto es el conjunto de símbolos de un lenguaje. En nuestro caso, nuestro alfabeto es

$$\Sigma = \{P_0, P_1, P_2, \ldots, Q_0, Q_1, Q_2, \ldots, R_0, R_1, R_2, \ldots\}$$

Definición 1.2.2.2. Se define una proposición atómica como un elemento de Σ. Una proposición atómica es verdadera o falsa. Las proposiciones compuestas son proposiciones que involucran una o más proposiciones atómicas unidas mediante unas constantes lógicas, llamadas conectivas, que vamos a definir en lo sucesivo. El conjunto de conectivas es

$$C = \{\neg, \wedge, \vee, \to, \leftrightarrow\}$$

Nota 1.2.2.3. Al igual que en las operaciones aritméticas, podríamos establecer una jerarquía entre las distintas conectivas, pero en vez de ello, introduciremos artificialmente los símbolos de paréntesis para indicar la prioridad.

Definición 1.2.2.4. Una tabla de verdad (o veracidad) es una tabla que nos permite definir la semántica de una proposición compuesta a partir de las proposiciones atómicas.

Definición 1.2.2.5. Dada la proposición P, su negación, $\neg P$, es una proposición que se lee "no P". Se define a partir de su tabla de verdad:

P	$\neg P$
V	F
F	V

Definición 1.2.2.6. Dadas las proposiciones P y Q, su conjunción, $P \wedge Q$, es una proposición que se lee "P y Q". Se define a partir de su tabla de verdad:

P	Q	$P \wedge Q$
V	V	V
V	F	F
F	V	F
F	F	F

Definición 1.2.2.7. Dadas las proposiciones P y Q, su disyunción,$P \vee Q$, es una proposición que se lee "P o Q". Se define a partir de su tabla de verdad:

P	Q	$P \vee Q$
V	V	V
V	F	V
F	V	V
F	F	F

Ejemplo 1.2.2.8. La disyunción que hemos definido no es exclusiva. Para definir la disyunción exclusiva, que denotaremos como $\bigoplus$, a través de su tabla de verdad, deberíamos primero remarcar que esta disyunción consiste en que "o bien se da esto, o bien se da lo otro", pero no ambas al mismo tiempo. Es decir, será V si una de las proposiciones es V y la otra es F, y será F en otro caso.

P	Q	$P \bigoplus Q$
V	V	F
V	F	V
F	V	V
F	F	F

Definición 1.2.2.9. Dadas las proposiciones P y Q la implicación, $P \to Q$ (o $P \Rightarrow Q$), es una proposición que se lee "P implica Q" o "si P, entonces Q". A P se le llama hipótesis y a Q, conclusión. Se define a partir de su tabla de verdad:

P	Q	$P \to Q$
V	V	V
V	F	F
F	V	V
F	F	V

Observación 1.2.2.10.

(i) De una hipótesis falsa se puede deducir cualquier cosa: "me pondré un tutú para dar clase cuando los cerdos vuelen". La clave en este punto es tener en cuenta que lo que es V a partir de una hipótesis F es el razonamiento que nos lleva a la conclusión. Veamos un par de ejemplos:

- Si asumimos $0 = 1$ como cierto, entonces, podemos sumar 1 a ambos lados de la igualdad y obtener $1 = 2$. De una hipótesis falsa hemos llegado a una conclusión falsa utilizando un razonamiento correcto.
- De nuevo, asumiendo $0 = 1$, podemos sumar 1 a ambos lados de la igualdad, $0 + 1 = 1 + 1$. Pero como $0 = 1$, puedo transformar el último 1, que suma en el lado derecho de la igualdad, en 0 y tener $0 + 1 = 1 + 0$, es decir, $1 = 1$. De una hipótesis falsa hemos llegado a una conclusión cierta utilizando un razonamiento correcto.

(ii) Si $P \to Q$, se dice que P es **suficiente** para Q y Q es **necesaria** para P.

Definición 1.2.2.11. Sea $P \to Q$ una proposición. Se define su proposición:

(i) Recíproca: $Q \to P$

(ii) Contrarrecíproca: $\neg Q \to \neg P$

(iii) Inversa: $\neg P \to \neg Q$

Definición 1.2.2.12. Dadas las proposiciones P y Q, la doble implicación, $P \leftrightarrow Q$ (o $P \Leftrightarrow Q$), es una proposición que se lee "P si y solo si Q" y significa $P \to Q$ y $Q \to P$, es decir, P es necesaria y suficiente para Q. Se define a partir de su tabla de verdad:

P	Q	$P \leftrightarrow Q$
V	V	V
V	F	F
F	V	F
F	F	V

Ejemplo 1.2.2.13. Construir la tabla de verdad de $(P \vee (\neg P \wedge \neg Q)) \to \neg(Q \vee P)$.

P	Q	$\neg P$	$\neg Q$	$\neg P \wedge \neg Q$	$P \vee (\neg P \wedge \neg Q)$	$Q \vee P$	$\neg(Q \vee P)$	$(P \vee (\neg P \wedge \neg Q)) \to \neg(Q \vee P)$
V	V	F	F	F	V	V	F	F
V	F	F	V	F	V	V	F	F
F	V	V	F	F	F	V	F	V
F	F	V	V	V	V	F	V	V

Observación 1.2.2.14. Si tenemos una expresión $f(P_1, P_2, \ldots, P_n)$ formada por las proposiciones atómicas $P_1, P_2, \ldots, P_n$, la tabla de verdad tendrá 2^n filas, ya que tenemos que contar las distintas posibilidades de repartir los elementos de $\{V, F\}$ entre las n proposiciones.

Para terminar este apartado, veamos en qué consiste traducir afirmaciones en lenguaje natural.

Definición 1.2.2.15. Supongamos que tenemos una afirmación en lenguaje natural que puede ser expresada en lógica proposicional. Se dice que una traducción de esta afirmación es una expresión en lógica proposicional que la modeliza.

Ejemplo 1.2.2.16. A modo de ejemplo, consideremos la afirmación "Si llueve o nieva, el partido se suspende". Para traducirla a lógica proposicional, debemos distinguir las distintas proposiciones y las conectivas que en ella aparecen. Esta es una muestra del proceso que nos lleva a la correcta traducción:

(i) Identificamos las proposiciones: por una parte tenemos "llueve", por otra "nieva" y por otra, "el partido se suspende" (realmente, las identificamos gracias, en parte, a la identificación de las conectivas, que a su vez se identifican gracias a las proposiciones, por lo que no se sigue un proceso plenamente lineal). Por tanto, tenemos las proposiciones

$$P \equiv \text{"llueve"}$$

$$Q \equiv \text{"nieva"}$$

$$R \equiv \text{"el partido se suspende"}$$

(ii) Identificamos las conectivas: por una parte, tenemos "llueve o nieva", así que hay una disyunción. Por otra parte, tenemos un "si... entonces", luego hay una implicación cuya hipótesis es "llueve o nieva" y cuya conclusión es "el partido se suspende".

(iii) Con todos los ingredientes, la traducción es

$$(P \vee Q) \to R$$

Observemos que, si no hubiésemos introducido paréntesis, habría una ambigüedad.

Ejercicio 1.2.2.17. Traducir las siguientes afirmaciones a lógica proposicional y enunciar sus recíprocas, contrarrecíprocas e inversas.

(i) Que los Pistons ganen el campeonato implica que previamente vencieron a los Lakers.

(ii) Es necesario caminar 12 km para llegar a la cima.

1.2.3. Equivalencia, consistencia, tautología y contradicción

Definición 1.2.3.1. Dadas dos proposiciones P y Q, se dice que son equivalentes si tienen las mismas tablas de verdad.

Ejercicio 1.2.3.2.

(i) Comprobar que $P \leftrightarrow Q$ es equivalente a $(P \to Q) \wedge (Q \to P)$.

(ii) Comprobar que $\neg P \vee Q$ es equivalente a $P \to Q$ y a $\neg Q \to \neg P$.

(iii) Comprobar que $P \bigoplus Q$ es equivalente a $(P \wedge \neg Q) \vee (\neg P \wedge Q)$.

Ejemplo 1.2.3.3. Supongamos que tenemos la afirmación "voy al cine **solo si** es el día del espectador". Identificamos las proposiciones

$$P \equiv \text{“voy al cine”}$$

$$Q \equiv \text{“es el día del expectador”}$$

Sin embargo, la conectiva no está clara. En un principio podríamos suponer que "solo si" sería $\leftrightarrow$, pero eso solo se daría si hubiese un "si y solo si". Entonces, ¿qué conectiva utilizamos? La afirmación indica que, solo si se da Q, se tiene entonces P. Luego, si no se da Q, entonces no se tiene P. Esto ya sí sabemos traducirlo a lógica proposicional, sería

$$\neg Q \to \neg P$$

Además, por el ejercicio 1.2.3.2, es equivalente a

$$P \to Q$$

Observación 1.2.3.4. Este es un buen momento para realizar un comentario acerca de las conectivas de la lógica proposicional. Aunque hayamos definido el conjunto de conectivas

$$\{\neg, \wedge, \vee, \to, \leftrightarrow\}$$

en realidad no son necesarias todas ellas para la lógica proposicional, pues algunas pueden definirse en función de otras, es decir, son equivalentes. Esto ya lo hemos visto en el último ejemplo, puesto que se ha demostrado que $\neg P \vee Q$ es lógicamente equivalente a $P \to Q$, luego la implicación es una conectiva redundante si hemos definido la negación y la disyunción. Además,

también hemos probado que $P \leftrightarrow Q$ es equivalente a $(P \to Q) \wedge (Q \to P)$, y como cada implicación se puede transformar en una proposición formada por negaciones y disyunciones, la doble implicación es redundante si están definidas la negación, la disyunción y la conjunción.

Como moraleja podemos concluir que con el conjunto de conectivas $\{\neg, \wedge, \vee\}$ podemos reescribir toda la lógica proposicional. De hecho, solo con $\{\neg, \wedge\}$ o solo con $\{\neg, \vee\}$ nos bastaría.

Nota 1.2.3.5. En ocasiones, cuando una proposición está compuesta por n proposiciones atómicas $P_1, P_2, \ldots, P_n$, conviene escribirla como $f(P_1, P_2, \ldots, P_n)$.

Definición 1.2.3.6. Dada una expresión $f(P_1, P_2, \ldots, P_n)$, cuya tabla de verdad es

P_1	P_2	$\ldots$	P_n	$f(P_1, P_2, \ldots, P_n)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

se dice que es consistente si podemos encontrar una fila cuyos elementos sean todos V.

En la práctica, imponemos que $P_1, P_2, \ldots, P_n$ sean todos V y estudiamos si de esta forma $f(P_1, P_2, \ldots, P_n)$ es V.

Ejercicio 1.2.3.7. ¿Es $[P \vee (\neg P \wedge \neg Q)] \to \neg(Q \vee P)$ consistente?

Definición 1.2.3.8. Un razonamiento, conocido en la antigüedad como silogismo, es la exposición de una serie de premisas, que involucran proposiciones atómicas, de las que se deduce una conclusión. Esquemáticamente, un razonamiento parte de la siguiente estructura:

(P1) $X_1 \equiv f_1(P_1, \ldots, P_n)$

(P2) $X_2 \equiv f_2(P_1, \ldots, P_n)$

$\vdots$

(Pr) $X_r \equiv f_r(P_1, \ldots, P_n)$

(C) $X \equiv f(P_1, \ldots, P_n)$

El razonamiento es la expresión

$$(X_1 \wedge X_2 \wedge \ldots \wedge X_r) \to X$$

Cuando tenemos un razonamiento, nos interesa saber si es consistente.

Ejemplo 1.2.3.9. Analicemos la consistencia del siguiente razonamiento.

- Los salarios no suben si no aumentan los precios.
- Se van a incrementar los salarios y no los precios, a no ser que suban los salarios y simultáneamente se produzca inflación.
- Se producirá inflación.

Lo primero que debemos hacer es traducir cada una de las afirmaciones a lógica proposicional. Llamamos

$$P \equiv \text{“los salarios suben”}$$

$$Q \equiv \text{“aumentan los precios”}$$

$$R \equiv \text{“producirse inflación”}$$

- $\neg Q \to \neg P$
- $(P \wedge \neg Q) \bigoplus (P \wedge R)$
- R

Por tanto, el razonamiento es

$$[(\neg Q \to \neg P) \wedge ((P \wedge \neg Q) \bigoplus (P \wedge R))] \to R$$

Construyendo una tabla como en el ejemplo 1.2.2.13 fijándonos exclusivamente en la fila en la que P, Q y R son V, la columna del razonamiento es V, por lo que es consistente.

Definición 1.2.3.10. Dada una expresión $f(P_1, P_2, \ldots, P_n)$, cuya tabla de verdad es

P_1	P_2	$\ldots$	P_n	$f(P_1, P_2, \ldots, P_n)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

se dice que es una tautología si la columna de $f(P_1, P_2, \ldots, P_n)$ está formada solo por V.

Ejemplo 1.2.3.11. $P \vee \neg P$ es una tautología.

Definición 1.2.3.12. Dada una expresión $f(P_1, P_2, \ldots, P_n)$, cuya tabla de verdad es

P_1	P_2	$\ldots$	P_n	$f(P_1, P_2, \ldots, P_n)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

se dice que es una contradicción si la columna de $f(P_1, P_2, \ldots, P_n)$ está formada solo por F.

Ejemplo 1.2.3.13. $P \wedge \neg P$ es una contradicción.

1.3. Lógica de predicados

1.3.1. Introducción

Ya hemos visto el alcance y las limitaciones de la lógica proposicional. La lógica de predicados, o de primer orden, es más rica expresivamente que la lógica proposicional, pero se requiere la introducción de nuevos conceptos: variables, cuantificadores y predicados. En esta sección nos aproximaremos a la lógica de predicados, pero debemos tener en cuenta que no podremos razonar sobre la veracidad o falsedad de una expresión utilizando tablas. El ejemplo que dimos

en la introducción de la sección previa es paradigmático en este sentido: "todo número par puede escribirse como $2k$ para algún número k". Esta expresión es equivalente a la conjunción $P_0 \wedge P_1 \wedge P_2 \wedge \ldots$ donde:

$$P_0 \equiv 0 \textit{ puede ser escrito como } 2k, \textit{ con } k \textit{ natural}$$

$$P_1 \equiv 2 \textit{ puede ser escrito como } 2k, \textit{ con } k \textit{ natural}$$

$$P_2 \equiv 4 \textit{ puede ser escrito como } 2k, \textit{ con } k \textit{ natural}$$

$$\vdots$$

Sin embargo, construir una tabla de verdad para esta conjunción de infinitos términos sería imposible, ya que necesitaríamos una tabla de tamaño infinito.

1.3.2. Predicados

De manera informal, los predicados en la lógica de predicados juegan el papel de las proposiciones en la lógica proposicional, son las fórmulas de nuestro lenguaje, todo aquello que podemos expresar y razonar sobre su veracidad o falsedad. No obstante, en lógica de predicados, no todo predicado va a ser cierto o falso, pero en este curso no nos preocuparemos demasiado por este hecho.

Definición 1.3.2.1. Una variable es un símbolo que puede tomar cualquier valor de un rango específico de valores, llamado dominio. Las variables, típicamente denotadas x, y, z, $t \ldots$, pueden ser libres, si su introducción en la expresión no depende de otras variables, o ligadas, si su valor depende del valor que tomen otras variables.

Ejemplo 1.3.2.2. En la expresión $y = x + 3$, x es una variable libre e y es una variable ligada.

Definición 1.3.2.3. Un predicado (o propiedad) n-ádico $P(x_1, \ldots, x_n)$ es una expresión que relaciona n variables. Por ejemplo, $P(x, y) \equiv x > y$ es un predicado 2-ádico, también llamado diádico. En términos semánticos, es una función que toma valores de un dominio y devuelve verdadero o falso, es decir, si cada variable x_i pertenece a un dominio D_i, podemos leer el predicado $P(x_1, \ldots, x_n)$ como una función

$$\begin{aligned} P : D_1 \times D_2 \times \cdots \times D_n &\longrightarrow \{F, V\} \\ (x_1, x_2, \ldots, x_n) &\longmapsto P(x_1, \ldots, x_n) \end{aligned}$$

Observación 1.3.2.4. Hay que tener muy en cuenta que un predicado debe tener uno o varios sujetos que realizan la acción y una acción propiamente dicha. Por ejemplo, "la raíz cuadrada de x es positiva" es un predicado, porque tiene un sujeto, la variable x y una acción, que es tomar la raíz cuadrada de x y ver si es positiva. Sin embargo, "la raíz cuadrada de x" no es un predicado, ya que tiene un sujeto pero no hay acción. Siempre se debe comprobar que si instanciamos la variable asignándole un valor, el predicado nos va a devolver verdadero o falso.

Definición 1.3.2.5. Un cuantificador es un símbolo que indica la cantidad de elementos de un dominio que satisfacen un predicado.

- Cuantificador universal: $\forall$.
- Cuantificador existencial: $\exists$.

Ejemplo 1.3.2.6. Supongamos que queremos traducir a lógica de predicados nuestro ejemplo "todo número par puede escribirse como $2k$ para algún número k". El método que vamos a seguir es el siguiente:

(i) Identificar todas las variables y sus dominios.

(ii) Identificar los predicados.

(iii) Identificar los cuantificadores que cuantifican las variables.

(iv) Traducir la afirmación.

En nuestro caso:

(i) Tenemos una variable que es número (par) y número (natural, la k). 2 no es una variable porque es una constante. Además, la primera variable es libre, pero la segunda es ligada, ya que k depende del número par que escojamos.

En cuanto al dominio de la primera variable, podríamos decir que su dominio es el conjunto de números pares $\{n \in \mathbb{N} : n \text{ es par}\}$, pero vamos a dejarlo como el conjunto de números naturales $\mathbb{N}$ y dejaremos la propiedad "ser número par" como predicado. La segunda variable tiene por dominio $\mathbb{N}$. Cuantos menos dominios añadamos y más generales sean, mejor.

(ii) Como ya hemos adelantado, el primer predicado es la propiedad "ser número par". ¿Quién es el número par? La primera variable, x. Lo podemos escribir como

$$P(x) \equiv x \text{ es número par}$$

Observemos que no importa ahora llamarlo x, n o como sea, es una variable muda; una vez escribamos la traducción e introduzcamos las variables con un símbolo, este será el que tengamos que pasar al predicado P como parámetro. El otro predicado es la propiedad "poder escribirse como $2k$". ¿Quién puede escribirse como $2k$? La primera variable, x. Pero en este predicado también está incluida la segunda variable, por lo que será un predicado diádico. Además, "poder escribirse" matemáticamente lo representamos como "es igual a". Así, el predicado es

$$Q(x, y) \equiv x = 2y$$

Como podemos observar, hemos sustituido k por y. Realmente da igual el nombre de variable que utilicemos, como hemos mencionado anteriormente.

(iii) Para los cuantificadores, primero nos fijamos en la variable libre, esta era "cualquier número", por lo que irá cuantificada con un $\forall$. Mientras que la variable ligada era un número que dependía de la primera variable. Como no dice que puede ser cualquier número, pero sí se afirma su existencia, irá cuantificada con un $\exists$.

(iv) Finalmente, la afirmación ya puede ser traducida:

$$\forall n \in \mathbb{N}\, \exists k \in \mathbb{N}\, (P(n) \to Q(n, k))$$

Notemos que ahora hemos utilizado los nombres de variables n y k. La razón es que son los nombres más habituales para números naturales. Para profundizar un poco más en nombres de variables, puede leerse este post https://elescritoriodeenrique.com/inicio/matematicas-basicas/variables/.

Debemos remarcar dos puntos importantes:

- Toda expresión en lógica de predicados comienza cuantificando las variables, e indicando a qué dominio pertenecen, y sigue con los predicados, unidos, si procede, mediante conectivas lógicas.
- $P(n) \to Q(n, k)$ es a su vez un predicado, pero no atómico. Debemos tratar siempre de atomizar al máximo todos los predicados, como hemos hecho en nuestro ejemplo.

Ejercicio 1.3.2.7. Traducir a lógica de predicados las siguientes afirmaciones:

(i) Todos los alumnos de esta clase han estudiado Cálculo.

(ii) Algunos alumnos de esta clase no han visitado Australia.

(iii) Algunos alumnos de esta clase que han estudiado Cálculo no han visitado Australia.

Proposición 1.3.2.8. Dada una expresión del tipo $\forall x \in X\, P(x)$, su negación, $\neg(\forall x \in X\, P(x))$, es $\exists x \in X\, (\neg P(x))$. De igual forma, si tenemos una expresión $\exists x \in X\, P(x)$, su negación, $\neg(\exists x \in X\, P(x))$, es $\forall x \in X\, (\neg P(x))$.

Esto tiene todo el sentido. Si negamos que todos los elementos de un conjunto satisfacen una propiedad, querrá decir que hay al menos un elemento que no la satisface. Y, respectivamente, si negamos que hay algún elemento de un conjunto que satisface una propiedad, querrá decir que ninguno la satisface, es decir, que todos no la satisfacen.

Observación 1.3.2.9. En cuanto a la veracidad o falsedad de una expresión en lógica de primer orden, ya hemos comentado la imposibilidad de recurrir a las tablas de veracidad. En su lugar, debemos recurrir a las demostraciones propias de las matemáticas. Algunas muy sencillas no requieren de conocimientos profundos en la materia, sin embargo, muchas otras quedan fuera del alcance y del propósito de este curso introductorio a las matemáticas de la Ingeniería del Software.

1.4. Álgebra de Boole

1.4.1. Introducción

Vamos a estudiar en esta sección cuál es la estructura subyacente de las operaciones de la lógica proposicional (y también de la teoría de conjuntos, pero esta la veremos en otra unidad). Al fin y al cabo, si tenemos una expresión $f(P, Q)$, semánticamente no deja de ser una función que toma pares de valores *booleanos* (es decir, V o F) y devuelve otro valor booleano. Ya en la observación 1.2.3.4 discutimos la posibilidad de formalizar la lógica proposicional utilizando las conectivas $\{\neg, \wedge, \vee\}$. Aunque se pueden utilizar muchas formas de desarrollar la lógica proposicional, la que, por simplicidad, vamos a modelizar algebraicamente es la que utiliza las conectivas $\{\neg, \wedge, \bigoplus\}$ (recordemos que $\bigoplus$ era la disyunción exclusiva definida en el ejemplo 1.2.2.8). Esta va a ser la estructura que modelizaremos de manera algebraica en esta sección.

1.4.2. Estructuras algebraicas. Álgebras de Boole

Definición 1.4.2.1. A un conjunto X sobre el que están definidas una serie de operaciones que satisfacen una serie de propiedades se le conoce como estructura algebraica.

Ejemplo 1.4.2.2. Pensemos en el conjunto de números naturales, $\mathbb{N}$. Sobre este conjunto están definidas, por ejemplo, la suma y el producto. Además, estas satisfacen una serie de propiedades, como la asociativa o la distributiva. Pero no solo los conjuntos numéricos son estructuras algebraicas. Por ejemplo, un cuadrado en el plano es un conjunto. Si definimos sobre él las operaciones rotación de 90 grados alrededor de su centro y reflexión sobre la recta paralela a dos de sus lados que pasa por su centro, esto también es una estructura algebraica, aunque excede el alcance de este curso.

Aunque hay algunas estructuras algebraicas muy interesantes, como los grupos y los anillos, vamos a centrar nuestro interés en las álgebras; más en concreto, las álgebras de Boole.

Definición 1.4.2.3. Sea X un conjunto sobre el que están definidas dos operaciones binarias (es decir, que operan dos elementos), $+$ y $\cdot$, llamadas suma y producto (generalmente escribiremos xy en lugar de $x \cdot y$), y una operación unaria (es decir, que opera un solo elemento), $^-$, llamada complemento. Se dice que $(X, +, \cdot, ^-)$ es un álgebra de Boole si satisface las siguientes propiedades:

(i) **Asociatividad de la suma:** $x + (y + z) = (x + y) + z$, $\forall x, y, z \in X$.

(ii) **Conmutatividad de la suma:** $x + y = y + x$, $\forall x, y \in X$.

(iii) **Existencia del elemento neutro para la suma:** existe un único elemento llamado $0 \in X$ tal que $x + 0 = 0 + x = x$, $\forall x \in X$.

(iv) **Distributividad de la suma respecto del producto:** $x(y + z) = xy + xz$, $(x + y)z = xz + yz$, $\forall x, y, z \in X$.

(v) **Existencia del elemento complementario para la suma:** $\forall x \in X$, existe un único elemento, $\bar{x} \in X$, tal que $x + \bar{x} = \bar{x} + x = 1$.

(vi) **Asociatividad del producto:** $x(yz) = (xy)z$, $\forall x, y, z \in X$.

(vii) **Conmutatividad del producto:** $xy = yx$, $\forall x, y \in X$.

(viii) **Existencia del elemento unitario para el producto:** existe un único elemento llamado $1 \in X$ tal que $1x = x1 = x$, $\forall x \in X$.

(ix) **Existencia del elemento complementario para el producto:** $\forall x \in X$, existe un único elemento, $\bar{x} \in X$, tal que $x\bar{x} = \bar{x}x = 0$.

Proposición 1.4.2.4. Sea $(X, +, \cdot, \bar{x})$ un álgebra de Boole. Entonces, se satisfacen las siguientes propiedades:

(i) **Idempotencia para el producto:** $xx = x$, $\forall x \in X$.

(ii) **Absorción para el producto:** $0x = x0 = 0$, $\forall x \in X$.

(iii) **Involución:** $\bar{\bar{x}} = x$, $\forall x \in X$.

Hasta ahora hemos visto la estructura de álgebra de Boole, pero todavía no hemos visto ningún conjunto ni ningunas operaciones que tengan dicha estructura. Como hemos adelantado al comienzo de esta sección, pretendemos modelizar la semántica de lógica proposicional con las conectivas $\{\neg, \wedge, \bigoplus\}$. Como una proposición puede ser V o F, el conjunto será $X = \{F, V\}$ o, de forma más rigurosa, $X = \{0, 1\}$.

(i) La operación suma la vamos a definir de la misma forma que la disyunción exclusiva:

$+$	0	1
0	0	1
1	1	0

(ii) La operación producto la vamos a definir de la misma forma que la conjunción:

$\cdot$	0	1
0	0	0
1	0	1

(iii) La operación complemento la vamos a definir de la misma forma que la negación:

$$\bar{x} = \begin{cases} 1 & \text{si } x = 0 \\ 0 & \text{si } x = 1 \end{cases}$$

De este modo, se puede comprobar que $(\{0, 1\}, +, \cdot, \bar{})$, tal y como hemos definido las operaciones, satisface las propiedades de álgebra de Boole.

Para terminar, veamos un par de ejemplos típicos de los ejercicios que nos podemos encontrar en esta sección.

Ejemplo 1.4.2.5. Simplifiquemos la expresión

$$x + y(x + y) + x(y + \bar{x})$$

Para ello, debemos aplicar todas las propiedades que hemos visto a lo largo de la sección para álgebras de Boole. Por una parte, $y(x + y) = yx + yy$, y por otra, $x(y + \bar{x}) = xy + x\bar{x}$. Así, llevamos

$$x + y(x + y) + x(y + \bar{x}) = x + yx + yy + xy + x\bar{x}$$

Ahora, aplicamos la conmutatividad de la suma y el producto para agrupar xy e yx. Por otra parte, por idempotencia, $yy = y$. También sabemos que x y $\bar{x}$ son elementos diferentes, uno es 0 y el otro es 1 (da igual cuál sea cuál), y que el producto de 0 y 1 es siempre 0. De esta forma,

$$x + y(x + y) + x(y + \bar{x}) = x + yx + yy + xy + x\bar{x} = x + (xy + xy) + y + 0 = x + (xy + xy) + y$$

Para terminar, xy será 0 o 1, pero al sumar 0 y 0 o 1 y 1, el resultado es siempre 0. Por tanto,

$$x + y(x + y) + x(y + \bar{x}) = x + (xy + xy) + y = x + 0 + y = x + y$$

Ejercicio 1.4.2.6. Determinar la tabla de valores de la expresión

$$F(x, y, z) = x(yz + \bar{y}\bar{z})$$

1.5. Demostraciones

1.5.1. Introducción

En esta sección estudiaremos brevemente algunos de los tipos más comunes de demostraciones en Matemáticas, salvo las demostraciones por inducción que serán estudiadas en la próxima unidad. El propósito de esta sección no es enseñar a demostrar, pues cada problema requiere de diversas técnicas para ser abordado. Simplemente nos limitaremos a ver, a grandes rasgos en qué consisten estas técnicas de demostración. Es importante señalar que, con frecuencia, demostrar un resultado requiere combinar distintos tipos de demostración.

1.5.2. Tipos de demostraciones

Demostración directa

En el tipo de demostración conocido como demostración directa (hacia adelante) se trata de demostrar que $A \Rightarrow B$ partiendo de A y deduciendo proposiciones hasta llegar a B.

Ejemplo 1.5.2.1. Demostrar que el cubo de un número impar es, a su vez, impar.

Demostración. Sea $n = 2k + 1$ un número impar. Entonces,

$$n^3 = (2k+1)^3 = 8k^3 + 12k^2 + 6k + 1 = 2(4k^3 + 6k^2 + 3k) + 1$$

por lo que n^3 es impar. □

Demostración marcha atrás

Una estrategia para encontrar una demostración directa consiste en proceder marcha atrás, más o menos como sigue. Como antes, queremos probar que $A \Rightarrow B$. Nos preguntamos (siempre con un ojo en A) qué proposiciones implican B. Encontramos que $P \Rightarrow B$; no es lo que buscamos, pero tal vez P está más cerca de A. Nos preguntamos a continuación cómo podríamos llegar a P. Encontramos que $Q \Rightarrow P$. Tal vez ahora ya somos capaces de ver que $A \Rightarrow Q$. Si fuera así, ahora ya podríamos construir la demostración directa

$$A \Rightarrow Q \Rightarrow P \Rightarrow B$$

Ejemplo 1.5.2.2. Demostrar que $x + \frac{1}{x} \geq 2$ si $x > 0$.

Demostración. Podemos ver si

$$\frac{x^2}{x} + \frac{1}{x} \geq 2,\ x > 0$$

Como aún no sabemos si es cierto, podemos ver si

$$x^2 + 1 \geq 2x,\ x > 0$$

Si todavía no está claro, podríamos ver si

$$x^2 - 2x + 1 \geq 0,\ x > 0$$

Ahora ya sí podemos construir una demostración directa, pues

$$x^2 - 2x + 1 = (x-1)^2 \geq 0$$

□

Demostración por contraposición

En ocasiones, para conseguir demostrar la proposición $A \Rightarrow B$, resulta más sencillo demostrar la proposición $\neg B \Rightarrow \neg A$.

Ejemplo 1.5.2.3. Sea $a \in \mathbb{R}$ irracional. Demostrar que $7a$ también es irracional.

Demostración. Veamos que si $7a \in \mathbb{Q}$, entonces $a \in \mathbb{Q}$. Para ello, si $7a \in \mathbb{Q}$, se tiene que $\exists n,\ m \in \mathbb{Z},\ m \neq 0$, tales que

$$7a = \frac{n}{m}$$

luego

$$a = \frac{n}{7m} \in \mathbb{Q}$$

□

Demostración por reducción al absurdo

Otra forma de demostración muy utilizada es la conocida como demostración por reducción al absurdo: Quieres demostrar que $A \Rightarrow B$ y para ello demuestras que $(A \wedge \neg B) \Rightarrow (P \wedge \neg P)$, para cierta proposición P.

Ejemplo 1.5.2.4. Demostrar que $\sqrt{2}$ es irracional.

Demostración. Supongamos que $\sqrt{2}$ es racional y que podemos escribirlo como una fracción irreducible

$$\sqrt{2} = \frac{n}{m}$$

donde n y m son primos entre sí. Elevando al cuadrado ambos miembros de la igualdad tenemos que

$$2 = \frac{n^2}{m^2}$$

Por tanto,

$$2m^2 = n^2$$

Así, n^2 es un número par y, de este modo, n es par (como ejercicio, ¿por qué?). Pero si n es par y es primo con m, entonces m es impar, pues de lo contrario, ambos serían divisibles por 2. Escribimos $n = 2k$. Por tanto,

$$n^2 = (2k)^2 = 4k^2$$

Sustituyéndolo en el razonamiento que estamos siguiendo, tenemos que

$$2m^2 = n^2 = 4k^2$$

Si dividimos por 2 en ambos lados, tenemos que

$$m^2 = 2k^2$$

De aquí deducimos que m^2 es par. Pero, de nuevo, m tiene que ser par!! Por consiguiente, $\sqrt{2}$ es irracional. □

1.6. Cuestionario

Ejercicio 1. La tabla de verdad de $P \to (\neg Q \vee (P \leftrightarrow Q))$ para P falso y Q falso es:

(a) V.

(b) F.

Ejercicio 2. ¿Cuál es la traducción correcta de la afirmación "Solo si copio en el examen, o el profesor se porta bien, aprobaré Historia del Arte"? Ten en cuenta que

$$P \equiv \text{“copio en el examen”}$$

$$Q \equiv \text{“el profesor se porta bien”}$$

$$R \equiv \text{“aprobaré Historia del Arte”}$$

(a) $(R \to P) \vee Q$

(b) $R \to (P \vee Q)$

(c) $(P \vee Q) \to R$

(d) $R \leftrightarrow (P \vee Q)$

Ejercicio 3. ¿Qué expresión es equivalente a $\neg(P \vee Q)$?

(a) $\neg(P \wedge Q)$

(b) $\neg P \vee \neg Q$

(c) $\neg P \wedge \neg Q$

(d) $P \wedge Q$

Ejercicio 4. Decidir si el siguiente razonamiento es consistente o no:

- Si mi abuela me da 10 euros y no me pide que compre pan, compraré golosinas.
- Mi abuela me ha pedido que compre el pan, pero no me ha dado 10 euros.
- Voy a comprar golosinas y el pan.

(a) Consistente.

(b) No consistente.

Ejercicio 5. Decidir si la proposición $(\neg P \vee \neg Q) \leftrightarrow \neg(P \wedge Q)$ es una tautología o no.

(a) Tautología.

(b) No tautología.

Ejercicio 6. Decidir si la proposición $(P \vee Q) \leftrightarrow \neg(P \wedge Q)$ es una contradicción o no.

(a) Contradicción.

(b) No contradicción.

Ejercicio 7. ¿Cual es la traducción de la afirmación "quien a buen árbol se arrima, buena sombra le cobija"?

(a) $\forall x\, \exists y\, \exists z(P(x,\, y) \rightarrow Q(x,\, z))$

(b) $\forall x\, \exists y\, \exists z(P(x,\, y) \wedge Q(x,\, z))$

(a) $\exists x\, \exists y\, \forall z(P(x,\, z) \wedge Q(y,\, z))$

(d) $\exists x\, \exists y\, \forall z(P(x,\, z) \rightarrow Q(y,\, z))$

Ejercicio 8. ¿Con qué expresión se corresponde $\neg(\forall x\, (P(x) \rightarrow Q(x))$?

(a) $\exists x\, (P(x) \wedge \neg Q(x))$

(b) $\forall x\, \neg(P(x) \rightarrow Q(x))$

(c) $\exists x\, \neg(P(x) \rightarrow Q(x))$

(d) $\forall x\, (P(x) \wedge \neg Q(x))$

Ejercicio 9. La expresión $x(\bar{y} + x) + \bar{y}(x + y)$ es igual a:

(a) $x\bar{y}$

(b) $x + y$

(c) x

(d) 0

Ejercicio 10. Asumiendo que estas dos afirmaciones son ciertas:

- Pinocho siempre miente
- Pinocho dice "todos mis sombreros son verdes"

¿Qué información podemos concluir?

(a) Pinocho tiene al menos un sombrero

(b) Pinocho tiene un único sombrero verde

(c) Pinocho no tiene sombreros

(d) Pinocho no tiene sombreros verdes

Capítulo 2

Conjuntos

2.1. Introducción

La Teoría de Conjuntos es, junto a la Lógica, la piedra fundamental de las Matemáticas. La mayoría de conceptos matemáticos que cualquier persona que no se especialice en Matemáticas se va a encontrar a lo largo de su vida, están definidos mediante conjuntos.

Como toda rama de las matemáticas, la Teoría de Conjuntos está fundamentada en una serie de axiomas (proposición asumida como cierta de la cual se pueden deducir resultados mediante pasos lógicos) que, en su mayoría, nos indican qué objetos son conjuntos y cómo obtener otros conjuntos a partir de estos. Esta axiomática recibe el nombre de Zermelo-Fraenkel, o ZF. Sin embargo, el propósito de esta unidad no es presentar la axiomática ZF, sino mostrar los conceptos más básicos sobre conjuntos. A esto es a lo que llamamos teoría *ingenua* de conjuntos y dedicaremos la primera sección a estudiarla.

En Matemáticas, y en particular en Matemática Discreta, cobran especial importancia los distintos conjuntos numéricos, sobre todo los números naturales. En la segunda sección trataremos este tema, veremos cómo se define el concepto de número y estudiaremos sus propiedades fundamentales.

Para terminar la unidad, veremos qué significa un número expresado en distintas bases de numeración, centrándonos en el sistema binario, y aprenderemos a operar números en este sistema.

2.2. Teoría ingenua de conjuntos

2.2.1. Introducción

Dentro de la lógica de predicados, un conjunto no tiene una definición matemática precisa; todo intento por definir conjunto hará referencia a "colección de objetos o elementos". Se puede decir que los conjuntos son un concepto primitivo, y nos limitaremos a hablar de ellos con nuestra idea intuitiva de lo que es un conjunto. La formalización de la Teoría de Conjuntos llegó a finales del siglo XIX, debido a la necesidad de fundamentar las Matemáticas sobre unos cimientos lógicos y

estructurales robustos (axiomas y conjuntos), y eliminar paradojas que aparecían en las propias bases, como la paradoja de Russell, a la cuál nos referiremos más tarde. Los primeros intentos de formalización son los que veremos en lo sucesivo.

En lo que sigue de curso, deberemos tener en cuenta que en Matemáticas, si bien el lenguaje es riguroso, se realizan ligeras concesiones con respecto a la Lógica para agilizar o simplificar la lectura de las mismas. Así, por ejemplo, si queremos utilizar un símbolo para la implicación, utilizaremos $\Rightarrow$ en lugar de $\rightarrow$. Lo mismo aplica para la doble implicación. La conjunción y la disyunción frecuentemente se escriben de palabra en lugar de utilizando los símbolos de conectiva, y el símbolo de negación raramente es utilizado. Por otra parte, los predicados de la forma

$$\exists x \in X \, P(x)$$

se escriben

$$\exists x \in X \text{ tal que } P(x)$$

En general, todas estas adaptaciones mezclan símbolos y palabras para facilitar la comprensión. Yo siempre digo que la notación debe estar al servicio de las Matemáticas y no al revés. Pero no se debe dejar de lado el rigor y, en todo momento, hay que recordar que la escritura es transmisión de información; una mala sintaxis podría cambiar por completo el significado de un predicado.

2.2.2. Conceptos básicos

Definición 2.2.2.1. Si x es un elemento que pertenece a un conjunto X se denota $x \in X$, mientras que si no pertenece al conjunto, se denota $x \notin X$.

Observación 2.2.2.2. Un conjunto puede ser elemento de otro conjunto.

Un conjunto queda completamente caracterizado por sus elementos. Por ello, para especificar un conjunto tenemos dos formas de hacerlo:

Definición 2.2.2.3. Si X está formado por los elementos x_1, x_2, x_3 podemos escribirlo como

$$X = \{x_1, x_2, x_3\}$$

A esta forma de expresar X se la conoce como definición por extensión, es decir, se explicitan todos sus elementos.

Observación 2.2.2.4. Si queremos definir un conjunto por extensión y posee una *gran* cantidad de elementos, podemos emplear puntos suspensivos a partir de cierto elemento si estos tienen un patrón fácilmente identificable. Por ejemplo, podemos definir por extensión los números naturales como

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

Observación 2.2.2.5.

(i) $\{a\} = \{a, a\}$. Es decir, un conjunto no tiene elementos repetidos.

(ii) $\{a, b\} = \{b, a\}$. Es decir, un conjunto no distingue primer elemento de segundo elemento.

Definición 2.2.2.6. Sea X un conjunto. Se dice que está definido por compresión si existe una propiedad P que satisfacen exactamente todos sus elementos. En este caso, el conjunto se escribe

$$X = \{x \,:\, P(x)\}$$

Aunque también puede escribirse con una línea vertical | en vez de los dos puntos. Se lee "el conjunto formado por todos los elementos x tales que satisfacen $P(x)$."

Ejemplo 2.2.2.7. Supongamos que queremos definir por compresión el conjunto X de todos los números naturales pares. La propiedad de ser número par la podemos expresar como

$$P(x) \equiv \exists k \in \mathbb{N} \text{ tal que } x = 2k$$

Así,

$$X = \{n \in \mathbb{N} \,:\, \exists k \in \mathbb{N} \text{ tal que } n = 2k\}$$

Observación 2.2.2.8. A finales del siglo XIX, Bertrand Russell descubrió que las definiciones por compresión podían llevar a paradojas. Primero veámosla de forma narrada como el Problema del Barbero y luego de forma matemática.

En un pueblo, un barbero afeita a todos los hombres que no se afeitan a sí mismos. ¿Quién afeita al barbero? Si no se afeitase a sí mismo, por definición debería afeitarse a sí mismo, mientras que si se afeitase a sí mismo, por definición no podría hacerlo.

En su forma matemática, tenemos que recordar que, por la observación 2.2.2.2, un conjunto puede ser elemento de otro. Si definimos la propiedad $P(x) \equiv x \notin x$, y definimos por compresión

$$R = \{x \,:\, x \notin x\}$$

este es el conjunto de todos los conjuntos que no se pertenecen a sí mismos (análogo al problema anterior). En este caso, la pregunta es si $R \in R$.

Como podemos imaginar, si en las bases de las Matemáticas aparecen paradojas, no podríamos garantizar que lo que se deduce de ellas sea correcto, pues ya sabemos que falso implica cualquier cosa. Por ello, la axiomática ZF vino a solucionar paradojas como la de Russell.

Ejemplo 2.2.2.9. Expresar por extensión los siguientes conjuntos:

(i) El conjunto formado por todos los reales cuyo cuadrado es igual a 1.

(ii) El conjunto formado por todos los cuadrados perfectos menores que 100.

(i) Los únicos números reales cuyo cuadrado es 1 son 1 y -1. Por tanto, el conjunto es $\{-1, 1\}$.

(ii) Los cuadrados perfectos son números naturales resultado de elevar un natural al cuadrado. Así, el conjunto es $\{0, 1, 4, 9, 16, 25, 36, 49, 64, 81\}$.

Ejemplo 2.2.2.10. Expresar por compresión el conjunto formado por todos los cuadrados perfectos.

La definición de cuadrado perfecto que hemos dado en el ejemplo anterior se puede escribir como: n es cuadrado perfecto si $\exists k \in \mathbb{N}$ tal que $n = k^2$. Por tanto, el conjunto que buscamos es $\{n \in \mathbb{N} \,:\, \exists k \in \mathbb{N} \text{ tal que } n = k^2\}$.

La siguiente definición parece una obviedad, pero es la primera piedra sobre la que se construyen otros conjuntos.

Definición 2.2.2.11. Existe el conjunto sin elementos, llamado conjunto vacío y denotado $\emptyset$.

Definición 2.2.2.12. Llamamos conjunto universal, o universo, U al conjunto con más elementos en un determinado contexto.

Observación 2.2.2.13. Generalmente, cuando estemos en un problema, haremos referencia a que se está planteando dentro de un universo o conjunto universal, sin especificar este conjunto. Por ello, no es un concepto común a todos los conjuntos, sino que depende de cada problema. Más adelante veremos aplicaciones de este concepto.

Definición 2.2.2.14. Sea X un conjunto. Se llama cardinal de X a la cantidad de elementos que posee, y se denota $|X|$. En la literatura también podemos encontrarnos la notación $\#X$.

Si $|X| < \infty$, se dice que el conjunto es finito; en otro caso se dice que es infinito.

Ejemplo 2.2.2.15. Sea el conjunto

$$X = \{n \in \mathbb{N} : \exists k \in \mathbb{N} \text{ tal que } n = 5k \text{ y } 3 \leq n < 100\}$$

Este es el conjunto de los múltiplos de 5 mayores o iguales que 3 y menores que 100, es decir, múltiplos de 5 entre 5 y 95. Por tanto, $|X| = 19$.

Observación 2.2.2.16. No existe un único infinito en conjuntos. Por ejemplo, hay infinitos números naturales e infinitos números reales, pero $|\mathbb{N}| < |\mathbb{R}|$. No entraremos en el porqué de la siguiente cadena de desigualdades, pero está bien conocerla:

$$|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| < |\mathbb{I}| = |\mathbb{R}|$$

Definición 2.2.2.17. Sean A y B dos conjuntos. Se dice que A es subconjunto de B si para todo $a \in A$, se tiene que $a \in B$. Se denota $A \subseteq B$.

De hecho, esta definición nos lleva a la siguiente proposición que nos permite saber cuándo dos conjuntos son iguales y que utilizaremos en la siguiente subsección cuando veamos las operaciones entre conjuntos.

Proposición 2.2.2.18. Sean A y B dos conjuntos. Entonces,

$$A = B \Leftrightarrow A \subseteq B \text{ y } B \subseteq A$$

Ejemplo 2.2.2.19. Sea $X = \{0, 1, 2, 3, 4, 5\}$. Entonces, el conjunto $\{0, 2, 3\}$ es subconjunto de X. El conjunto $\{0, 6\}$ no es subconjunto de X, ya que $6 \notin X$.

La observación 2.2.2.2 nos indicaba que había conjuntos que podían ser elementos de otros conjuntos. La definición de subconjunto no tiene nada que ver, pero puede confundir. El próximo ejercicio nos ayudará a diferenciar los conceptos de pertenencia y de inclusión.

Ejercicio 2.2.2.20. Sea $X = \{0, 1, 2, \{0, 1\}, \{2\}\}$. Determinar si, con respecto de X, los siguientes elementos son subconjunto, elemento, ambos o ninguno:

(i) 0

(ii) $\{0, 1\}$

(iii) $\{0, \{2\}\}$

(iv) $\{2\}$

(v) $\{\{0, 1, 2\}\}$

(vi) $\{\{0, 1\}, \{2\}\}$

(vii) $\{0, 1, 2\}$

(viii) 2

Proposición 2.2.2.21. Sea X un conjunto. Entonces:

(i) $\emptyset \subseteq X$.

(ii) $X \subseteq X$.

Definición 2.2.2.22. Sea X un conjunto. Se define el conjunto *partes* de X, y se denota $\mathcal{P}(X)$, como aquel formado por todos los subconjuntos de X. Es decir,

$$\mathcal{P}(X) = \{A \subseteq X\}$$

Ejemplo 2.2.2.23. Sea $X = \{a, b, c\}$. Entonces,

$$\mathcal{P}(X) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, X\}$$

Proposición 2.2.2.24. Sea X un conjunto. Entonces, $|\mathcal{P}(X)| = 2^{|X|}$.

Ejemplo 2.2.2.25. En el ejemplo anterior, $|X| = 3$ y $|\mathcal{P}(X)| = 8 = 2^3$.

Veamos una forma interesante de representar subconjuntos de un conjunto finito cualquiera a partir de 0's y 1's.

Definición 2.2.2.26. Sea $U = \{x_1, x_2, \ldots, x_n\}$ un conjunto finito, y sea $X \subseteq U$. La tira de bits que representa a X, como subconjunto de U, es una cadena (o string) formada por 0's y 1's de la forma $b_1 b_2 \cdots b_n$ tal que, para todo $i \in \{1, 2, \ldots, n\}$,

$$b_i = \begin{cases} 1 & x_i \in X \\ 0 & x_i \notin X \end{cases}$$

Es decir, será una cadena de longitud $|U|$ con un 1 en la posición del elemento x_i si está en X y un 0 si no está.

Ejemplo 2.2.2.27. Sea

$$U = \{n \in \mathbb{N} : n < 10\}$$

y sea

$$X = \{n \in U : n = 2k + 1, 0 \leq k \leq 4\}$$

Si queremos representar X mediante tiras de bits, primero debemos saber quiénes son estos dos conjuntos. U es el conjunto formado por los números del 0 al 9, mientras que X es el conjunto formado por todos los números impares entre $2 \cdot 0 + 1$ y $2 \cdot 4 + 1$, es decir, entre 1 y 9. Por tanto,

$$U = \{0, 1, 2, \ldots, 9\}$$

y

$$X = \{1, 3, \ldots, 9\}$$

La tira de bits que representa a X es $b_0 b_1 \cdots b_9 = 0101010101$.

2.2.3. Más sobre conjuntos

Hasta ahora hemos estado estudiando definiciones y propiedades sobre conjuntos sin preocuparnos sobre cómo generar más conjuntos a partir de los existentes. Ahora vamos a centrarnos en las operaciones que se pueden realizar sobre conjuntos, las clásicas unión, intersección, diferencia, diferencia simétrica, complementario y producto cartesiano. En lo que sigue, supondremos que todos los conjuntos están dentro de un universo U.

Definición 2.2.3.1. Sean X e Y dos conjuntos. Se define la unión de X e Y, y se denota $X \cup Y$ como

$$X \cup Y = \{x \in U \,:\, x \in X \text{ o } x \in Y\}$$

Es decir, es el conjunto formado por todos los elementos de X e Y.

Observación 2.2.3.2. Cuando queremos realizar la unión de, digamos, n conjuntos, en lugar de escribirla como

$$X_1 \cup X_2 \cup \cdots \cup X_n$$

podemos escribirla como

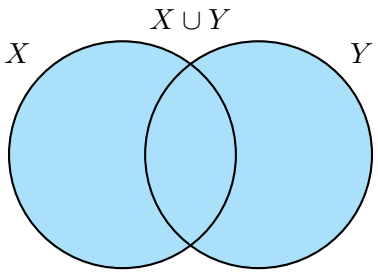
$$\bigcup_{i=1}^{n} X_i$$

Ejemplo 2.2.3.3. Sean $X = \{a, b, d\}$ e $Y = \{a, c, e\}$. Entonces,

$$X \cup Y = \{a, b, c, d, e\}$$

Observación 2.2.3.4. Cuando trabajamos con conjuntos y operamos con ellos, para hacernos una idea gráfica de lo que está sucediendo podemos recurrir a los diagramas de Venn, que representan de manera abstracta a cada uno de los conjuntos involucrados.

En el caso de $X \cup Y$, el diagrama de Venn tiene la siguiente forma:



Proposición 2.2.3.5. Sean X, Y, $Z \subseteq U$. Entonces:

(i) $X \cup Y = Y \cup X$

(ii) $(X \cup Y) \cup Z = X \cup (Y \cup Z)$

(iii) $X \subseteq Z$ e $Y \subseteq Z$ si y solo si $X \cup Y \subseteq Z$

(iv) $X \subseteq Y$ y $X \subseteq Z$ si y solo si $X \subseteq Y \cup Z$

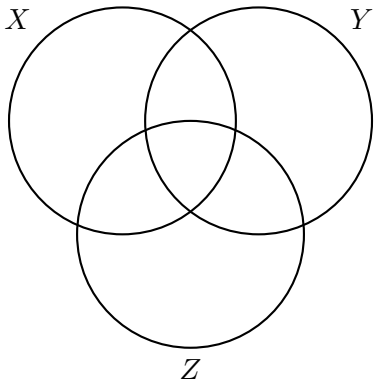
(v) $X \subseteq Y$ si y solo si $X \cup Y = Y$

(vi) $X \cup U = U$

(vii) $X \cup X = X$

(viii) $X \cup \emptyset = X$

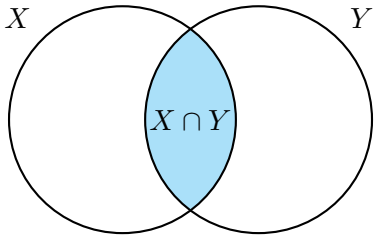
Observación 2.2.3.6. Las propiedades que acabamos de enunciar son muy intuitivas y no requieren mucho esfuerzo visualizarlas, pero en general, cuando queremos representar mediante un diagrama de Venn un problema en el que aparecen involucrados tres conjuntos, la forma de dibujarlos es la siguiente:



Definición 2.2.3.7. Sean X e Y dos conjuntos. Se define la intersección de X e Y, y se denota $X \cap Y$, como

$$X \cap Y = \{x \in U \,:\, x \in X \text{ y } x \in Y\}$$

Es decir, es el conjunto formado por todos los elementos que están tanto en X como en Y. El diagrama de Venn es el siguiente:



Observación 2.2.3.8. Cuando queremos realizar la intersección de, digamos, n conjuntos, en lugar de escribirla como

$$X_1 \cap X_2 \cap \cdots \cap X_n$$

podemos escribirla como

$$\bigcap_{i=1}^{n} X_i$$

Ejemplo 2.2.3.9. Sean $X = \{a, b, d\}$ e $Y = \{a, c, e\}$. Entonces,

$$X \cap Y = \{a\}$$

Definición 2.2.3.10. Se dice que dos conjuntos, X e Y, son disjuntos si $X \cap Y = \emptyset$.

Proposición 2.2.3.11. Sean X, Y, $Z \subseteq U$. Entonces:

(i) $X \cap Y = Y \cap X$

(ii) $(X \cap Y) \cap Z = X \cap (Y \cap Z)$

(iii) $X \subseteq Y$ si y solo si $X \cap Y = X$

(iv) $X \subseteq Y$ y $X \subseteq Z$ si y solo si $X \subseteq Y \cap Z$

(v) $X \cap U = X$

(vi) $X \cap X = X$

(vii) $X \cap \emptyset = \emptyset$

Observación 2.2.3.12. Casi todas las propiedades para la unión tienen su análogo para la intersección, pero hay una de ellas que no. La enunciamos y demostraremos que es falsa mediante la técnica del contraejemplo, muy útil cuando queremos demostrar que una afirmación es falsa.

$$X \subseteq Z \text{ e } Y \subseteq Z \text{ si y solo si } X \cap Y \subseteq Z$$

Demostración. La implicación $X \subseteq Z$ e $Y \subseteq Z \Rightarrow X \cap Y \subseteq Z$ sí es cierta, ya que pueden suceder dos cosas:

- Si $X \cap Y = \emptyset$, por la proposición 2.2.2.21 sabemos que el conjunto vacío es subconjunto de cualquier conjunto, luego $X \cap Y \subseteq Z$.
- Si $X \cap Y \neq \emptyset$, entonces tomamos un elemento $x \in X \cap Y$. Como $X \subseteq Z$ e $Y \subseteq Z$, esto implica que $x \in Z$.

Sin embargo, la implicación que no es cierta es $X \cap Y \subseteq Z \Rightarrow X \subseteq Z$ e $Y \subseteq Z$. Para demostrarlo, construyamos los conjuntos $Z = \{1\}$, $X = \{1, 2\}$, $Y = \{1\}$. Evidentemente, $X \cap Y = \{1\} \subseteq Z$, ya que es el propio conjunto. Sin embargo, aunque $Y \subseteq Z$, X no es subconjunto de Z.

La siguiente proposición recoge algunas propiedades interesantes que relacionan la unión con la intersección.

Proposición 2.2.3.13. Sean X, Y, $Z \subseteq U$. Entonces:

(i) $X \cap Y \subseteq X \cup Y$. Además, $X \cap Y = X \cup Y$ si y solo si $X = Y$

(ii) $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$

(iii) $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$

(iv) $X \cup (X \cap Y) = X$

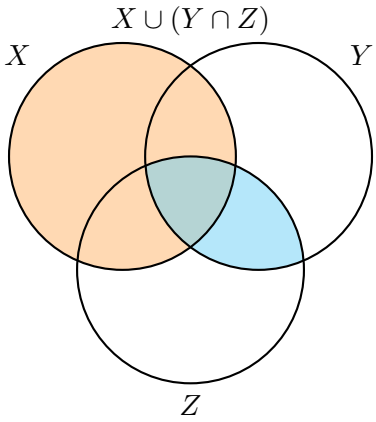
(v) $X \cap (X \cup Y) = X$

A modo de ejemplo, veamos cómo demostrar una igualdad entre conjuntos de dos formas diferentes probando la propiedad (ii). La primera forma será mediante diagramas de Venn. Aunque este método no es del todo formal, es muy útil para hacernos una idea del conjunto al que se hace referencia. La segunda forma será utilizando la proposición 2.2.2.18, que nos proporcionaba un método para demostrar la igualdad entre dos conjuntos.

Primera forma. Para demostrar que

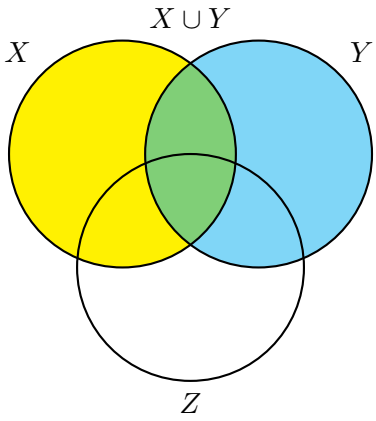
$$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$$

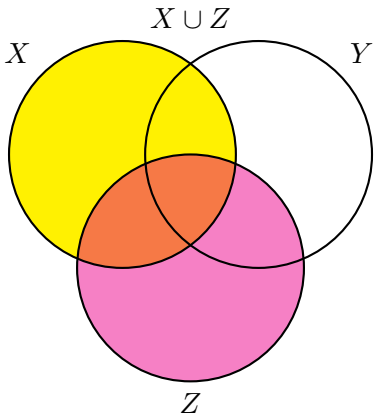
dibujemos por separado los diagramas de Venn de $X \cup (Y \cap Z)$ y de $(X \cup Y) \cap (X \cup Z)$.



Como podemos ver, el conjunto coloreado de naranja es X, el conjunto coloreado de azul es $Y \cap Z$, y el conjunto $X \cup (Y \cap Z)$ es el conjunto coloreado por ambos colores.

En el caso del segundo conjunto es más complicado ver el resultado y debemos pensar en qué regiones aparecen coloreadas en cada una de las uniones.





Como hablamos de la intersección de ambos conjuntos, las regiones coloreadas en ambos diagramas son todo X y la intersección de Y y Z, exactamente igual que en el diagrama de $X \cup (Y \cap Z)$. Por tanto, deducimos que ambos conjuntos son iguales.

Segunda forma. Ya hemos adelantado el procedimiento que vamos a seguir para demostrar formalmente la igualdad. Debemos probar la doble inclusión:

($\subseteq$) Veamos que $X \cup (Y \cap Z) \subseteq (X \cup Y) \cap (X \cup Z)$. Para ello, tomemos un elemento $x \in X \cup (Y \cap Z)$. Por estar en la unión, $x \in X$ o $x \in Y \cap Z$ (realmente puede estar en ambos conjuntos a la vez, pero ese caso queda incluido en nuestra discusión).

- Si $x \in X$, entonces $x \in X \cup Y$ y $x \in X \cup Z$, luego $x \in (X \cup Y) \cap (X \cup Z)$, como queríamos probar.
- Si $x \in Y$ y $x \in Z$, entonces $x \in X \cup Y$ y $x \in X \cup Z$, por lo que $x \in (X \cup Y) \cap (X \cup Z)$ como queríamos probar.

Así, queda demostrada la primera inclusión, ya que todo elemento de $X \cup (Y \cap Z)$ está en $(X \cup Y) \cap (X \cup Z)$.

($\supseteq$) Veamos que $(X \cup Y) \cap (X \cup Z) \subseteq X \cup (Y \cap Z)$. Tomemos $x \in (X \cup Y) \cap (X \cup Z)$. Entonces, $x \in X \cup Y$ y $x \in X \cup Z$.

- Del primero de los dos conjuntos deducimos que si $x \in X$, entonces $x \in X \cup (Y \cap Z)$ como queríamos probar.
- Si $x \in Y$, como x también está en $X \cup Z$, no queda otra que concluir que $x \in Z$. Así, $x \in Y \cap Z$ y, finalmente, $x \in X \cup (Y \cap Z)$.

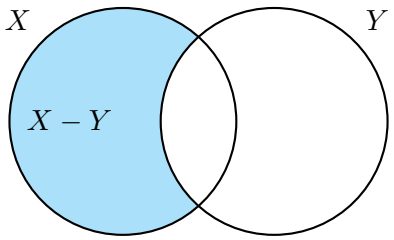
De esta forma queda probado que $(X \cup Y) \cap (X \cup Z) \subseteq X \cup (Y \cap Z)$.

Como hemos probado que cada conjunto es subconjunto del otro, por la proposición 2.2.2.18, se cumple la igualdad.

Definición 2.2.3.14. Sean X e Y dos conjuntos. Se define la diferencia X menos Y, y se denota $X - Y$ (o $X \backslash Y$), como el conjunto

$$X - Y = \{x \in X \, : \, x \notin Y\}$$

Es decir es el conjunto formado por todos los elementos de X que no están en Y. El diagrama de Venn correspondiente a la diferencia es el siguiente:



Ejemplo 2.2.3.15. Sean $X = \{0, 1, 2, 3, 4, 5\}$ e $Y = \{1, 3, 5\}$. Entonces,

$$X - Y = \{0, 2, 4\}$$

Proposición 2.2.3.16. Sean X, Y, Z tres conjuntos. Entonces:

(i) Si X e Y son disjuntos, entonces $X - Y = X$.

(ii) $X - (Y \cup Z) = (X - Y) \cap (X - Z)$

(iii) $X - (Y \cap Z) = (X - Y) \cup (X - Z)$

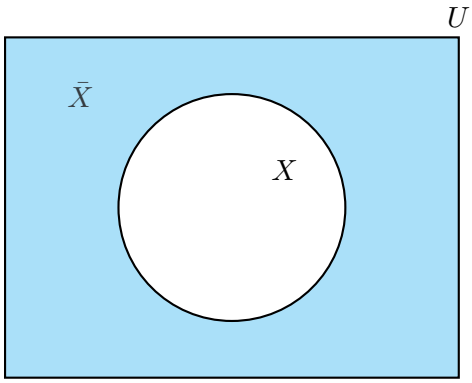
Ejercicio 2.2.3.17. Demostrar utilizando diagramas de Venn y formalmente que

$$(X - Y) \cap Z = (X \cap Z) - (Y \cap Z)$$

Definición 2.2.3.18. Sea $X \subseteq U$. Se define el conjunto complementario de X, y se denota $\bar{X}$ (o X^c) como

$$\bar{X} = U - X = \{x \in U \, : \, x \notin X\}$$

Gráficamente se representa de la siguiente forma:



Ejemplo 2.2.3.19. Sea $U = \{a, b, c, d, e\}$, y sea $X = \{a, d\}$. Entonces,

$$\bar{X} = \{b, c, e\}$$

Proposición 2.2.3.20. Sea X un conjunto. Entonces:

(i) $\bar{\bar{X}} = X$

(ii) $\bar{\emptyset} = U$

(iii) $\bar{U} = \emptyset$

El siguiente resultado es uno de los más importantes que vamos a ver en esta unidad. Tiene una versión análoga en lógica proposicional.

Teorema 2.2.3.21 (Leyes de De morgan)**.** Sean X e Y dos conjuntos. Entonces:

(i) $\overline{X \cup Y} = \bar{X} \cap \bar{Y}$

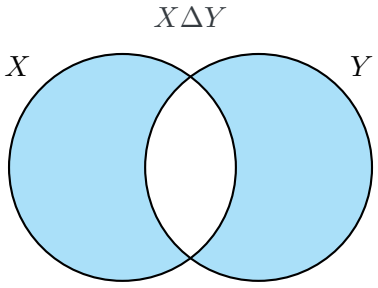
(ii) $\overline{X \cap Y} = \bar{X} \cup \bar{Y}$

La demostración quedará como ejercicio en la hoja de actividad práctica.

Definición 2.2.3.22. Sean X e Y dos conjuntos. Se define la diferencia simétrica de X e Y, y se denota $X \Delta Y$, como

$$X \Delta Y = (X - Y) \cup (Y - X)$$

Gráficamente se representa de la siguiente forma:



Ejemplo 2.2.3.23. Si $X = \{1, 3, 5\}$ e $Y = \{1, 2, 3\}$, entonces

$$X\Delta Y = \{2, 5\}$$

Proposición 2.2.3.24. Sean X e Y dos conjuntos. Entonces,

$$X\Delta Y = (X \cup Y) - (X \cap Y)$$

La demostración se deja como ejercicio en la hoja de actividad práctica.

Definición 2.2.3.25. Sean X e Y dos conjuntos. Se define el producto cartesiano de X por Y, y se denota $X \times Y$, como

$$X \times Y = \{(x, y) : x \in X, y \in Y\}$$

Es decir, los elementos del producto cartesiano son pares ordenados cuya primera coordenada es un elemento del primer conjunto y su segunda coordenada es un elemento del segundo conjunto.

Observación 2.2.3.26. En general, se puede definir el producto cartesiano de n conjuntos $X_1 \times X_2 \times \cdots \times X_n$ (o $\prod_{i=1}^{n} X_i$) como

$$\prod_{i=1}^{n} X_i = \{(x_1, x_2, \ldots, x_n) : x_i \in X_i, i \in \{1, \ldots, n\}\}$$

Ejemplo 2.2.3.27. Veamos un par de ejemplos:

(i) El conjunto $\mathbb{R}^2$, es decir, el plano real, cuyos elementos son los puntos (x, y), es el conjunto $\mathbb{R} \times \mathbb{R}$.

(ii) Si $X = \{a, b, c\}$ e $Y = \{b, d\}$, entonces el producto cartesiano es

$$X \times Y = \{(a, b), (a, d), (b, b), (b, d), (c, b), (c, d)\}$$

Proposición 2.2.3.28. Sean X e Y dos conjuntos finitos. Entonces, $|X \times Y| = |X| \cdot |Y|$.

Definición 2.2.3.29. Sea X un conjunto no vacío, y sean $X_1, X_2, \ldots, X_n \subseteq X$. Se dice que $X_1, X_2, \ldots, X_n$ forman una partición de X si se satisfacen las siguientes propiedades:

(i) $\bigcup_{i=1}^{n} X_i = X$.

(ii) $X_i \cap X_j = \emptyset$ si $i \neq j$. Es decir, si los conjuntos son disjuntos dos a dos.

Ejemplo 2.2.3.30. Para el conjunto $\mathbb{N}$, una partición es la formada por el conjunto de números pares y el conjunto de números impares, ya que la unión de ambos es el conjunto de naturales y no hay ningún número que sea par e impar a la vez.

Finalizamos esta sección con un resultado muy importante relacionado con la cantidad de elementos pertenecientes a la unión de conjuntos.

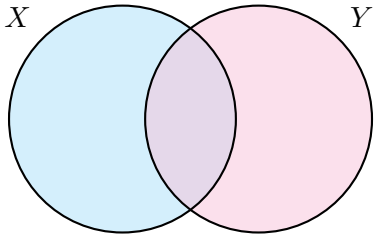
Teorema 2.2.3.31 (Principio de inclusión-exclusión)**.** Sean X e Y dos conjuntos. Entonces,

$$|X \cup Y| = |X| + |Y| - |X \cap Y|$$

La idea de este resultado es que, para contar los elementos de la unión de X e Y contamos los elementos de X y los de Y, pero en este caso estamos contando dos veces los elementos que pertenecen a ambos conjuntos, es decir

$$|X| + |Y| = |X \cup Y| + |X \cap Y|$$

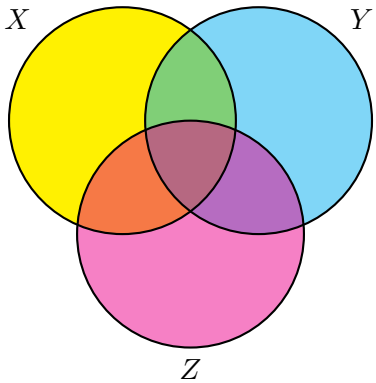
Por tanto, debemos restar a esta cantidad la cantidad de elementos de la intersección, contados dos veces. En el diagrama de Venn se aprecia que la intersección tiene combinados dos colores, que equivale, en nuestro caso, a decir que la hemos contado dos veces.



Corolario 2.2.3.32 (Principio de inclusión-exclusión caso $n = 3$)**.** Sean X, Y, Z tres conjuntos. Entonces,

$$|X \cup Y \cup Z| = |X| + |Y| + |Z| - |X \cap Y| - |X \cap Z| - |Y \cap Z| + |X \cap Y \cap Z|$$

Este resultado incluso admite una extensión para el caso n general, pero no es necesario verlo. La idea en este caso es que al contar los elementos de X, Y y Z, estamos contando dos veces aquellas zonas comunes a dos conjuntos pero no a tres, y estamos contando tres veces la cantidad de elementos $X \cap Y \cap Z$. Por tanto, si restamos la cantidad de elementos de las intersecciones dos a dos, el primer problema lo habremos resuelto, pero habremos quitado tres veces la cantidad de elementos de $X \cap Y \cap Z$, por tanto debemos sumarla una vez. De nuevo, los colores pueden darnos una idea intuitiva del procedimiento.



Veamos un ejemplo de este resultado.

Ejemplo 2.2.3.33. De una muestra de 100 pacientes recogida en un centro de salud, 74 padecen artritis, 17 fibromialgia y 25 osteoporosis. Además, 4 pacientes padecen las tres enfermedades. Sabiendo que todos los pacientes sufren alguna enfermedad, ¿cuántos padecen dos enfermedades?

Lo primero que haremos será definir los conjuntos:

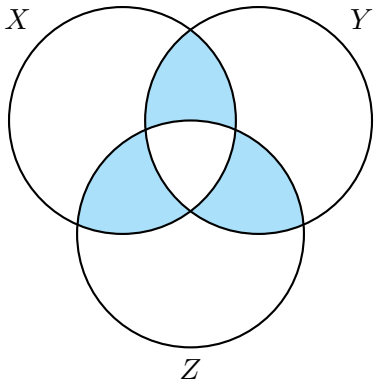
- $X = \{\text{pacientes que padecen artritis}\}$
- $Y = \{\text{pacientes que padecen fibromialgia}\}$
- $Z = \{\text{pacientes que padecen osteoporosis}\}$

Entonces, la pregunta que nos están haciendo es cuántas personas pertenecen a, exactamente, dos conjuntos. Es decir, calcular

$$|X \cap Y| + |X \cap Z| + |Y \cap Z| - 3|X \cap Y \cap Z|$$

Se resta tres veces la cantidad de elementos de la intersección de los tres conjuntos porque al sumar los elementos de las intersecciones dos a dos, los hemos contado tres veces y son elementos que no nos interesan.

Gráficamente, queremos calcular la cantidad de elementos que aparecen en las regiones sombreadas.



Los datos de los que disponemos son los siguientes:

- $|X| = 74$
- $|Y| = 17$
- $|Z| = 25$
- $|X \cap Y \cap Z| = 4$
- $|X \cup Y \cup Z| = 100$

Llamemos $a = |X \cap Y| + |X \cap Z| + |Y \cap Z|$. Por el corolario 2.2.3.32, sabemos que

$$|X \cup Y \cup Z| = |X| + |Y| + |Z| - a + |X \cap Y \cap Z|$$

Si sustituimos los datos que tenemos y despejamos a, tenemos que

$$100 = 74 + 17 + 25 - a + 4 \Leftrightarrow a = 20$$

Además, $3|X \cap Y \cap Z| = 3 \cdot 4 = 12$. Por tanto, la solución buscada es $20 - 12 = 8$. Es decir, 8 pacientes padecen dos enfermedades.

2.3. Conjuntos numéricos

2.3.1. Introducción

Probablemente, el concepto de las Matemáticas con el que más familiarizada está la sociedad es el número. De hecho, general, y erróneamente, se identifica a las Matemáticas con los números. Pero, ¿qué es un número? ¿Cómo podríamos definirlo?

En un primer intento, podríamos pensar en que los números representan cantidades. Esta idea puede tener sentido, de hecho lo tiene, con números como el 1, el 27 o incluso el 0 o el -4. Pero esta hipótesis pierde fuerza cuando pensamos en el $\frac{1}{2}$, el $\sqrt{2}$, π o i (la unidad imaginaria, $\sqrt{-1}$). Lo que realmente sucede es que estamos englobando dentro del concepto de número a objetos de distinta clase, por eso es tan difícil dar una definición de número más allá de decir que número es un elemento de $\mathbb{C}$ (el conjunto de números complejos, al cuál pertenecen todos los números que conocemos). Deberíamos centrarnos en definir los elementos de cada tipo de conjunto numérico. A eso nos vamos a dedicar en esta sección. El apartado más importante será el primero, sobre los números naturales. El resto de apartados pretenden servir como repaso de algunas de las propiedades más importantes. Una versión divulgativa de esta sección puede leerse en este post https://elescritoriodeenrique.com/2021/09/02/la-verdadera-naturaleza-de-los-numeros/

2.3.2. Números naturales

Los números naturales surgen de la necesidad de contar, tanto una cantidad de objetos (cardinal) como la posición de un objeto en una ordenación (ordinal).

Nota 2.3.2.1. La inclusión o exclusión del 0 como número natural es un debate ampliamente extendido que no tiene una respuesta correcta. En este curso, consideraremos al 0 número natural, es decir, $\mathbb{N} = \{0, 1, 2, \ldots\}$. Cuando hagamos referencia a todos los números naturales excluyendo al 0 podemos hablar de $n \in \mathbb{N}$ tal que $n \geq 1$ o de enteros positivos.

Las propiedades o axiomas que caracterizan a los números naturales son las siguientes:

Axiomas de Peano.

(i) $0 \in \mathbb{N}$. *Es decir, asumimos la existencia de un número natural. El resto de números se construyen a partir de este con los siguientes axiomas.*

(ii) Existe una función sucesor, s, de forma que a cada número natural, n, le asocia un número natural $s(n)$. *Esta función sucesor es, intuitivamente, la función que a cada n le asocia $n+1$.*

(iii) El 0 no es sucesor de ningún número natural. *Con este axioma hacemos referencia a que el 0 es el primer número natural, es decir, el conjunto de números naturales tiene un primer elemento.*

(iv) Si $s(n) = s(m)$, entonces $n = m$. *Por lo que sabemos de lógica proposicional, esta afirmación es equivalente a que si $n \neq m$, entonces $s(n) \neq s(m)$. Es decir, este axioma viene a decir que el sucesor de un natural es único.*

(v) Si A es un conjunto con $0 \in A$ tal que, para todo $n \in A$, $s(n) \in A$, entonces $A = \mathbb{N}$. *Este axioma nos dice que si un conjunto tiene un primer elemento y, dado cualquier elemento, el siguiente también está en el conjunto, entonces el conjunto es el de los números naturales.*

En realidad, el quinto axioma debería decir que dicho conjunto es *equiparable* al conjunto de números naturales, pues si pensamos en el conjunto de números naturales pares

$$X = \{n \in \mathbb{N} : \exists k \text{ tal que } n = 2k\}$$

este conjunto satisface todos los axiomas: en efecto, el conjunto de números pares tiene un primer elemento, el 0. La función sucesor es $s(n) = n+2$, y cada número par lo lleva a un único número. Además, $n+2 \in X$. Por tanto, este conjunto satisface los Axiomas de Peano y no es el conjunto de números naturales.

Del quinto axioma podemos deducir un razonamiento para demostrar propiedades sobre números naturales denominado Principio de Inducción.

Definición 2.3.2.2 (Principio de Inducción)**.** Sea A un conjunto que satisface los Axiomas de Peano cuyo primer elemento es n_0, y sea P una propiedad definida sobre los elementos de A. Entonces, $P(n)$ es cierto para todo $n \in A$ si satisface las siguientes propiedades:

(i) $P(n_0)$ es cierto.

(ii) Si $P(n)$ es cierto para cierto $n \geq n_0$, entonces $P(n+1)$ es cierto.

A la propiedad (i) se la conoce como **caso base**, lo denotaremos CB. A la propiedad (ii) se la conoce como **paso inductivo** (o paso de inducción), y lo denotaremos PI. Dentro del paso inductivo, a la premisa de la implicación se la conoce como **hipótesis de inducción**, y la denotaremos HI.

Una metáfora clásica sobre el funcionamiento del Principio de Inducción es el siguiente: si tenemos colocadas unas fichas de dominó y demostramos que podemos tirar la primera ficha y que, tirando cualquier, ficha podríamos tirar la siguiente, habremos demostrado que tirando la primera ficha podemos tirarlas todas.

Ejemplo 2.3.2.3. Queremos demostrar que, para todo $n \in \mathbb{N}$,

$$\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$$

Lo primero de todo es recordar que la notación $\sum$ se utiliza para el sumatorio, es decir, la suma de los elementos. En este caso

$$\sum_{k=0}^{n} k = 0 + 1 + 2 + 3 + \cdots + n$$

Ahora debemos identificar la propiedad, que es

$$P(n) \equiv \sum_{k=0}^{n} k = \frac{n(n+1)}{2}$$

(CB) El primer elemento es $n = 0$, por tanto, queremos probar que $P(0)$ es cierto. Por una parte,

$$\sum_{k=0}^{0} k = 0$$

Por otra parte,

$$\frac{0 \cdot 1}{2} = 0$$

Como ambos son iguales, $P(0)$ es cierto.

(PI) Siempre debemos escribir la hipótesis de inducción y, a continuación, enunciar la propiedad $P(n+1)$ que queremos demostrar. Finalmente, partiremos del lado izquierdo de la igualdad, iremos operando hasta poder utilizar la hipótesis de inducción y, a partir de ese momento, seguiremos operando hasta obtener el lado derecho de la igualdad que queríamos probar.

La hipótesis de inducción es la siguiente: dado $n \in \mathbb{N}$,

$$\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$$

Es decir, asumimos que esto es cierto para ese n.

Queremos probar que es cierto

$$P(n+1) \equiv \sum_{k=0}^{n+1} k = \frac{(n+1)(n+2)}{2}$$

Así,

$$\sum_{k=0}^{n+1} k = \left(\sum_{k=0}^{n} k\right) + (n+1)$$

Simplemente hemos partido la suma para poder aplicar la hipótesis de inducción. En este primer ejemplo vamos a detallarlo mucho más. Hemos realizado lo siguiente:

$$0 + 1 + 2 + 3 + \cdots + n + (n+1) = (0 + 1 + 2 + 3 + \cdots + n) + (n+1)$$

Ahora, por HI, podemos sustituir $\displaystyle\sum_{k=0}^{n} k$ por $\dfrac{n(n+1)}{2}$ y obtenemos

$$\sum_{k=0}^{n+1} k = \left(\sum_{k=0}^{n} k\right) + (n+1) = \frac{n(n+1)}{2} + (n+1)$$

En este punto, ya solo debemos operar.

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

De esta forma,

$$\sum_{k=0}^{n+1} k = \left(\sum_{k=0}^{n} k\right) + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2}$$

como queríamos demostrar.

Habiendo demostrado que se cumplen el caso base y el paso inductivo, hemos demostrado la propiedad para todo $n \in \mathbb{N}$.

Observación 2.3.2.4. Debemos fijarnos en que son absolutamente necesarios los dos pasos de la inducción para la demostración. Si solo demostramos el caso base, no podemos garantizar que la propiedad se cumpla para todos los elementos, solo para el que la hemos probado. Y si solo demostramos el paso inductivo, eso tampoco garantiza que la propiedad sea cierta para todos los elementos.

Veamos dos ejemplos que muestran la importancia de ambos pasos para poder demostrar que una propiedad es cierta.

Ejemplo 2.3.2.5. Sea $P(n) \equiv n^2 + n + 11$ es primo. Se puede comprobar que $P(0)$, $P(1)$, $P(2)$, …, $P(9)$ son todas ciertas (casos base). Sin embargo, esto no implica que $P(n)$ sea cierta para todo $n \in \mathbb{N}$. Solo basta con fijarse en que $P(10)$ ya no es cierta, pues $10^2 + 10 + 11 = 121 = 11^2$.

Ejemplo 2.3.2.6. Sea $P(n) \equiv 3n + 2$ es múltiplo de 3. Podemos reescribirla, para hacerla más operativa, como

$$P(n) \equiv \exists k \in \mathbb{N} \text{ tal que } 3n + 2 = 3k$$

Demostramos el paso inductivo directamente. Asumimos que se cumple la HI, es decir, que dado $n \in \mathbb{N}$, $\exists k \in \mathbb{N}$ tal que $3n + 2 = 3k$. Queremos ver que $\exists m \in \mathbb{N}$ tal que $3(n+1) + 2 = 3m$.

$$3(n+1) + 2 = 3n + 3 + 2(3n + 2) + 3$$

Nos conviene escibirlo de esta forma y no como $3n+3$ para poder aplicar la hipótesis de inducción.

$$3(n+1) + 2 = 3n + 3 + 2(3n + 2) + 3 = 3k + 3 = 3(k+1)$$

Si llamamos $m = k + 1$, hemos encontrado el $m \in \mathbb{N}$ tal que

$$3(n+1) + 2 = 3n + 3 + 2(3n + 2) + 3 = 3k + 3 = 3(k+1) = 3m$$

Sin embargo, la propiedad no es cierta, de hecho, para ningún $n \in \mathbb{N}$. Por ejemplo, $3 \cdot 0 + 2 = 2$.

Ejercicio 2.3.2.7. Demostrar que $10^n + 1$ es múltiplo de 11 para cualquier $n \in \mathbb{N}$ impar.

Observación 2.3.2.8. Hay ocasiones en que el Principio de Inducción no es suficiente para demostrar una propiedad sobre los naturales. El ejemplo más clásico es la demostración del Teorema Fundamental de la Aritmética. Este enunciado afirma que todo número natural mayor que 1 puede descomponerse como producto de números primos. Vamos a verlo.

Vamos a reescribir el enunciado: $\forall n \in \mathbb{N}$ tal que $n > 1$, $\exists\, p_1, p_2, \ldots, p_r$ primos (algunos de ellos probablemente iguales entre sí) tales que $n = p_1 p_2 \cdots p_r$.

(CB) Si $n = 2$, entonces $2 = 2$, que es primo, luego el resultado es cierto trivialmente.

(PI) Supongamos que, dado $n > 1$, existen p_1, p_2, ..., p_r primos tales que $n = p_1 p_2 \cdots p_r$ (HI). Queremos ver que existen p'_1, p'_2, ..., p'_m primos (nótese que no tienen por qué ser los mismos ni haber una relación entre la cantidad de factores primos de n y $n+1$) tales que $n+1 = p'_1 p'_2 \cdots p'_s$.

Una primera idea pasaría por dar el siguiente paso aplicando la HI:

$$n + 1 = p_1 p_2 \cdots p_r + 1$$

Sin embargo, poder demostrar el resultado desde este punto resulta imposible, dado que tenemos una suma cuyo único factor común es el 1. Por tanto, vamos a hacer una discusión de las posibilidades para $n + 1$.

(i) Si $n + 1$ es primo, la demostración ya habría terminado.

(ii) Si $n+1$ no es primo, entonces existen dos números, a, $b < n+1$ tales que $n+1 = ab$. Ahora tenemos un producto, mucho más manejable, de términos menores o iguales que n (de hecho, son menores estrictos, pero no es necesario profundizar en ello). Se nos puede ocurrir que, si hemos llegado a demostrar la propiedad para n, podemos argumentar que cada término es producto de primos; digamos

$$a = p'_1 p'_2 \cdots p'_k$$

$$b = p'_{k+1} p'_{k+2} \cdots p'_s$$

Así,

$$n + 1 = ab = p'_1 p'_2 \cdots p'_s$$

El problema radica en que el Principio de Inducción solo parte de la premisa de que el resultado es cierto para n, no para todos los números menores o iguales que n.

El siguiente resultado es el conocido como Principio de Inducción Fuerte (o Completa), y nos garantiza que el procedimiento propuesto en la observación anterior es correcto.

Definición 2.3.2.9 (Principio de Inducción Fuerte)**.** Sea A un conjunto que satisface los Axiomas de Peano cuyo primer elemento es n_0, y sea P una propiedad definida sobre los elementos de A. Entonces, $P(n)$ es cierto para todo $n \in A$ si satisface las siguientes propiedades:

(i) $P(n_0)$ es cierto.

(ii) Si $P(k)$ es cierto para cierto $n_0 \leq k \leq n$, entonces $P(n+1)$ es cierto.

Las propiedades fundamentales de los números naturales son las siguientes:

Proposición 2.3.2.10. Sean n, m, $k \in \mathbb{N}$ Entonces:

(i) $n + (m + k) = (n + m) + k$

(ii) $n + m = m + n$

(iii) $0 + n = n + 0 = n$

(iv) $n(mk) = (nm)k$

(v) $nm = mn$

(vi) $1n = n1 = n$

(vii) Si $nm = 1$, entonces $n = m = 1$

(viii) $n(m + k) = nm + nk$

Observación 2.3.2.11. Hay que tener en cuenta que en $\mathbb{N}$ no existen las operaciones de resta ni división. Ni siquiera se pueden hacer raíces cuadradas, ya que son operaciones que no tienen por qué devolver un número natural. Solo existen la suma, el producto y la potenciación. Realmente, fijándonos en la resta y en la división, estas operaciones no dejan de ser la suma de un número negativo y el producto por un número fraccionario respectivamente.

2.3.3. Números enteros

Los números enteros son una extensión de los números naturales que surgen de resolver ecuaciones del tipo

$$x + n = 0, \text{ donde } n \in \mathbb{N}$$

El conjunto de números enteros se denota $\mathbb{Z}$.

Proposición 2.3.3.1. Sean n, m, $k \in \mathbb{Z}$. Entonces:

(i) $n + (m + k) = (n + m) + k$

(ii) $n + m = m + n$

(iii) $0 + n = n + 0 = n$

(iv) $\exists - n \in \mathbb{Z}$ tal que $n + (-n) = -n + n = 0$.

(v) $n(mk) = (nm)k$

(vi) $nm = mn$

(vii) $1n = n1 = n$

(viii) Si $nm = 1$, entonces $n = m = 1$

(ix) $n(m + k) = nm + nk$

En cuanto al orden, tema que veremos en otra unidad más a fondo, en $\mathbb{Z}$, podemos dar dos propiedades importantes.

Proposición 2.3.3.2. Sean n, $m \in \mathbb{Z}$ tales que $n \leq m$. Entonces:

(i) $n + k \leq m + k$, $\forall k \in \mathbb{Z}$

(ii) $nk \leq mk$, si $k \geq 0$, y $nk \geq mk$, si $k \leq 0$

2.3.4. Números racionales

Los números racionales surgen de la necesidad de resolver ecuaciones de la forma

$$mx + n = 0, \text{ donde } n \in \mathbb{Z} \text{ y } m \in \mathbb{Z} - \{0\}$$

El conjunto de números racionales se denota $\mathbb{Q}$.

Proposición 2.3.4.1. Sean r_1, r_2, $r_3 \in \mathbb{Z}$. Entonces:

(i) $r_1 + (r_2 + r_3) = (r_1 + r_2) + r_3$

(ii) $r_1 + r_2 = r_2 + r_1$

(iii) $0 + r_1 = r_1 + 0 = r_1$

(iv) $\exists - r_1 \in \mathbb{Z}$ tal que $r_1 + (-r_1) = -r_1 + r_1 = 0$.

(v) $r_1(r_2r_3) = (r_1r_2)r_3$

(vi) $r_1r_2 = r_2r_1$

(vii) $1r_1 = r_1 1 = r_1$

(viii) Dado $r \in \mathbb{Q} - 0$, $\exists r^{-1} \in \mathbb{Q}$ tal que $rr^{-1} = r^{-1}r = 1$. Además, si $r = \frac{a}{b}$, entonces $r^{-1} = \frac{b}{a}$

(ix) $r_1(r_2 + r_3) = r_1r_2 + r_1r_3$

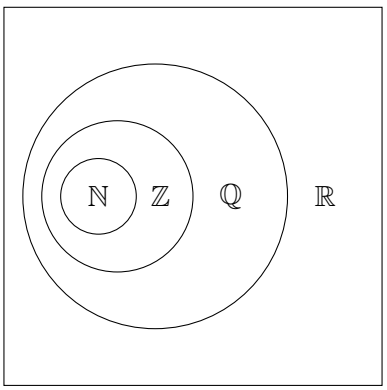
2.3.5. Números reales

Los números irracionales no solo surgen de resolver ecuaciones. Algunos de ellos sí, como $\sqrt{2}$, que es una solución de

$$x^2 - 2 = 0$$

Las soluciones reales de ecuaciones de grado n con coeficientes en $\mathbb{Z}$ reciben el nombre de números algebraicos, mientras que los que no son solución de ninguna de estas ecuaciones reciben el nombre de números trascendentes, como π. La complejidad de la definición de los irracionales queda fuera del alcance de este curso. El conjunto de irracionales se denota $\mathbb{I}$

Los números reales están formados por la unión de $\mathbb{Q}$ y $\mathbb{I}$. El conjunto de reales se denota $\mathbb{R}$. El siguiente diagrama muestra la inclusión de los distintos conjuntos numéricos.



2.4. Bases de numeración

2.4.1. Introducción

Formas de denotar los números naturales hay muchas. Podemos citar la romana (I, II, III, IV, V, VI, ...) o la que todos conocemos, la indoarábiga (1, 2, 3, 4, 5, 6, ...), pero a lo largo de la Historia ha habido muchas. Sin embargo, para realizar fácilmente operaciones, un sistema de numeración debe tener dos propiedades fundamentales:

(i) Debe tener una *base*, es decir, algo que nos agrupe los números de alguna manera para contarlos más fácilmente. Por ejemplo, en el sistema decimal, base 10, contamos de diez en diez. Así, podemos hablar de 2 centenas, que son 20 decenas y que son 200 unidades. En el sistema de base 12, podemos hablar de 2 docenas, que son 24 unidades. En nuestro día a día usamos muchos sistemas de numeración: para el dinero usamos un sistema decimal, para medir ángulos usamos un sistema sexagecimal (base 60) y, para marcar las horas, usamos un sistema en base 12 (además de un sistema hexadecimal para minutos y segundos). Los números romanos no parecen seguir ninguna base.

(ii) Debe ser un sistema *posicional*, es decir, si escribimos un número, cada posición de cada cifra nos debe indicar si estamos en las unidades, decenas, centenas (en la base que sea)... Por ejemplo, el número 123 es un número que nos indica que posee 1 centena, 2 decenas y 3 unidades.

En esta sección estudiaremos los conceptos básicos relacionados con los sistemas de numeración y nos centraremos en el sistema decimal y en el binario. Veremos cómo escribir cualquier número racional en ambos sistemas. No estudiaremos el caso de los números irracionales, ya que el propósito de la sección es entender el sistema binario, utilizado por las computadoras, y estas no son capaces de computar números irracionales.

2.4.2. Conceptos básicos

Definición 2.4.2.1. En un sistema de numeración posicional, se le llama base al número que define el orden de magnitud en que se ve incrementada cada una de las cifras sucesivas que componen el número. Es también la cantidad de símbolos presentes en dicho sistema.

Ejemplo 2.4.2.2. Los números del 0 al 9 tienen una sola cifra porque son lo que llamamos "unidades". A partir del 10 hasta el 99 lo llamamos decenas. En estos números, que podemos representar como XY, tenemos que X representa cuántas decenas llevamos contadas, e Y cuántas unidades en esa última decena. El número 12 significa 1 decena y 2 unidades, y el número 23 significa 2 decenas y 3 unidades. Después del 99 viene el 100. Este número de tres cifras quiere decir que ya hemos contado 10 decenas, y a esas 10 decenas la llamamos centena. Entonces, los números de tres cifras, que podemos representarlos como XYZ, significan X centenas, Y decenas y Z unidades. Para llegar a un millar, 1000, necesitamos contar 100 decenas, y así sucesivamente. Es una progresión que crece de forma exponencial. Cada vez que añadimos 1 cifra al número, hay que añadir un 0. Para tener una decena necesitamos $10^0 = 1$ decenas. Para tener una centena necesitamos $10^1 = 10$ decenas. Para tener un millar necesitamos $10^2 = 100$ decenas. El exponente del 10 indica cuántos ceros se añaden al 1.

Ejemplo 2.4.2.3. En el sistema binario (base 2) tenemos dos cifras: 0 y 1. Al alcanzar dos unidades tenemos una decena (en base 2) y lo escribimos 10. Otro sistema de numeración bastante más reciente es el hexadecimal, es decir, contando de 16 en 16. Los números en este sistema son 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F (del 10 al 15 se representan con las letras de A a F).

Observación 2.4.2.4. Muchas veces se utiliza un subíndice para saber en qué sistema estamos leyendo el número. El número 14 en sistema decimal se escribe 14_{10}. El 1110 en sistema binario se escribe 1110_2.

2.4.3. El sistema binario. Números no negativos

Veamos primero cómo traducir un número natural binario a decimal. En sistema decimal, la posición de las cifras importa mucho. Por ejemplo, el 329 tiene un 9 multiplicado por 10^0 (diremos que la posición es 0). Tiene un 2 multiplicado por 10^1 (la posición es 1). Y tiene un 3 multiplicado por 10^2 (la posición es 2). Así, empezamos a contar por la posición 0 de derecha a izquierda y sumamos todos los términos:

$$329 = 9 \cdot 10^0 + 2 \cdot 10^1 + 3 \cdot 10^2$$

Número natural de binario a decimal

Para encontrar la representación decimal de un número binario vamos a hacer lo mismo. Queremos saber qué número es el 1110_2 en sistema decimal. Así que contamos las posiciones: hay un 0 en la posición 0 y tres 1's en las posiciones 1, 2 y 3. Cuando hay un 0, lo multiplicamos por $2^{\text{posición}}$, y cuando hay un 1, lo mismo. Así,

$$1110_2 = 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 8 + 4 + 2 + 0 = 14_{10}$$

Ejercicio 2.4.3.1. ¿Cuál es la representación decimal de 1101_2?

(a) 42.

(b) 13.

(c) 14.

(c) 43.

Solución. (b).

Número natural de decimal a binario

El procedimiento consiste en tomar el número, dividirlo entre 2, quedarnos con el resto (que será 0 o 1, en función de si el número decimal es par o impar respectivamente) y realizar de nuevo el proceso con el cociente de la división hasta que este sea 0. Dividiremos utilizando la expresión

$$\text{dividendo} = \text{divisor} \cdot \text{cociente} + \text{resto}$$

Tomemos por ejemplo 14_{10}. Entonces,

$$14 = 7 \cdot 2 + 0$$

$$7 = 3 \cdot 2 + 1$$

$$3 = 1 \cdot 2 + 1$$

$$1 = 0 \cdot 2 + 1$$

Los restos, de abajo a arriba forman el número en binario 1110_2.

Ejercicio 2.4.3.2. ¿Cuál es la representación binaria de 25_{10}?

(a) 10110

(b) 1001

(c) 11001

(d) 01001

Solución. (c).

Número no negativo con decimales de binario a decimal

Las posiciones de los dígitos a la derecha de la coma son negativas. Comenzando desde la más cercana a la coma y moviéndonos hacia la derecha, las posiciones son -1, -2, $-3\ldots$ Por tanto, el procedimiento a seguir es una extensión del que vimos para números naturales. Por ejemplo, si queremos traducir 0.101001_2 a decimal, tenemos que

$$0.101001_2 = 0 \cdot 2^0 + 1 \cdot 2^{-1} + 0 \cdot 2{-}2 + 1 \cdot 2^{-3} + 0 \cdot 2^{-4} + 0 \cdot 2^{-5} + 1 \cdot 2^{-6}$$

Realizamos las operaciones, teniendo en cuenta que $2^{-n} = \frac{1}{2^n}$, y obtenemos

$$0.101001_2 = 0.5 + 0 + 0.125 + 0 + 0 + 0.015625 = 0.640625_{10}$$

Ejercicio 2.4.3.3. Cuál es la representación decimal de 10.101_2?

(a) 0.625

(b) 3.125

(c) 2.5

(d) 2.625

Solución. (d)

Antes de explicar el procedimiento para traducir números no negativos con decimales de decimal a binario, debemos definir un par de conceptos.

Definición 2.4.3.4. Sea $x \in \mathbb{R}$. Se define la parte entera de x, y se denota $\lfloor x \rfloor$, como el mayor de los números enteros menores o iguales que x.

Ejemplo 2.4.3.5.

(i) $\left\lfloor \frac{1}{2} \right\rfloor = 0$

(ii) $\left\lfloor -\frac{1}{2} \right\rfloor = -1$, ya que $-1 \leq -\frac{1}{2}$

(iii) $\lfloor 5 \rfloor = 5$

(iv) $\lfloor 0.\hat{9} \rfloor = 1$, donde $0.\hat{9}$ denota al número cero coma nueve periódico, ya que $0.\hat{9} = 1$. ¿Sabrías decir por qué?

Definición 2.4.3.6. Sea $x \geq 0$. Se define la parte decimal de x como $x - \lfloor x \rfloor$.

La definición varía ligeramente para números negativos, pero como solo vamos a necesitar este concepto para números positivos, no necesitamos generalizarla.

Ejemplo 2.4.3.7. La parte decimal de 12.443 es 0.443.

Números no negativos con decimales de decimal a binario

- Se transforma la parte entera a binario. (Si la parte entera es 0 en binario será 0, si la parte entera es 1 en binario será 1, si la parte entera es 5 en binario será 101 y así sucesivamente).
- Se sigue con la parte fraccionaria, multiplicando cada número por 2. Si el resultado obtenido es mayor o igual a 1 se anota como un uno (1) binario. Si es menor que 1 se anota como un 0 binario. (Por ejemplo, al multiplicar 0.6 por 2 obtenemos como resultado 1.2 lo cual indica que nuestro resultado es un uno (1) en binario, solo se toma la parte decimal del resultado).
- Después de realizar cada multiplicación, se colocan los números obtenidos en el orden de su obtención.

Por ejemplo, si queremos escribir 0.3125_{10} en binario, primero calculamos la parte entera:

$$\lfloor 0.3125 \rfloor = 0$$

Por tanto, la parte entera del número en binario será 0.

Siguiendo con la parte decimal, tenemos:

$$0.3125 \cdot 2 = 0.625 \to 0$$

$$0.625 \cdot 2 = 1.25 \to 1$$

$$0.25 \cdot 2 = 0.5 \to 0$$

$$0.5 \cdot 2 = 1 \to 1$$

De esta forma,

$$0.3125_{10} = 0.0101_2$$

Observación 2.4.3.8. Algunos números que en el sistema decimal no tienen un decimal periódico, en binario sí, como 0.1. Queda como ejercicio la comprobación.

2.4.4. Números negativos. Complemento a dos

Para sumar números binarios, tenemos que tener en cuenta la siguiente tabla:

+	0	1
0	0	1
1	1	0

Así, para sumar dos números binarios, lo haremos teniendo en cuenta las posiciones de las cifras.

Ejemplo 2.4.4.1. $1011 + 101 = 10000$.

Como ya sabemos, la posición de una cifra en un número binario viene dada por potencias de 2. Los números del 0 al 1 los podemos escribir con una cifra. Los números del 0 al 3 los podemos escribir con dos cifras. Los números del 0 al 7 los podemos escribir con tres cifras. Los números del 0 al 15 los podemos escribir con cuatro cifras. En general, los números del 0 al $2^n - 1$ los podemos escribir con n cifras. A estas cifras las llamaremos bits.

Proposición 2.4.4.2. Supongamos que tenemos n bits. Entonces, cualquier número binario de $k < n$ cifras lo podemos escribir con n bits añadiendo $n - k$ ceros a la izquierda.

Ejemplo 2.4.4.3. Los números del 0 al 7 podemos representarlos con 4 bits como:

$$0 = 0000$$

$$1 = 0001$$

$$2 = 0010$$

$$3 = 0011$$

$$4 = 0100$$

$$5 = 0101$$

$$6 = 0110$$

$$7 = 0111$$

Nuestro objetivo es representar números negativos en binario. Una opción podría ser añadir un 0 delante de la representación en binario del número en valor absoluto. Por ejemplo, el 14 en binario es 1110, así que -14 sería 01110. Sin embargo, si queremos operar números binarios no es la mejor opción, ya que $14 - 14 = 14 + (-14) = 0$, pero $1110 + 01110 = 11100$, que por una parte es 56 y por otra parte tiene más cifras de las deseadas.

El segundo intento para representar números negativos es mediante el complemento a uno.

Definición 2.4.4.4. Dado un número binario escrito con n bits, se define su complemento a uno como el resultado de transformar todas las apariciones de 0's por 1's y viceversa.

Ejemplo 2.4.4.5. Con 4 bits, el complemento a uno de 1110 es 0001.

Observación 2.4.4.6. El inconveniente de este método es la doble representación del 0, ya que, por ejemplo, con 4 bits, tenemos que

$$+0 = 0000$$

$$-0 = 1111$$

La versión más aceptada para representar números negativos es el complemento a dos.

Definición 2.4.4.7. Dado un número binario escrito con n bits, se define el complemento a dos de ese número como el resultado de sumar 1 al complemento a uno. Otra forma de calcularlo es comenzar por la derecha copiando todas las cifras hasta llegar a la primera que sea 1, esta también se copia y, el resto de cifras se transforman: si son 0, en 1; si son 1, en 0.

Ejemplo 2.4.4.8. El complemento a dos de 0010100 es 1101100.

2.5. Cuestionario

Ejercicio 11. El conjunto $\{x \in \mathbb{R} : x^2 = 1\}$ está definido por:

(a) compresión

(b) extensión

Ejercicio 12. Dado un conjunto X con n elementos, $|\mathcal{P}(X)|$ es igual a:

(a) $2n$

(b) n^2

(c) 2^n

(d) $\frac{n}{2}$

Ejercicio 13. Dado $X = \{n \in \mathbb{N} : \exists k \in \mathbb{N} \text{ tal que } n = 3k\}$ subconjunto de $U = \{n \in \mathbb{N} : n \leq 9\}$, su representación como tiras de bits es:

(a) 1001001001

(b) 1110000000

(c) 0010010010

(d) 0101010101

Ejercicio 14. $\bar{X} \cap (Y \cup Z)$ es igual a:

(a) $(\bar{X} \cup Y) \cap (\bar{X} \cup Z)$

(b) $(Y - X) \cup (Z - X)$

(c) $(Y - X) \cap (Z - X)$

(d) $(\bar{X} \cap Y) \cup (\bar{X} \cap Z)$

Ejercicio 15. Si $|X| = 12$, $|Y| = 8$, $|X \cap Y| = 6$, entonces $|X \cup Y|$ es igual a:

(a) 20

(b) 26

(c) 14

(d) 10

Ejercicio 16. $n^3 - n$ es múltiplo de 3 para todo $n \in \mathbb{N}$:

(a) Verdadero

(b) Falso

Ejercicio 17. Si una propiedad sobre números naturales no puede demostrarse por inducción, entonces es falsa:

(a) Verdadero

(b) Falso

Ejercicio 18. Todo número natural expresado en base decimal puede expresarse en base binaria.

(a) Verdadero

(b) Falso

Ejercicio 19. 11.01_2 es igual a:

(a) 11.01_{10}

(b) 3.5_{10}

(c) 2.25_{10}

(d) 3.25_{10}

Ejercicio 20. El complemento a dos de 010 es:

(a) 2

(b) 101

(c) 110

(d) 011

Capítulo 3

Combinatoria y Recursividad

3.1. Introducción

La Combinatoria es la rama de las Matemáticas dedicada al estudio de las técnicas de conteo y ordenación de elementos. Lo que caracteriza a la Combinatoria es que no se necesita contar los elementos de un conjunto uno a uno para saber cuántos hay, sino que se desarrollan métodos específicos para hacerlo. Por lo general, todo estudiante universitario está familiarizado con los conceptos de variación, permutación y combinación desde Secundaria, pero frecuente, y erróneamente, Combinatoria y Probabilidad son confundidas como una sola cosa. La Probabilidad estudia cómo medir la certidumbre de que ocurra un determinado suceso, tiene que ver con el azar. La Combinatoria ayuda a la Probabilidad a la hora de calcular la probabilidad de un suceso en un espacio muestral de sucesos equiprobables, aplicando la famosa Regla de Laplace:

$$\frac{\text{número de casos favorables}}{\text{número de casos posibles}}$$

Sin embargo, la Combinatoria, como rama de las Matemáticas tiene sus propios problemas de interés. En esta unidad no daremos por supuestos ningunos conocimientos previos en esta temática, solo aquellos que ya hemos estudiado en las dos unidades anteriores. En la primera sección explicaremos tres de los principios básicos del conteo de elementos: las reglas de la suma y el producto y el principio del palomar. Las dos primeras sirven como base para deducir los conceptos de variación, permutación y combinación, a quienes dedicaremos toda la segunda sección. La tercera se dedicará a los números combinatorios y sus propiedades. Nuestros objetivos en este apartado serán el binomio de Newton y el Triángulo de Pascal, dos de los conceptos matemáticos más bonitos de la Combinatoria. En la cuarta y última sección nos dedicaremos a la recursividad, un tema fundamental en Matemáticas y programación. En este apartado veremos en qué consiste la recursividad y plantearemos métodos para resolver unos tipos concretos de recurrencias, las recurrencias lineales.

Esta unidad se ha planteado desde una visión eminentemente práctica, con numerosos ejemplos y ejercicios que recomiendo encarecidamente intentar resolver antes de mirar sus soluciones. No obstante, se ha dedicado un esfuerzo considerable en la deducción teórica de las distintas fórmulas que aparecen a lo largo de la unidad. Los problemas de Combinatoria generalmente son muy fáciles de entender una vez vista la solución, pero algo más esquivos a la hora de abordarlos, es por esta razón que mi consejo es intentar resolver tantos problemas como sea posible.

3.2. Principios básicos del conteo

3.2.1. Introducción

Como ya hemos adelantado, e incluso hemos podido empezar a ver en la unidad anterior con el Principio de inclusión-excusión, no es necesario contar todos los elementos para saber cuántos hay. Las dos técnicas más sencillas, y de las que se derivan el resto de las que veremos, las vamos a exponer en esta sección: las reglas de la suma y el producto.

Finalizaremos la sección viendo otra técnica de la Combinatoria que, si bien no nos ayuda a contar elementos, sí que nos permite sacar conclusiones muy interesantes en ciertos contextos muy diversos, como una partida de cartas.

3.2.2. Reglas de la suma y el producto

A lo largo de esta unidad vamos a estar hablando de **sucesos**. Intuitivamente, un suceso es una de entre todas las posibilidades que se pueden dar en un experimento o proceso. No entraremos en mayor detalle para no confundir Combinatoria con Probabilidad. Como ejemplo podemos citar el siguiente: de una clase de 20 alumnos de Ingeniería del Software, escogemos un delegado. Este es un ejemplo de experimento con un único suceso, la elección de un delegado. Hay 20 distintas posibilidades para que se dé el suceso, una por cada alumno, ya que cada una de ellas daría lugar a distintos resultados.

Ejemplo 3.2.2.1. Supongamos que en una clase hay 10 estudiantes de Matemáticas y 15 estudiantes de Ingeniería del Software. Si quisiéramos elegir un delegado para toda la clase, entonces este será de Matemáticas o de Ingeniería. Como de Matemáticas hay 10 alumnos y de Ingeniería hay 15, habrá $10 + 15 = 25$ posibilidades. A este hecho tan intuitivo se le conoce como regla de la suma.

Proposición 3.2.2.2 (Regla de la suma)**.** Sean dos sucesos A y B independientes, es decir, no se pueden dar de manera simultánea, tales que para cada uno de ellos hay n y m posibilidades respectivamente. Entonces, hay $n + m$ posibilidades de que se dé A o B.

Observación 3.2.2.3. Se suele hablar de sucesos en el contexto de la Combinatoria, pero todos los resultados que vamos a ver tienen su versión para conjuntos. De hecho, como ya mencionamos en la anterior unidad, los conjuntos son la base que fundamenta las Matemáticas, incluidos los sucesos. En este sentido, la regla de la suma podríamos enunciarla de la siguiente forma:

Sean dos conjuntos disjuntos A y B tales que $|A| = n$, $|B| = m$. Entonces, $|A \cup B| = n + m$.

Este resultado no es más que un caso particular del Principio de inclusión-exclusión en el que $A \cap B = \emptyset$.

Ejemplo 3.2.2.4. Volvamos al ejemplo anterior y supongamos ahora que queremos elegir un delegado de entre los matemáticos y otro delegado de entre los ingenieros. Tenemos 10 posibilidades distintas de escoger al primero y 15 para el segundo. Como el hecho de escoger al primero no afecta a la forma de escoger al segundo, intuitivamente hay $10 \cdot 15 = 150$ formas de elegir un delegado de Matemáticas y un delegado de Ingeniería del Software. La idea para llegar a esta cifra es la siguiente:

denotemos por (M, I) a la pareja de delegados de Matemáticas y de Ingeniería. Debemos contar la cantidad de parejas distintas (M, I) que puede haber. Para ello, supongamos que fijamos un delegado de Matemáticas, digamos M_0. Entonces, habrá 15 distintas parejas (M_0, I) de delegados, una por cada alumno de Ingeniería. Pero estos emparejamientos los hemos realizado fijando al delegado de Matemáticas. Así que, como hay 10 posibles delegados, tendremos que contar 15 parejas distintas para cada uno, dando como resultado $10 \cdot 15$.

Proposición 3.2.2.5 (Regla del producto)**.** Dado un suceso C que puede descomponerse en dos etapas sucesivas e independientes entre sí A y B, tales que para cada uno de ellos hay n y m posibilidades respectivamente, se tiene que hay nm posibilidades de que se dé C.

Observación 3.2.2.6. Al igual que con la regla de la suma, esta proposición tiene su versión análoga para conjuntos, que se desprende de cómo hemos llegado a la fórmula en el ejemplo. El enunciado es el siguiente:

Sean dos conjuntos A y B tales que $|A| = n$ y $|B| = m$. Entonces, $|A \times B| = nm$.

Ambas reglas son trivialmente generalizables a una cantidad arbitraria finita de sucesos.

3.2.3. Principio del palomar

Ejemplo 3.2.3.1. Supongamos que en una partida de cartas hay 3 jugadores y se han repartido todos los ases de una baraja española. Como hay 4 ases de cada palo, sabemos que hay al menos un jugador que ha recibido 2 o más ases. Esto es lo que se conoce como **principio del palomar** o principio de Dirichlet.

Proposición 3.2.3.2 (Principio del palomar)**.** Supongamos que hay n cajas (o palomares) y colocamos $n + 1$ palomas en esas cajas. Entonces, existe al menos una caja en la que hay 2 o más palomas.

Observación 3.2.3.3. La idea que subyace detrás de este principio es la siguiente: volviendo al ejemplo anterior, la forma de demostrar que al menos un jugador recibía 2 o más ases es encontrar el reparto que "separa" más las cartas entre un jugador y otro, ya que si se le reparten los 4 ases a un jugador, por ejemplo, el resultado es trivial. La idea en el razonamiento es suponer que repartimos el primer as al jugador 1, el segundo as al jugador 2 y el tercer as al jugador 3. Así, como todavía queda un as por repartir, este irá a un jugador que ya tenía un as, por lo que se cumple el resultado.

Repetimos que este es el razonamiento clave porque, en caso de que fuese falso el resultado, sería la forma mediante la que encontraríamos el contraejemplo. Por ejemplo, si en lugar de 4 ases hubiese solo 3, no podríamos garantizar que al menos un jugador recibe dos ases.

Nuestro siguiente objetivo es tratar de generalizar este principio a n cajas y $m > n$ palomas.

Ejemplo 3.2.3.4.

- Supongamos, en el ejemplo anterior, que en lugar de 4 ases, hay 5. Siguiendo con el razonamiento de la observación 3.2.3.3, en el peor de los casos, ningún jugador tendría más de dos ases. Es decir, solo podemos afirmar lo mismo que cuando había 4 ases. Notemos que no podemos afirmar que hay al menos dos jugadores con 2 o más ases porque puede darse el caso de que un mismo jugador los tenga todos.

  Vamos a recalcar que hay $n = 3$ jugadores y $m = 5 = n + 2$ ases.

- Si ahora hay 6 ases, es decir, $m = n + 3 = 2n$ (ya que $n = 3$), el mismo razonamiento nos indica que solo podemos seguir afirmando lo mismo.
- En el caso de que haya 7 ases, es decir, $m = 2n + 1$, sí que podemos garantizar que hay al menos un jugador que recibe 3 o más ases. Y lo mismo ocurre para $2n + 2$ y $3n$.

Lo que podemos ver es que cada vez que hay $kn+1$, $kn+2$ y $(k+1)n$ ases, con $k \in \mathbb{N}$, podemos garantizar que hay al menos un jugador que recibe $k + 1$ o más ases.

Para poder enunciar esta propiedad de forma general, vamos a repasar un resultado sobre la división entera.

Nota 3.2.3.5. Sean m, $n \in \mathbb{N}$. Entonces, existen de manera única $c \in \mathbb{N}$ y $r \in \{0, 1, \ldots, n-1\}$ tales que

$$m = nc + r$$

A m se le conoce como dividendo, a n como divisor, a c como cociente y a r como resto. Además, como se puede leer en el enunciado, r siempre es no negativo y menor que el divisor.

Esta es la forma en la que se escribe la división de m entre n.

En nuestro ejemplo tenemos que el dividendo es el número de ases, m, y el divisor es el número de jugadores, n. Por tanto:

Proposición 3.2.3.6 (Principio del palomar generalizado)**.** Supongamos que hay n cajas y colocamos $m > n$ palomas en esas cajas. Si $m = nk + r$, entonces:

(i) Si $r = 0$, entonces hay al menos una caja con k o más palomas.

(ii) Si $r \neq 0$, entonces hay al menos una caja con $k + 1$ o más palomas.

Ejemplo 3.2.3.7. En un grupo de 200 personas hay, al menos, 4 que han nacido en la misma semana del año.

Para comprobarlo, como un año tiene 52 semanas, decimos que $m = 200$ y $n = 52$. Ahora, debemos dividir 200 entre 52. Así,

$$200 = 3 \cdot 52 + 44$$

Por tanto, como el resto es distinto de 0 y el cociente es 3, por el Principio del palomar garantizamos que hay al menos 4 personas que nacieron en la misma semana del año.

Vamos con un ejemplo un poco más complicado.

Ejemplo 3.2.3.8. Si elegimos 100 números naturales al azar, siempre habrá 2 de ellos cuya diferencia sea múltiplo de 99.

Llamemos a los números n_1, n_2, $\ldots$, n_{100} y dividámoslos a todos entre 99. Entonces, por la nota 3.2.3.5 cada n_i es de la forma

$$n_i = 99c_i + r_i$$

Ahora, como todo múltiplo de 99 es de la forma $99k$, fijémonos en que la diferencia de dos de estos números es

$$n_i - n_j = 99c_i + r_i - (99c_j + r_j) = 99(c_i - c_j) + (r_i - r_j)$$

y será un múltiplo de 99 si $r_i - r_j = 0$, es decir, si $r_i = r_j$. Pero hay 100 números y los restos $r_i \in \{0, 1, \ldots, 98\}$, es decir, hay 99 posibles restos. Por tanto, por el Principio del palomar, habrá al menos dos de estos números cuyo resto al dividirlos entre 99 sea igual y, así, su diferencia será múltiplo de 99.

3.3. Variaciones, permutaciones y combinaciones

3.3.1. Introducción

Una vez hemos visto los principios básicos del recuento, nuestro objetivo es desarrollar las fórmulas que nos permitan hacer cálculos en el conteo y la ordenación de elementos de manera eficiente. Veremos también que las variaciones y las permutaciones son el mismo concepto y, finalmente, haremos una recapitulación en forma de tabla con todo lo visto en la sección. No obstante, mi recomendación es que no se haga uso de esta tabla en ningún momento, ya que puede llevar a una falta de comprensión de los problemas a la hora de enfrentarse a ellos.

3.3.2. Sin repetición

Definición 3.3.2.1. Sea $n \in \mathbb{N}$. Se define el factorial de n, se denota $n!$ y se lee "factorial de n", como

$$n! = \begin{cases} 1 & n = 0 \\ n(n-1)! & n > 0 \end{cases}$$

Observación 3.3.2.2. La definición de factorial es una definición recursiva, es decir, cada término se define a partir del anterior. Para este tipo de definiciones se necesita un caso base, que no dependa de ningún otro término. Para el factorial, el caso base es el 0. Se define $0! = 1$ por conveniencia a la hora de realizar cálculos, pero tiene sentido definirlo de esta forma cuando veamos las permutaciones. Volveremos a ello más adelante.

Ejemplo 3.3.2.3. Los primeros factoriales son los siguientes:

(i) $0! = 1$

(ii) $1! = 1 \cdot 0! = 1$

(iii) $2! = 2 \cdot 1! = 2$

(iv) $3! = 3 \cdot 2! = 6$

(v) $4! = 4 \cdot 3! = 24$

(vi) $5! = 5 \cdot 4! = 120$

Supongamos que un conjunto X tiene n elementos (distinguibles, ya que es un conjunto) y queremos saber cuántas ordenaciones podemos realizar con $r \leq n$ elementos de X. Para empezar, tenemos que fijarnos en que queremos calcular cuántas $r-$uplas (es decir, tuplas de r elementos) de la forma $(x_1, x_2, \ldots, x_r)$ hay.

- Como al principio tenemos n elementos, hay n distintas posibilidades para escoger el elemento x_1. Podemos decir que $x_1 \in X$.
- Para escoger el elemento x_2, ya no tenemos n posibilidades, pues ya hemos escogido previamente el elemento x_1. Así que habrá $n-1$ posibilidades. Podemos decir que $x_2 \in X - \{x_1\}$.
- Si seguimos el proceso, llegamos a que para escoger el elemento x_r tenemos $n - r + 1$ posibilidades. Podemos decir que $x_r \in X - \{x_1, x_2, \ldots, x_{r-1}\}$.

Por tanto, por la Regla del producto, como tenemos que calcular

$$|X \times X - \{x_1\} \times \cdots \times X - \{x_1, x_2, \ldots, x_{r-1}\}|$$

la cantidad de ordenaciones que podemos hacer con r elementos de X es

$$n(n-1)\cdots(n-r+1)$$

A esta cantidad la llamamos **variaciones de n elementos tomados de r en r**, y se denota $V_{n,r}$.

Para sintetizar lo que llevamos hasta ahora, vamos a escribirlo formalmente.

Definición 3.3.2.4. Sea X un conjunto con $|X| = n$, y sea $0 \leq r \leq n$. A la cantidad de distintas ordenaciones de r elementos de X se le llama variación y se calcula como

$$V_{n,r} = n(n-1)\cdots(n-r+1)$$

Observación 3.3.2.5. Por la definición 3.3.2.1, podemos concluir que

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

ya que

$$n! = n(n-1)(n-2)\cdots(n-r+1)(n-r)!$$

Ejemplo 3.3.2.6. ¿Cuántos números de 3 cifras pueden formarse con los elementos del conjunto $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$?

Al ser un conjunto, cada elemento lo podemos utilizar una única vez, luego las cifras no se repiten. Como además, por ejemplo, 123 es distinto de 132, debemos calcular el número de ordenaciones. Estamos en el caso de una variación de 9 elementos tomados de 3 en 3. Así, habrá

$$V_{9,3} = \frac{9!}{6!} = 9 \cdot 8 \cdot 7 = 504 \text{ números diferentes}$$

Definición 3.3.2.7. Sea X un conjunto con $|X| = n$. A la cantidad de distintas ordenaciones de los n elementos de X se le llama permutación de n elementos, se denota P_n, y se define como

$$P_n = n!$$

Observación 3.3.2.8. Una permutación es un caso particular de variación donde $r = n$. La fórmula se obtiene de

$$P_n = V_{n,n} = \frac{n!}{(n-n)!} = \frac{n!}{0!} = \frac{n!}{1} = n!$$

En la observación 3.3.2.2 indicábamos que $0! = 1$ tiene sentido gracias a las permutaciones. Esto es así porque hay 1 única forma de ordenar 0 elementos.

Ejemplo 3.3.2.9. ¿Cuántas palabras (tengan sentido o no) pueden formarse con las letras de la palabra COPA?

Al haber 4 letras, utilizarlas todas y obtener palabras diferentes al reordenar las letras, estamos en el caso de una permutación. Así, se podrán formar

$$P_4 = 4! = 24 \text{ palabras distintas}$$

Hay un caso muy interesante de permutaciones que vamos a exponer. Supongamos que se van a sentar 5 comensales, A, B, C, D y E, alrededor de una mesa circular. Nos planteamos calcular de cuántas formas diferentes pueden sentarse. Una primera idea pasa por plantear una permutación de 5 elementos. Sin embargo, en este caso estamos contando como diferentes las ordenaciones

$$ABCDE,\ BCDEA$$

lo cual no es cierto, ya que todo comensal sigue teniendo a su derecha y a su izquierda a las mismas personas. Por ejemplo, A tiene a B a su derecha y a E a su izquierda (recordemos que están sentados en una mesa circular). Por tanto, de estas 5! formas deberíamos eliminar todas aquellas en las que los comensales solo se han corrido un asiento a la derecha, o izquierda. En nuestro ejemplo de ordenación, son iguales

$$ABCDE = BCDEA = CDEAB = DEABC = EABCD$$

Esto nos lleva a la fórmula

$$\frac{5!}{5} = 4!$$

A este tipo de permutaciones se las conoce como **permutaciones circulares**. En general, si hay n elementos, las permutaciones circulares de n elementos se denotan PC_n y se calculan como

$$PC_n = (n-1)!$$

Definición 3.3.2.10. Sea X un conjunto tal que $|X| = n$. A la cantidad de distintas ordenaciones de los n elementos de X colocados en círculo se le llama permutación circular de n elementos, se denota PC_n, y se define como

$$PC_n = (n-1)!$$

Definición 3.3.2.11. Sean n, $m \in \mathbb{N}$ tales que $m \leq n$. Se define el número combinatorio $\binom{n}{m}$, y se lee "n sobre m", como

$$\binom{n}{m} = \frac{n!}{m!(n-m)!}$$

Supongamos que un conjunto X tiene n elementos y queremos calcular la cantidad de conjuntos diferentes que podemos formar con $r \leq n$ elementos de X. En este caso, no es relevante el orden en el que aparecen los elementos de cada subconjunto. La forma de calcular esta cantidad, que llamaremos $C_{n,r}$, es tomar las variaciones $V_{n,r}$ y descontar de este número las distintas ordenaciones de cada conjunto. Como los conjuntos tienen r elementos, habrá $r!$ ordenaciones en cada conjunto de los formados. Por tanto,

$$C_{n,r} = \frac{V_{n,r}}{r!} = \frac{\frac{n!}{(n-r)!}}{r!} = \frac{n!}{r!(n-r)!} = \binom{n}{r}$$

Definición 3.3.2.12. Sea X un conjunto con $|X| = n$, y sea $0 \leq r \leq n$. A la cantidad de subconjuntos de r elementos de X se le llama combinación y se calcula como

$$C_{n,\,r} = \frac{n!}{r!(n-r)!} = \binom{n}{r}$$

Ejemplo 3.3.2.13. Un equipo de baloncesto dispone de 12 jugadores: 3 bases, 4 aleros y 5 pívots. ¿Cuántos equipos diferentes puede presentar el entrenador como quinteto titular formado por 1 base, 2 aleros y 2 pívots?

Para resolver este problema tenemos que tomar la decisión de si importa si un alero o un pívot juega por la izquierda o por la derecha. Si decidiésemos que importa este orden, trabajaríamos con variaciones, mientras que si no importa, deberíamos trabajar con combinaciones. Nosotros vamos a elegir la segunda opción.

Separaremos la resolución del problema en tres etapas y después aplicaremos la Regla del producto (tenemos que encontrar todas las ternas de la forma $(b,\, \{a_1,\, a_2\},\, \{p_1,\, p_2\})$).

(i) De los 3 bases debemos escoger 1, luego tenemos 3 posibilidades.

(ii) De los 4 aleros debemos escoger 2, luego habrá

$$C_{4,\,2} = \frac{4!}{2!2!} = 6 \text{ posibilidades}$$

(iii) De los 5 pívots debemos escoger 2, luego habrá

$$C_{5,\,2} = \frac{5!}{2!3!} = 10 \text{ posibilidades}$$

En total, hay $3 \cdot 6 \cdot 10 = 180$ posibles alineaciones diferentes.

De la definición de combinación podemos deducir un resultado interesante:

Proposición 3.3.2.14. Sea X un conjunto tal que $|X| = n$. Entonces,

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

Demostración. Para ver este resultado, tengamos en cuenta que $\binom{n}{k} = C_{n,\,k}$, que significa la cantidad de subconjuntos de X con k elementos. Como estamos sumando la cantidad de subconjuntos de cero elementos (conjunto vacío), un elemento, dos elementos, etc., hasta n elementos (el conjunto total X), estamos contando todos los elementos del conjunto $\mathcal{P}(X)$, que sabemos que tiene 2^n elementos. □

3.3.3. Con repetición

Hasta ahora hemos supuesto que los elementos no podían estar repetidos. En lo sucesivo vamos a desarrollar formas de contar que tienen en cuenta estos casos. La única diferencia a nivel teórico

que nos vamos a encontrar va a ser que ya no podemos tomar un elemento x de un conjunto X y trabajar con $X - \{x\}$, pues en ese caso, x sería un elemento irrepetible. En lugar de eso, tomaremos el elemento x y seguiremos trabajando con X.

Supongamos que tenemos un conjunto X con n elementos y queremos contar las ordenaciones de $r \geq 0$ elementos de X de manera que estos se puedan repetir. En este caso, queremos contar las distintas $r-$uplas $(x_1, x_2, \ldots, x_r)$ que hay. La diferencia es que ahora calculamos

$$|\overbrace{X \times X \times \cdots \times X}^{r}|$$

Por tanto, por la regla del producto, como para cada x_i hay n posibilidades e $i \in \{1, 2, \ldots, r\}$, se tiene que hay

$$\overbrace{n \cdot n \cdots n}^{r} = n^r \text{ distintas ordenaciones}$$

A esta cantidad la llamamos **variación con repetición** de n elementos tomados de r en r.

Definición 3.3.3.1. Sea X un conjunto con $|X| = n$, y sea $r \geq 0$. A la cantidad de ordenaciones que podemos hacer con r elementos de X, no necesariamente distintos, se le llama variación con repetición, se denota $VR_{n,r}$, y se calcula como

$$VR_{n,r} = n^r$$

Ejemplo 3.3.3.2. ¿De cuántas formas puede rellenarse una quiniela de 15 casillas?

Una quiniela de 15 casillas es de esta forma:

1	X	2

Así, en cada fila debemos poner un 1, una X o un 2. Por la Regla del producto, o por la definición anterior, hay

$$VR_{3,5} = 3^5 = 243 \text{ formas diferentes de rellenar una quiniela}$$

Observación 3.3.3.3. Observemos que ahora no es necesario que $r \leq n$, ya que no quitamos elementos de X.

Imaginemos que, como en el ejemplo 3.3.2.9, queremos calcular las distintas palabras que se pueden formar con las letras de la palabra CASACA. Si no nos preocupásemos por las letras que aparecen repetidas, diríamos que hay $6! = 720$ palabras. Sin embargo, en este recuento hemos contado como diferentes, por ejemplo, las siguientes ordenaciones:

CASACA y CASACA

pero no dejan de ser la misma palabra. Por tanto, fijada una ordenación, debemos eliminar cada palabra repetida. Esto podemos realizarlo contando cuantas permutaciones hay entre las

letras repetidas. Por ejemplo, en la ordenación anterior, hay $2! = 2$ permutaciones de la C y $3! = 6$ permutaciones de la A. Para simplificar más el sucesivo desarrollo, también contaremos las permutaciones de S, $1! = 1$ Así, el número de ordenaciones totales será

$$\frac{6!}{2!3!1!} = 60$$

Notemos que $2 + 3 + 1 = 6$.

En general, este va a ser el proceso que realicemos.

Definición 3.3.3.4. Supongamos que hay r elementos, x_1, x_2, ..., x_r, de forma que x_i aparece repetido n_i veces y $n_1 + n_2 + \cdots + n_r = n$. Es decir, contando repeticiones hay n elementos. A la cantidad de ordenaciones diferentes que podemos hacer de estos n elementos se la conoce como permutación con repetición, se denota $PR_n^{n_1, n_2, ..., n_r}$, y se calcula como

$$PR_n^{n_1, n_2, ..., n_r} = \frac{n!}{n_1! n_2! \cdots n_r!}$$

Imaginemos que tenemos 6 caramelos idénticos para repartir a 4 personas y queremos calcular de cuántas formas podemos hacerlo. El mejor modelo para representar esta situación es ordenar a las 4 personas como 1, 2, 3, 4, que los caramelos son asteriscos, *, y para diferenciar cuántos caramelos se lleva cada persona, separaremos los asteriscos con barras, /. Así, por ejemplo, una repartición sería:

$$**/*/**/*$$

En esta repartición, la persona 1 se lleva $x_1 = 2$ caramelos, la persona 2 se lleva $x_2 = 1$ caramelo, la persona 3 se lleva $x_3 = 2$ caramelos, y la persona 4 se lleva $x_4 = 1$ caramelo. Observemos que necesitamos 6 asteriscos para representar a los caramelos y 3 barras para representar la separación entre las personas. Además, evidentemente,

$$x_1 + x_2 + x_3 + x_4 = 6$$

Otra ordenación sería

$$**//***/*$$

Ahora, $x_1 = 2$, $x_2 = 0$, $x_3 = 3$, $x_4 = 1$. En total, independientemente de la ordenación, tenemos $6 + 3 = 9$ símbolos, uno que se repite 6 veces y otro que se repite 3. Habrá tantas posibles reparticiones de caramelos como distintas ordenaciones de estos 9 elementos. Pero esto ya sabemos cómo hacerlo, pues son permutaciones con repetición. En este ejemplo concreto serán

$$PR_9^{6,3} = \frac{9!}{6!3!} = 84$$

Definición 3.3.3.5. Supongamos que hay n elementos indistinguibles a repartir en r colecciones. A la cantidad de reparticiones diferentes que pueden hacerse se le llama combinaciones con repetición de n elementos tomados de r en r, se denota como $CR_{n,r}$, y se calcula como

$$CR_{n,r} = PR_{n+r-1}^{n,r-1} = \frac{(n+r-1)!}{n!(r-1)!} = \binom{n+r-1}{n}$$

Una aplicación muy interesante de las combinaciones con repetición es el cálculo del número de soluciones naturales de una ecuación diofántica cuyos coeficientes son todos 1.

Definición 3.3.3.6. Una ecuación diofántica es una ecuación de la forma

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$$

donde a_i, $x_i \in \mathbb{Z}$, $\forall i \in \{1, 2, \ldots, n\}$, y $c \in \mathbb{Z}$.

Ejemplo 3.3.3.7. Supongamos que queremos saber cuántas soluciones naturales tiene la ecuación

$$x_1 + x_2 + x_3 = 12$$

es decir, soluciones enteras tales que x_1, x_2, $x_3 \geq 0$. Planteamos el problema con asteriscos y barras. El modelo tendrá la siguiente forma:

$$****/***/*****$$

En ese caso particular, la solución de la ecuación es $(x_1, x_2, x_3) = (4, 3, 5)$.

Por tanto, el número de soluciones es

$$CR_{12,3} = \frac{14!}{12!2!} = 91$$

Observación 3.3.3.8. Todo problema que puede resolverse utilizando combinaciones con repetición puede plantearse como un problema de ecuaciones diofánticas como el que hemos visto. De hecho, será, generalmente, el modelo que utilicemos.

El siguiente problema tiene una mayor dificultad que los anteriores.

Ejemplo 3.3.3.9. Calcular de cuántas formas se pueden distribuir 20 bolas idénticas en 5 cajas diferentes de forma que:

(i) en cada caja haya, como mínimo, 2 bolas.

(ii) en la caja 1 no haya más de 5 bolas.

Lo primero que vamos a hacer es plantear el problema como una ecuación diofántica:

$$x_1 + x_2 + x_3 + x_4 + x_5 = 20$$

(i) Que en cada caja haya, como mínimo, 2 bolas quiere decir que $x_i \geq 2$, $\forall i \in \{1, 2, 3, 4, 5\}$. Por tanto, si dejamos repartidas 2 bolas en cada caja, quedarán por repartir 10 bolas en 5 cajas y el problema será calcular el número de soluciones de

$$x_1 + x_2 + x_3 + x_4 + x_5 = 10,\ x_i \geq 0$$

Por tanto, habrá

$$CR_{10,5} = \frac{14!}{10!4!} = 1001 \text{ formas diferentes}$$

(ii) Que en la caja 1 no haya más de 5 bolas quiere decir que $0 \leq x_1 \leq 5$. En este caso, recurriremos al cálculo del caso complementario. Que en la caja 1 no haya más de 5 bolas es el caso contrario a que haya al menos 6 bolas. Así, dejamos repartidas 6 bolas a la caja 1 y el problema queda como

$$x_1 + x_2 + x_3 + x_4 + x_5 = 14,\ x_i \geq 0$$

Por tanto, habrá

$$CR_{14,\,5} = \frac{18!}{14!4!} = 3060 \text{ formas diferentes}$$

De este modo, para resolver el problema inicial debemos calcular el número de formas totales de repartir 20 bolas en 5 cajas, sin ninguna restricción, y restar 3060. Estas son

$$CR_{20,\,5} = \frac{14!}{20!4!} = 10626 \text{ formas diferentes}$$

Así, el resultado final es $10626 - 3060 = 7566$.

Finalizamos la sección con una tabla que recoge todos los casos de aplicación de las fórmulas que hemos aprendido de Combinatoria.

	El orden no importa	El orden sí importa	
	Combinaciones	Variaciones	Permutaciones
Sin repetición	$C_n^r = \binom{n}{r} = \frac{n!}{r!(n-r)!}$	$V_n^r = \frac{n!}{(n-r)!}$	$P_n = n!$
Con repetición	$CR_n^r = \binom{n+r-1}{n} = \frac{(n+r-1)!}{n!(r-1)!}$	$VR_n^r = n^r$	$PR_n^{n_1,n_2,\ldots,n_r} = \frac{n!}{n_1!n_2!\cdots n_r!}$

3.4. Números combinatorios

3.4.1. Introducción

En la sección anterior ya hemos introducido los números combinatorios como forma de calcular combinaciones. Esta breve sección va a servir para profundizar un poco más en algunas de sus propiedades. Es la sección más teórica de todas las de la unidad, y en ella aparecen unas cuantas demostraciones de los resultados que aparecen en el texto que, por supuesto, no tienen como propósito ser memorizadas. Se ha valorado no incluirlas, debido a que es un curso diseñado para Ingeniería del Software. Sin embargo, se ha decidido mantenerlas porque resultan interesantes las técnicas de los razonamientos en Combinatoria que aparecen en ellas.

3.4.2. El binomio de Newton

El primer resultado que vamos a ver nos indica que los números combinatorios son simétricos con respecto de $\frac{n}{2}$.

Proposición 3.4.2.1. Sean $n,\ k \in \mathbb{N}$ tales que $n \geq k$. Entonces,

$$\binom{n}{k} = \binom{n}{n-k}$$

Demostración.

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n!}{(n-k)!k!} = \binom{n}{n-k}$$

□

Observación 3.4.2.2. En particular, se tiene que

$$\binom{n}{0} = \binom{n}{n} = 1$$

Proposición 3.4.2.3. Sean n, $k \in \mathbb{N}$ tales que $n \geq 2$ y $k \in \{1, 2, \ldots, n-1\}$. Entonces,

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

Demostración.

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{k!(n-k-1)!} = \frac{k(n-1)! + (n-k)(n-1)!}{k!(n-k)!} =$$

$$\frac{n(n-1)!}{k!(n-k)!} = \frac{n!}{k!(n-k)!} = \binom{n}{k}$$

□

Ejemplo 3.4.2.4.

$$\binom{6}{4} = \binom{5}{3} + \binom{5}{4} = 15$$

El binomio de Newton es bien conocido de la Educación Secundaria, especialmente el caso $n = 2$, que afirma que

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

Pero, en general, se tiene el siguiente resultado.

Teorema 3.4.2.5 (Binomio de Newton)**.** Sean x, $y \in \mathbb{R}$, y sea $n \in \mathbb{N}$. Entonces,

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

Demostración. El teorema se demuestra por inducción sobre n.

(CB) Los casos $n = 0$, 1, 2 son triviales.

(PI) Supongamos el resultado cierto para cierto $n \geq 2$ (de hecho, deberíamos suponerlo para $n \in \mathbb{N}$, pero como están probados los casos base $n = 0$, 1 y 2, no es necesario incluir 0 y 1). Debemos probar que se sigue cumpliendo para $n+1$, es decir, queremos ver que

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

Por tanto,

$$(x+y)^{n+1} = (x+y)^n (x+y)$$

Por hipótesis de inducción, tenemos que

$$(x+y)^{n+1} = (x+y)^n(x+y) = \left(\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k\right)(x+y) =$$

$$\sum_{k=0}^{n}\binom{n}{k}x^{n+1-k}y^k + \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^{k+1}$$

En el último paso hemos multiplicado x por toda la suma e y por toda la suma. Desarrollemos ahora las sumas:

$$\sum_{k=0}^{n}\binom{n}{k}x^{n+1-k}y^k = \binom{n}{0}x^{n+1}y^0 + \binom{n}{1}x^ny^1 + \binom{n}{2}x^{n-1}y^2 + \cdots + \binom{n}{n}x^1y^n$$

$$\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^{k+1} = \binom{n}{0}x^ny^1 + \binom{n}{1}x^{n-1}y^2 + \binom{n}{2}x^{n-2}y^3 + \cdots + \binom{n}{n}x^0y^{n+1}$$

Lo que vamos a hacer ahora es agrupar términos:

$$\sum_{k=0}^{n}\binom{n}{k}x^{n+1-k}y^k + \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^{k+1} = \binom{n}{0}x^{n+1}y^0 + \left[\binom{n}{1}x^ny^1 + \binom{n}{0}x^ny^1\right] +$$

$$\left[\binom{n}{2}x^{n-1}y^2 + \binom{n}{1}x^{n-1}y^2\right] + \cdots + \left[\binom{n}{n}x^1y^n + \binom{n}{n-1}x^1y^n\right] + \binom{n}{n}x^0y^{n+1} =$$

$$\binom{n}{0}x^{n+1}y^0 + \left[\binom{n}{1} + \binom{n}{0}\right]x^ny^1 + \left[\binom{n}{2} + \binom{n}{1}\right]x^{n-1}y^2 + \cdots +$$

$$\left[\binom{n}{n} + \binom{n}{n-1}\right]x^1y^n + \binom{n}{n}x^0y^{n+1}$$

Finalmente, como $n \geq 2$ (por esta razón supusimos el resultado cierto para $n \geq 2$ al inicio del paso inductivo), por la proposición 3.4.2.3, podemos operar de la siguiente forma:

$$\binom{n}{0}x^{n+1}y^0 + \left[\binom{n}{1} + \binom{n}{0}\right]x^ny^1 + \left[\binom{n}{2} + \binom{n}{1}\right]x^{n-1}y^2 + \cdots +$$

$$\left[\binom{n}{n} + \binom{n}{n-1}\right]x^1y^n + \binom{n}{n}x^0y^{n+1} = \binom{n}{0}x^{n+1}y^0 + \binom{n+1}{1}x^ny^1 +$$

$$\binom{n+1}{2}x^{n-1}y^2 + \cdots + \binom{n+1}{n}x^1y^n + \binom{n}{n}x^0y^{n+1}$$

La igualdad ya está prácticamente demostrada, ya solo falta observar que, por la observación 3.4.2.2

$$\binom{n}{0} = 1 = \binom{n+1}{0}$$

y

$$\binom{n}{n} = 1 = \binom{n+1}{n+1}$$

Por tanto, podemos cambiar los coeficientes de $x^{n+1}y^0$ y de x^0y^{n+1} por estos y obtenemos

$$\binom{n+1}{0}x^{n+1}y^0 + \binom{n+1}{1}x^ny^1 + \binom{n+1}{2}x^{n-1}y^2 + \cdots + \binom{n+1}{n}x^1y^n + \binom{n+1}{n+1}x^0y^{n+1} =$$

$$\sum_{k=0}^{n+1}\binom{n+1}{k}x^{n+1-k}y^k$$

como queríamos probar.

□

Observación 3.4.2.6. Si en lugar de $(x+y)^n$ tenemos $(x-y)^n$, podemos aplicar el teorema 3.4.2.5 a $(x+(-y))^n$. En este caso, la fórmula quedaría

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

Es decir, términos positivos para k par y términos negativos para k impar.

Ejemplo 3.4.2.7. Hallar el coeficiente de x^{11} en el desarrollo de

$$(3\sqrt[3]{x^2} - x\sqrt{x})^9$$

Por las propiedades de las potencias, podemos reescribir la expresión como

$$(3\sqrt[3]{x^2} - x\sqrt{x})^9 = \left(3x^{\frac{2}{3}} - x^{\frac{3}{2}}\right)^9$$

Entonces, el binomio de Newton tiene la forma

$$\left(3x^{\frac{2}{3}} - x^{\frac{3}{2}}\right)^9 = \sum_{k=0}^{9} (-1)^k \binom{9}{k} 3^{9-k} x^{\frac{2}{3}(9-k)} x^{\frac{3}{2}k} = \sum_{k=0}^{9} (-1)^k \binom{9}{k} 3^{9-k} x^{6+\frac{5}{6}k}$$

Por tanto,

$$x^{6+\frac{5}{6}k} = x^{11} \Leftrightarrow 6 + \frac{5}{6}k = 11 \Leftrightarrow k = 6$$

Así, el coeficiente de x^{11} es

$$(-1)^6 \binom{9}{6} 3^{9-6} = 27 \frac{9!}{6!3!} = 2268$$

3.4.3. El Triángulo de Pascal-Tartaglia

El Triángulo de Pascal, o de Pascal-Tartaglia, es una forma de representar y calcular los coeficientes del binomio de Newton de un modo muy curioso. Los primeros términos del Triángulo de Pascal son los siguientes:

0						1						
1					1		1					
2				1		2		1				
3			1		3		3		1			
4		1		4		6		4		1		
5	1		5		10		10		5		1	
6	1	6		15		20		15		6		1

Cuadro 3.1: Los términos en negrita a la izquierda hacen referencia a la potencia a la que está elevado el binomio.

La forma de construir el triángulo consiste en colocar un 1 en la fila 0 y dos 1 en la fila 1 tal y como aparecen arriba. A partir de aquí, cada fila n se construye colocando un 1 al inicio, otro 1 al final y el resto de términos se forman sumando los dos que aparecen encima de él. Por ejemplo, en la fila 3, el segundo término es un 3, que se obtiene al sumar el 1 y el 2 que tiene encima. La justificación de que estos son los distintos números combinatorios ha quedado patente en la observación 3.4.2.2 y en la proposición 3.4.2.3.

Sobre el Triángulo de Pascal también podemos observar cómo se satisface la proposición 3.3.2.14.

3.5. Relaciones de recurrencia

3.5.1. Introducción

En esta sección vamos a estudiar las relaciones de recurrencia, las cuales surgen en numerosos problemas de Matemáticas y programación. Sin entrar en mucho detalle, una recurrencia es una secuencia de términos que se definen a partir de sus predecesores. Ya hemos visto ejemplos de recurrencias, por ejemplo, el factorial de un número natural se define a partir del factorial del término anterior. En ocasiones, nos interesa saber cómo calcular el término general de la secuencia sin necesidad de calcular todos los términos precedentes. Es a lo que llamamos solución general de la recurrencia. Sin embargo, en general no hay técnicas que nos permitan obtenerlo. En este apartado nos centraremos en las recurrencias lineales, para las cuáles sí que existen métodos para resolverlas.

3.5.2. Recursividad

Definición 3.5.2.1. Se dice que una función

$$\begin{array}{rcl} a : \mathbb{N} & \longrightarrow & \mathbb{R} \\ n & \longmapsto & a(n) = a_n \end{array}$$

es una sucesión de números reales y la denotamos $(a_n)_{n\in\mathbb{N}}$ o, simplemente, (a_n). Al término a_n se le llama término general de la sucesión.

Ejemplo 3.5.2.2. Consideremos la sucesión cuyos primeros términos son

$$0,\ 1,\ 4,\ 9,\ 16,\ 25\ldots$$

Esta es la sucesión formada por los cuadrados de los números naturales. Por tanto, la sucesión es (a_n), donde $a_n = n^2$, $\forall n \in \mathbb{N}$.

Observación 3.5.2.3. Una sucesión no tiene por qué venir dada por un término general de manera explícita; en ocasiones, el término $n-$ésimo viene dado por sus predecesores. Por ejemplo, podemos encontrarnos una sucesión (a_n) tal que $a_n = na_{n-1}$, $\forall n \geq 1$. Podemos tratar de conocer un poco más en qué consiste esta sucesión. Para ello, como

$$a_n = n \cdot a_{n-1}$$

y como

$$a_{n-1} = (n-1)a_{n-2}$$

tenemos que

$$a_n = n(n-1)a_{n-2}$$

En un siguiente paso vemos que

$$a_n = n(n-1)(n-2)a_{n-3}$$

Del mismo modo llegamos a que

$$a_n = n(n-1)(n-2)\cdots 2 \cdot 1 \cdot a_0$$

Para conocer completamente cuáles son los términos de esta sucesión, al depender cada término solamente del inmediatamente anterior, necesitamos saber cuál es el primer elemento. Así, si $a_0 = 1$, el término general de esta sucesión será $a_n = n!$ Esta sucesión es un ejemplo de relación de recurrencia.

Definición 3.5.2.4. Una relación de recurrencia de orden r es la expresión del término $n-$ésimo de una sucesión en función de sus r términos precedentes. Matemáticamente, la escribimos

$$a_n = h(a_{n-1}, a_{n-2}, \ldots, a_{n-r})$$

Si se conocen los términos $a_0, a_1, \ldots, a_{r-1}$, se les llama condiciones iniciales de la recurrencia.

Definición 3.5.2.5. Una de las sucesiones más famosas es la sucesión de Fibonacci, consistente en que cada término de la sucesión se obtiene de sumar los dos términos anteriores. Esto define una relación de recurrencia de orden 2 dada por

$$f_n = f_{n-1} + f_{n-2}$$

Las condiciones iniciales de la recurrencia son $f_0 = f_1 = 1$.

Definición 3.5.2.6. Se dice que $g(n)$ es una solución de la relación de recurrencia si $a_n = g(n)$, $\forall n \in \mathbb{N}$.

Ejemplo 3.5.2.7. Para la sucesión dada por

$$\begin{cases} a_0 & = 1 \\ a_n & = na_{n-1}, \forall n \geq 1 \end{cases}$$

la solución es $a_n = n!$

Observación 3.5.2.8. En general, no existe un método para encontrar la solución de cualquier relación de recurrencia. En lo que sigue, veremos dos tipos de relaciones de recurrencia para las cuales sí que existen métodos para hayar su solución.

3.5.3. Relaciones de recurrencia homogéneas

Definición 3.5.3.1. Se dice que una relación de recurrencia de orden r es lineal si es de la forma

$$a_n = \sum_{i=1}^{r} c_i a_{n-i} + f(n) = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_r a_{n-r} + f(n)$$

donde $c_i \in \mathbb{R}$, $\forall i = 1, \ldots, r$ y $f(n)$ es una expresión dependiente de n e independiente de los términos a_i.

Si $f(n) = 0$, $\forall n$, se dice que la recurrencia lineal es homogénea.

Proposición 3.5.3.2 (Principio de superposición)**.** Sea $g_i(n)$ solución de

$$a_n = \sum_{i=1}^{r} c_i a_{n-i} + f_i(n),\ \forall i = 1,\ \ldots,\ k$$

Entonces, toda combinación lineal

$$\sum_{i=1}^{k} A_i g_i(n),\ A_i \in \mathbb{R},\ \forall i = 1,\ \ldots,\ k$$

es solución de

$$a_n = \sum_{i=1}^{r} c_i a_{n-i} + \sum_{i=1}^{k} A_i f_i(n)$$

En particular, si la relación de recurrencia lineal es homogénea, cualquier combinación lineal de las soluciones es, a su vez, solución de la recurrencia.

Podemos plantear una solución de la relación de recurrencia lineal homogénea

$$a_n = \sum_{i=1}^{r} c_i a_{n-i}$$

de la forma $a_n = x^n$. Veamos qué sucede si sustituimos esta expresión en la recurrencia:

$$x^n = \sum_{i=1}^{r} c_i x^{n-i} = c_1 x^{n-1} + c_2 x^{n-2} + \cdots + c_r x^{n-r}$$

Entonces, tenemos

$$x^n - c_1 x^{n-1} - c_2 x^{n-2} - \cdots - c_r x^{n-r} = 0$$

Como el término de menor grado es x^{n-r}, podemos sacarlo factor común y nos queda

$$x^{n-r}(x^r - c_1 x^{r-1} - c_2 x^{r-2} - \cdots - c_r) = 0$$

Una solución es $x = 0$, pero las soluciones que nos interesan son las de la ecuación

$$x^r - c_1 x^{r-1} - c_2 x^{r-2} - \cdots - c_r = 0$$

Definición 3.5.3.3. Dada una relación de recurrencia lineal homogénea

$$a_n = \sum_{i=1}^{r} c_i a_{n-i}$$

se define su ecuación característica como

$$x^r - \sum_{i=0}^{r} c_i x^{r-i} = 0$$

La ecuación característica tendrá r raíces, posiblemente repetidas. Es evidente que, si $x_1,\ \ldots,\ x_r$ son las r soluciones, entonces $a_n = x_i^n$ es solución de la recurrencia $\forall i = 1,\ \ldots,\ r$, pues hemos comenzado partiendo de la hipótesis de que una solución de la recurrencia tenía esta forma. Por tanto, por el principio de superposición, toda combinación lineal de estas soluciones es, a su vez, solución de la recurrencia.

El siguiente resultado nos indica cuál es la solución general de una relación de recurrencia lineal homogénea para la que las r raíces de la ecuación característica son reales y distintas.

Proposición 3.5.3.4. Sea una relación de recurrencia lineal homogénea

$$a_n = \sum_{i=1}^{r} c_i a_{n-i}$$

cuyas raíces x_1, x_2, ..., x_r de la ecuación característica asociada son reales y distintas entre sí. Entonces, toda solución general de la recurrencia es una combinación lineal de las raíces de la forma

$$\sum_{i=1}^{r} A_i x_i^n$$

Además, si son conocidas r condiciones iniciales consecutivas, a_k, a_{k+1}, ..., a_{k+r}, entonces se pueden conocer las constantes A_i y la solución será única.

Ejemplo 3.5.3.5. Sea la recurrencia

$$a_n = 5a_{n-1} - 6a_{n-2}$$

Queremos encontrar su solución general. Para ello obtenemos su ecuación característica

$$x^2 - 5x + 6 = 0$$

Las raíces de esta ecuación son $x_1 = 2$, $x_2 = 3$. Como son reales y distintas, por la proposición anterior, la solución general es $a_n = A \cdot 2^n + B \cdot 3^n$. Si tenemos como condiciones iniciales $a_0 = 1$, $a_1 = 0$, entonces:

$$a_0 = 1 = A2^0 + B3^0 = A + B \Leftrightarrow A + B = 1$$

$$a_1 = 0 = A \cdot 2^1 + B \cdot 3^1 \Leftrightarrow 2A + 3B = 0$$

Si resolvemos este sistema obtenemos como solución $A = 3$, $B = -2$. Por tanto, la solución de la recurrencia es $a_n = 3 \cdot 2^n - 2 \cdot 3^n$.

Ejercicio 3.5.3.6. Resolver la recurrencia

$$a_n = 9a_{n-2}$$

donde:

(i) $a_0 = 6$, $a_1 = 12$.

(ii) $a_3 = 324$, $a_4 = 486$

(iii) $a_0 = 6$, $a_2 = 54$

(iv) $a_0 = 6$, $a_2 = 10$

Estudiemos ahora el caso en que la ecuación característica tiene raíces repetidas, Digamos que t es una raíz de la ecuación característica de multiplicidad s (es decir, $(x-t)^s$ es factor de la ecuación característica). Entonces,

$$a_n = t^n(A_1 + A_2 n + \cdots + A_s n^{s-1})$$

es solución de la recurrencia, y se llama **solución básica** con respecto de t. La idea general de esto es que si t es raíz de multiplicidad s, entonces existe un polinomio $P(x)$ de grado $r - s$ tal que la ecuación característica se puede escribir como

$$(x-t)^s P(x) = 0$$

y las $s - 1$ sucesivas derivadas del lado izquierdo de la igualdad seguirán siendo 0.

En general, tenemos el siguiente resultado.

Proposición 3.5.3.7. Sea una relación de recurrencia lineal homogénea

$$a_n = \sum_{i=1}^{r} c_i a_{n-i}$$

cuyas raíces t_1, t_2, ..., t_l de la ecuación característica asociada son reales y tienen multiplicidad s_i, $\forall i = 1, \ldots, l$ y $\sum_{i=1}^{l} s_i = r$ (es decir, la suma de todas las multiplicidades es el grado de la ecuación característica). Entonces, la solución general de la recurrencia es combinación lineal de las soluciones básicas de la ecuación característica.

Ejemplo 3.5.3.8. Sea la recurrencia

$$a_n = 9a_{n-1} - 24a_{n-2} + 20a_{n-3}$$

para la cuál queremos saber su solución general. La ecuación característica asociada es

$$x^3 - 9x^2 + 24x - 20 = 0$$

Las soluciones de esta ecuación son $t_1 = 2$, de multiplicidad $s_1 = 2$, y $t_2 = 5$, de multiplicidad $s_2 = 1$. Entonces, la solución general de la recurrencia es $a_n = 2^n A + n2^n B + 5^n C$.

3.5.4. Relaciones de recurrencia no homogéneas

Consideremos una relación de recurrencia lineal no homogénea

$$a_n = \sum_{i=1}^{r} c_i a_{n-i} + f(n)$$

Denotemos $h_n = \sum_{i=1}^{r} c_i a_{n-i}$. Entonces la recurrencia se puede reescribir como $a_n = h_n + f(n)$. A $a_n = h_n$ se le llama **parte homogénea** de la recurrencia no homogénea. Si $a_n = u_n$ es la solución general de la parte homogénea y encontramos una solución particular $a_n = v_n$ de la recurrencia no homogénea, por el principio de superposición, $a_n = u_n + v_n$ es una solución general para la recurrencia no homogénea.

En general, no existe ningún método para encontrar una solución particular de la recurrencia no homogénea para cualquier $f(n)$. Sin embargo, para ciertos casos de $f(n)$.

Proposición 3.5.4.1. Sea una relación de recurrencia lineal no homogénea

$$a_n = h_n + f(n)$$

Entonces:

(i) Si $f(n) = ct^n$, con c constante, y t no es raíz de la ecuación característica asociada a $a_n = h_n$, se tiene que $v_n = At^n$. Mientras que si t sí es una raíz de multiplicidad s, se tiene que $v_n = An^s t^n$.

(ii) Si $f(n) = cn^k$, con c constante, y 1 no es raíz de la ecuación característica asociada a $a_n = h_n$, se tiene que $v_n = \sum_{i=0}^{k} A_i n^i$. Mientras que si 1 sí es una raíz de multiplicidad s, se tiene que $v_n = \sum_{i=0}^{k} A_i n^{s+i}$.

Ejemplo 3.5.4.2. Si la ecuación característica de una relación de recurrencia lineal no homogénea es

$$(x-1)^2(x-2)(x-3)^2 = 0$$

queremos encontrar la solución general de la recurrencia donde:

(i) $f(n) = 4n^3$

(ii) $f(n) = 5^n$

(iii) $f(n) = 4n^3 + 5^n$

Las soluciones de la ecuación característica son 1, de multiplicidad 2, 2, de multiplicidad 1, y 3, de multiplicidad 2. Así,

$$u_n = A_1 + A_2 n + A_3 2^n + A_4 3^n + A_5 n 3^n$$

(i) Si $f(n) = 4n^3$, como 1 es una raíz de la ecuación característica de multiplicidad 2, se tiene que la solución particular es

$$a_n = v_n = A_6 n^2 + A_7 n^3 + A_8 n^4 + A_9 n^5$$

Por tanto, la solución general será $a_n = u_n + v_n$.

(ii) Si $f(n) = 5^n$, como 5 no es una raíz de la ecuación característica, se tiene que la solución particular es

$$a_n = w_n = A_{10} 5^n$$

Por tanto, la solución general será $a_n = u_n + w_n$.

(iii) Si $f(n) = 4n^3 + 5^n$, por el principio de superposición, la solución particular de la relación de recurrencia es $a_n = v_n + w_n$. Por tanto, la solución general será $a_n = u_n + v_n + w_n$.

3.6. Cuestionario

Ejercicio 21. ¿Cuántas formas hay de sacar un as o un rey de una baraja española?

(a) 4

(b) 8

(c) 16

(d) 2

Ejercicio 22. En un tablero de ajedrez, 13 jugadores parten de una misma casilla que no se encuentra en un borde del tablero y, en el primer turno deben moverse a una de las 4 casillas adyacentes. Entonces, hay al menos una casilla con x o más jugadores. ¿Cuál es el valor de x?

(a) 1

(b) 2

(c) 3

(d) 4

Ejercicio 23. En un país muy supersticioso, un número de teléfono consta de 7 cifras de forma que la primera cifra tiene que ser entre un 4 y un 6. ¿Cuántos números distintos pueden formarse?

(a) $3 \cdot 10^6$

(b) 10^7

(c) $3 \cdot 10^7$

(d) 10^6

Ejercicio 24. En un centro de enseñanza se reciben solicitudes de ingreso, que se atienden según las calificaciones de Matemáticas, Física, Química e Inglés. Cada asignatura tiene una puntuación entera entre 5 y 10. ¿Cuántos expedientes académicos con diferentes puntuaciones se pueden recibir?

(a) $\dfrac{6!}{2!}$

(b) $\dfrac{6!}{4!2!}$

(c) 6^4

(d) 4^6

Ejercicio 25. En un centro de enseñanza se reciben solicitudes de ingreso, que se atienden según las calificaciones de Matemáticas, Física, Química e Inglés. Cada asignatura tiene una puntuación entera entre 5 y 10. ¿Cuántos expedientes académicos tienen una nota media de 7?

(a) $CR_{7,\,4}$

(b) $CR_{28,\,4}$

(c) $VR_{7,\,4}$

(d) $C_{7,\,4}$

Ejercicio 26. Sea $X = \{x_1, x_2, \ldots, x_n\}$ un conjunto con n elementos. Entonces,

$$|X \times X \times (X - \{x_1, x_2\})|$$

es igual a:

(a) n^3

(b) $n(n-1)(n-2)$

(c) $n^2(n-2)$

(d) $(n-2)^3$

Ejercicio 27. Si $n \geq 2$ y $k \in \{1, 2, \ldots, n-1\}$, entonces $\binom{n-1}{k-1} + \binom{n-1}{k}$ es igual a:

(a) $\binom{n}{k}$

(b) $\binom{n}{k-1}$

(c) $\binom{n}{k+1}$

(d) $\binom{n+1}{k}$

Ejercicio 28. $\binom{n}{k}\binom{k}{m}$ es igual a:

(a) $\binom{n}{m}\binom{m}{k-m}$

(b) $\binom{n}{n-k}\binom{k-m}{n-m}$

(c) $\binom{n+k}{k}\binom{n+m}{m}$

(d) $\binom{n}{m}\binom{n-m}{k-m}$

Ejercicio 29. ¿Cuánto vale la siguiente suma?

$$\sum_{k=0}^{10} \binom{10}{k}$$

(a) $\binom{10}{5}$

(b) 2^{10}

(c) 10^2

(d) $\binom{10}{2}$

Ejercicio 30. En las permutaciones circulares importa el orden.

(a) Verdadero

(b) Falso

Ejercicio 31. La ecuación característica asociada a la recurrencia

$$a_n = 3a_{n-3}$$

es

$$x^2 - 3 = 0$$

(a) Verdadero

(b) Falso

Ejercicio 32. La solución particular v_n de la recurrencia

$$a_n = 2a_{n-1} + 5 \cdot 4^n$$

es $An4^n$

(a) Verdadero

(b) Falso

Capítulo 4

Relaciones

4.1. Introducción

Una vez hemos visto qué son los conjuntos, cómo se operan y cómo contar elementos, es el turno de estudiar cómo se pueden relacionar los elementos de un mismo conjunto o entre conjuntos. En Matemáticas, Informática, Biología y en muchos otros ámbitos, las relaciones juegan un papel esencial, pues nos ayudan, por ejemplo, a clasificar o a ordenar.

En nuestro día a día estamos relacionando elementos constantemente: comparamos a dos personas y decimos si una es más alta que la otra o si son iguales, hablamos de mesas aunque no se parezcan en absoluto, clasificamos a las especies según unos rasgos comunes... Todos ellos son ejemplos de relaciones. En esta unidad estudiaremos cómo se define matemáticamente una relación, nos centraremos en dos tipos de relaciones: equivalencia y orden, y estudiaremos sus propiedades.

4.2. Relaciones binarias

4.2.1. Introducción

En esta sección veremos en qué consiste una relación, daremos los conceptos más generales sobre relaciones y veremos, dada una relación finita, cómo representarla tanto gráficamente como a través de matrices formadas por ceros y unos. Son conceptos muy básicos que convienen ser recordados para las siguientes secciones.

4.2.2. Conceptos elementales

Definición 4.2.2.1. Sean X e Y dos conjuntos. Se dice que $R \subseteq X \times Y$ es una relación (binaria) entre X e Y.

Ejemplo 4.2.2.2. Si $X = \{1, 2, 3\}$ e $Y = \{a, b\}$, entonces

$$R = \{(1, a), (2, a), (3, b)\}$$

es una relación.

Definición 4.2.2.3. Sea R una relación, y sea $(x, y) \in R$. Entonces, se dice que x está relacionado con y. También se suele denotar como xRy.

Observación 4.2.2.4. Las funciones también son relaciones. En efecto, una función no deja de ser una asignación de valores

$$\begin{aligned} f : X &\longrightarrow Y \\ x &\longmapsto f(x) \end{aligned}$$

Pero la asignación $x \mapsto f(x)$ también la podemos ver como el par $(x, f(x)) \in X \times Y$. Por tanto, una función es una relación

$$R = \{(x, f(x)) : x \in X\} \subseteq X \times Y$$

Observación 4.2.2.5. Muchas relaciones binarias están definidas sobre un único conjunto X (de hecho serán las que estudiemos). En estos casos, $R \subseteq X \times X = X^2$.

Una relación puede definirse de dos formas diferentes: de manera explícita o de manera implícita.

Una relación viene dada de manera explícita si se especifican todos sus elementos, como en el ejemplo 4.2.2.2. Una relación se define de manera implícita si se especifica la propiedad que cumplen los elementos para estar relacionados.

Ejemplo 4.2.2.6. Sobre $\mathbb{N}$ definimos la relación R de la siguiente forma:

$$nRm \Leftrightarrow n \leq m$$

Esta es una relación definida de manera implícita. Escrito de manera conjuntista, el conjunto R estaría definido por compresión como

$$R = \{(n, m) \in \mathbb{N}^2 : n \leq m\}$$

4.2.3. Representaciones de relaciones binarias finitas

Supongamos que tenemos un conjunto finito X y una relación R definida sobre él. Entonces, la relación podemos representarla utilizando una herramienta en la que profundizaremos en las dos últimas unidades: los grafos.

Definición 4.2.3.1. Sea $V = \{v_1, v_2, \ldots, v_n\}$ un conjunto y $E \subseteq V \times V$. Se llama grafo dirigido, o digrafo, al par $G = (V, E)$, donde V se conoce como conjunto de vértices, o nodos, y E conjunto de aristas.

Ejemplo 4.2.3.2. Sean

$$V = \{1, 2, 3, 4\}$$

y

$$E = \{(1, 1), (1, 2), (2, 1), (2, 3), (2, 4), (3, 1), (4, 1), (4, 2), (4, 4)\}$$

Entonces, $G = (V, E)$ es un grafo dirigido.

Observación 4.2.3.3. Observemos que en un grafo dirigido las aristas tienen un orden, no es lo mismo (v_i, v_j) que (v_j, v_i) si $i \neq j$. En la arista (v_i, v_j), a v_i se le llama vértice de salida, o partida, y a v_j vértice de entrada, o llegada, pues la arista parte de v_i y llega a v_j.

Un grafo dirigido se puede representar de manera gráfica utilizando círculos etiquetados con los nombres de los vértices y flechas entre círculos a modo de aristas con la punta de la flecha apuntando al vértice de entrada.

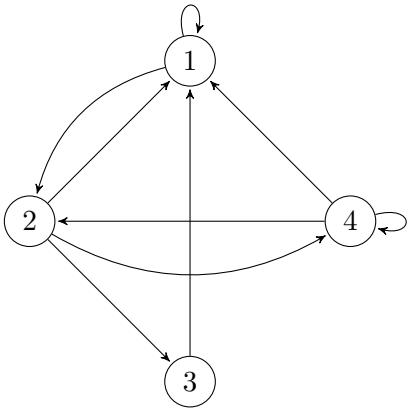
Ejemplo 4.2.3.4. Volviendo al grafo $G = (V, E)$, donde

$$V = \{1, 2, 3, 4\}$$

y

$$E = \{(1, 1), (1, 2), (2, 1), (2, 3), (2, 4), (3, 1), (4, 1), (4, 2), (4, 4)\}$$

lo representaríamos gráficamente como



Otra forma de representar un grafo dirigido es mediante una matriz llamada **matriz de adyacencia**. Veamos qué aspecto tiene:

Definición 4.2.3.5. Sea $G = (V, E)$ un grafo tal que $V = \{v_1, v_2, \ldots, v_n\}$. Entoces, podemos representar sus aristas (v_i, v_j) en una matriz, llamada matriz de adyacencia,

$$A = (a_{ij})_{i,j=1}^{n}$$

de tal forma que

$$a_{ij} = \begin{cases} 1 & (v_i, v_j) \in E \\ 0 & \text{otro caso} \end{cases}$$

Ejemplo 4.2.3.6. Siguiendo con nuestro grafo dado por

$$V = \{1, 2, 3, 4\}$$

y

$$E = \{(1, 1), (1, 2), (2, 1), (2, 3), (2, 4), (3, 1), (4, 1), (4, 2), (4, 4)\}$$

la matriz de adyacencia es

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

Observación 4.2.3.7.

(i) En una matriz de adyacencia aparecerá un 1 en la entrada $i-$ésima de la diagonal si y solo si el vértice v_i tiene una arista apuntando a él mismo. A estas aristas se les llama bucles.

(ii) Para un grafo no dirigido, su matriz de adyacencia no tiene por qué ser simétrica, como puede verse en el anterior ejemplo. Para que lo fuese sería necesario que tanto (v_i, v_j) como (v_j, v_i) pertenezcan a E.

Proposición 4.2.3.8. Si X es un conjunto finito y R es una relación definida sobre X, entonces la podemos representar como un grafo dirigido cuyo conjunto de vértices sea X y el conjunto de aristas sea R.

4.3. Relaciones de equivalencia

4.3.1. Introducción

Una relación de equivalencia es un tipo de relación binaria definida sobre un conjunto X que cumple una serie de propiedades que veremos a continuación. Se llaman de equivalencia porque relacionan objetos que, bajo la relación que se defina, son indistinguibles.

Supongamos que tenemos un conjunto X formado por todos los jugadores de la liga de fútbol española masculina. A este conjunto X pertenecen Benzema, Busquets, Joaquín, Iñaki Williams... Sobre X podemos definir la siguiente relación: dos jugadores, j_1 y j_2, están relacionados si y solo si juegan en el mismo equipo. Así, por ejemplo, Benzema y Modric están relacionados, ya que ambos juegan en el Real Madrid, pero Benzema y Busquets no lo están, pues Busquets juega en el Barcelona. Tal y como hemos definido esta relación, podemos observar tres propiedades que se cumplen:

(i) Un jugador siempre está relacionado consigo mismo. De trivial puede resultar confusa esta propiedad.

(ii) Si un jugador j_1 está relacionado con otro jugador j_2, entonces j_2 está relacionado con j_1, ya que si el primer jugador juega en el mismo equipo que el segundo, es evidente que el segundo jugador y el primero juegan en el mismo equipo.

(iii) Supongamos que j_1 juega en el mismo equipo que j_2, y que j_2 juega en el mismo equipo que j_3. Entonces, j_1 juega en el mismo que j_3.

Estas propiedades se llaman reflexiva, simétrica y transitiva, respectivamente y serán las que caractericen a las relaciones de equivalencia.

Nos podemos plantear qué jugadores están relacionados con un jugador dado. Por ejemplo, con Benzema aparecerían relacionados todos los jugadores del Real Madrid, pero ningún jugador de otro equipo. Análogamente, lo mismo ocurriría con Busquets y los jugadores del Barcelona, con Joaquín y los jugadores del Betis... Definamos el conjunto formado por todos los jugadores relacionados con Benzema, y denotémoslo [Benzema]. Este conjunto será:

$$[\text{Benzema}] = \{\text{Benzema, Modric, Courtois, Vinicius, Alaba, Kroos}, \ldots\}$$

Observemos que el conjunto es el mismo si en lugar de haber elegido a Benzema, hubiésemos elegido a cualquier otro jugador del conjunto. Eso es porque este conjunto no es otro que el propio Real Madrid. Si formásemos el conjunto [Busquets] habríamos obtenido el Barcelona. Y así con todos. En general, lo que obtenemos gracias a la relación que hemos definido sobre el

conjunto de jugadores de la liga es una partición del conjunto en los distintos equipos de la liga. A esto es a lo que llamaremos conjunto cociente y sobre el que trabajaremos a lo largo de la sección.

Este ejemplo introductorio recoge todos los conceptos clave de las relaciones de equivalencia y será conveniente volver a él una vez se haya estudiado la sección.

4.3.2. Conceptos elementales

Nota 4.3.2.1. En lo sucesivo, cada vez que trabajemos con relaciones de equivalencia, las denotaremos como $\sim$ en lugar de R.

Definición 4.3.2.2. Sea X un conjunto y $\sim$ una relación sobre X. Se dice que $\sim$ es una relación de equivalencia si satisface las siguientes propiedades:

(R) $\forall x \in X$, $x \sim x$.

(S) $\forall x, y \in X$, si $x \sim y$, entonces $y \sim x$.

(T) $\forall x, y, z \in X$, si $x \sim y$ e $y \sim z$, entonces $x \sim z$.

Estas propiedades se llaman reflexiva, simétrica y transitiva, respectivamente.

Ejemplo 4.3.2.3. Dados $n, m \in \mathbb{Z}$, definimos la relación

$$n \sim m \Leftrightarrow \exists k \in \mathbb{Z} \text{ tal que } n - m = 2k$$

Como todo número entero es par o impar, si la diferencia de dos enteros es un número par, esto quiere decir que los dos son pares o los dos son impares. Por lo tanto, significa que dos números están relacionados si y solo si ambos son pares o ambos son impares.

Queremos probar que es una relación de equivalencia. Para ello, veamos que se satisfacen las tres propiedades de la definición.

(R) $n \sim n$, ya que $n - n = 0$, y $0 = 2 \cdot 0$.

(S) Supongamos que $n \sim m$. Entonces, existe $k \in \mathbb{Z}$ tal que $n - m = 2k$. De esta igualdad deducimos que $m - n = -2k = 2(-k)$, y como $-k \in \mathbb{Z}$, entonces $m \sim n$.

(T) Supongamos $n_1 \sim n_2$ y $n_2 \sim n_3$. Entonces, existen k, $k' \in \mathbb{Z}$ tales que $n_1 - n_2 = 2k$ y $n_2 - n_3 = 2k'$. La técnica que vamos a utilizar ahora es muy frecuente en razonamientos de este tipo. Como queremos ver que existe un $\tilde{k} \in \mathbb{Z}$ tal que $n_1 - n_3 = 2\tilde{k}$, realizamos la siguiente operación:

$$n_1 - n_3 = n_1 - n_3 + n_2 - n_2 = (n_1 - n_2) + (n_2 - n_3)$$

Lo único que hemos hecho en el primer paso es sumar y restar el término n_2, que conserva la identidad pero introduce información valiosa. Luego hemos agrupado términos para que resulte más fácil operar y aplicar la hipótesis de la que partimos.

$$(n_1 - n_2) + (n_2 - n_3) = 2k + 2k' = 2(k + k')$$

Como $k + k' \in \mathbb{Z}$, lo llamamos $\tilde{k}$ y así tenemos que $n_1 - n_3 = 2\tilde{k}$. Por tanto, $n_1 \sim n_3$.

Al cumplirse todas las propiedades, concluimos que esta es una relación de equivalencia.

Observación 4.3.2.4. No toda relación es de equivalencia. Veamos algunos ejemplos:

(i) Sobre $\mathbb{N}$,
$$n \sim m \Leftrightarrow n < m$$
no cumple las propiedades reflexiva ni simétrica.

(ii) En el famoso juego piedra-papel-tijeras, la relación dada por: tijeras gana a papel, papel gana a piedra y piedra gana a tijeras no cumple ninguna de las tres propiedades.

(iii) La relación del ejemplo 4.3.2.3 modificada como
$$n \sim m \Leftrightarrow \exists k \in \mathbb{N} \text{ tal que } n - m = 2k$$
no es de equivalencia, ya que no cumple la propiedad simétrica.

Definición 4.3.2.5. Sea X un conjunto sobre el que se define una relación de equivalencia $\sim$ y sea $x \in X$. Se define la clase de equivalencia de x, y se denota $[x]$, como el conjunto formado por todos los elementos relacionados con x. Escrito de otra forma,
$$[x] = \{y \in X \, : \, x \sim y\}$$

Proposición 4.3.2.6. Sea X un conjunto sobre el que se define una relación de equivalencia $\sim$ y sean x, $y \in X$ tales que $x \sim y$. Entonces, $[x] = [y]$. A x se le llama representante de la clase.

Ejemplo 4.3.2.7. Ya hemos visto en el ejemplo 4.3.2.3 que la relación dada por
$$n \sim m \Leftrightarrow \exists k \in \mathbb{Z} \text{ tal que } n - m = 2k$$
es de equivalencia. Nos planteamos estudiar algunas clases de equivalencia. Por ejemplo, la clase del 0 es
$$[0] = \{n \in \mathbb{Z} \, : \, \exists k \in \mathbb{Z} \text{ tal que } n - 0 = 2k\} =$$
$$\{n \in \mathbb{Z} \, : \, \exists k \in \mathbb{Z} \text{ tal que } n = 2k\}$$
Es decir, son todos los números enteros pares. Por tanto,
$$\ldots = [-4] = [-2] = [0] = [2] = [4] = \ldots$$
por la proposición anterior.

La clase del 1 es
$$[1] = \{n \in \mathbb{Z} \, : \, \exists k \in \mathbb{Z} \text{ tal que } n - 1 = 2k\} =$$
$$\{n \in \mathbb{Z} \, : \, \exists k \in \mathbb{Z} \text{ tal que } n = 2k + 1\}$$
Es decir, son todos los números enteros impares. Por tanto,
$$\ldots = [-3] = [-1] = [1] = [3] = \ldots$$
De esta forma, podemos concluir que, salvo el representante elegido, las únicas clases de equivalencia para esta relación son $[0]$ y $[1]$.

Este ejemplo da pie a la siguiente definición.

Definición 4.3.2.8. Sea X un conjunto sobre el que se define una relación de equivalencia $\sim$. Se define el conjunto cociente, y se denota $\frac{X}{\sim}$, como el conjunto formado por todas las clases de equivalencia, es decir

$$\frac{X}{\sim} = \{[x] \,:\, x \in X\}$$

Ejemplo 4.3.2.9. Siguiendo con los ejemplos anteriores, dada la relación

$$n \sim m \Leftrightarrow \exists k \in \mathbb{Z} \text{ tal que } n - m = 2k$$

se tiene que

$$\frac{\mathbb{Z}}{\sim} = \{[0],\, [1]\}$$

Ejemplo 4.3.2.10. Sobre $\mathbb{Z}^2$ se define la relación

$$(n_1,\, m_1) \sim (n_2,\, m_2) \Leftrightarrow 2(n_1 - n_2) = 5(m_1 - m_2)$$

(i) Comprobar que es una relación de equivalencia.

(ii) Dar tres elementos de la clase $[(2,\, -3)]$. ¿Cuántos elementos hay en dicha clase?

(iii) ¿Cuál es el conjunto cociente?

(i) Veamos primero que, efectivamente, es una relación de equivalencia.

(R) $(n,\, m) \sim (n,\, m)$, pues

$$2(n - n) = 0 = 5(m - m)$$

(S) Supongamos que $(n_1,\, m_1) \sim (n_2,\, m_2)$. Entonces,

$$2(n_2 - n_1) = -2(n_1 - n_2) = -5(m_1 - m_2) = 5(m_2 - m_1)$$

Por tanto, $(n_2,\, m_2) \sim (n_1,\, m_1)$.

(T) Supongamos que $(n_1,\, m_1) \sim (n_2,\, m_2)$ y que $(n_2,\, m_2) \sim (n_3,\, m_3)$. Entonces,

$$2(n_1 - n_3) = 2(n_1 - n_2 + n_2 - n_3) = 2(n_1 - n_2) + 2(n_2 - n_3) =$$

$$5(m_1 - m_2) + 5(m_2 - m_3) = 5(m_1 - m_2 + m_2 - m_3) = 5(m_1 - m_3)$$

Por tanto, $(n_1,\, m_1) \sim (n_3,\, m_3)$.

De esta forma, hemos demostrado que se trata de una relación de equivalencia.

(ii) La clase de equivalencia del $(2,\, -3)$ es el conjunto de elementos de $\mathbb{Z}^2$ relacionados con él. Es decir,

$$[(2,\, -3)] = \{(n,\, m) \in \mathbb{Z}^2 \,:\, 2(n - 2) = 5(m - (-3))\}$$

Hagamos algunas cuentas para saber quién es este conjunto.

$$2(n - 2) = 5(m - (-3)) \Leftrightarrow 2n - 4 = 5m + 15 \Leftrightarrow 2n - 5m = 19$$

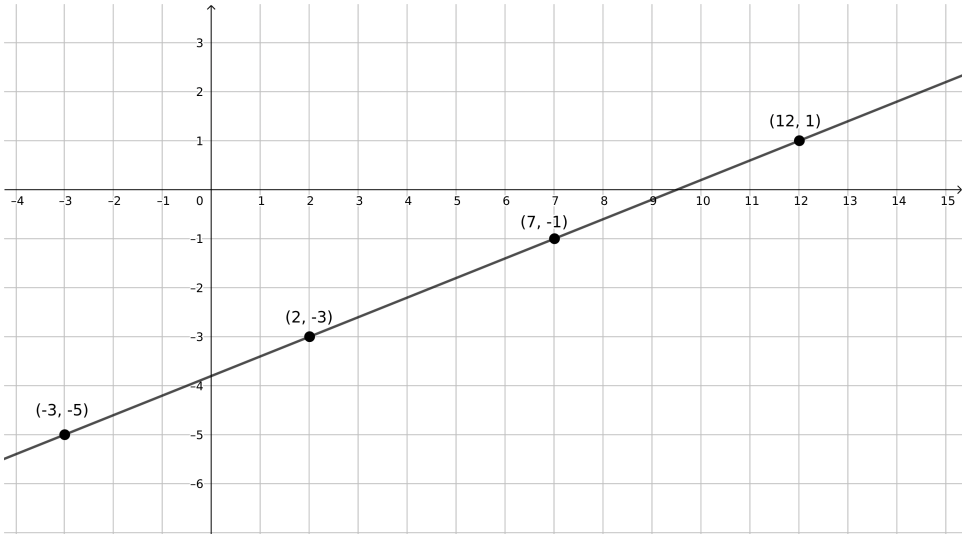
O también,

$$m = \frac{2n - 19}{5}$$

Por tanto,

$$[(2,\, -3)] = \{(n,\, m) \in \mathbb{Z}^2 \,:\, 2n - 5m = 19\}$$

Esta es la ecuación de una recta del plano. Algunos puntos de $\mathbb{Z}^2$ sobre esta recta son:



Se aprecia que las soluciones enteras de esta ecuación son de la forma

$$(n,\, m) = (2 + 5k,\, 2k - 3),\, \forall k \in \mathbb{Z}$$

Por tanto, hay infinitos elementos en $[(2,\, -3)]$, uno por cada k.

(iii) El conjunto cociente $\frac{\mathbb{Z}^2}{\sim}$ es el conjunto formado por todas las clases de equivalencia $[(a,\, b)]$, para $(a,\, b) \in \mathbb{Z}^2$. Así que, hay que ver cómo es la clase de equivalencia de un punto genérico $(a,\, b)$ del plano entero $\mathbb{Z}^2$. Para ello, procedemos de la misma forma que en el apartado anterior para $(2,\, -3)$.

$$[(a,\, b)] = \{(n,\, m) \in \mathbb{Z}^2 \,:\, 2(n - a) = 5(m - b)\}$$

Operando,

$$2(n - a) = 5(m - b) \Leftrightarrow 2n - 2a = 5m - 5b \Leftrightarrow 2n - 5m = 2a - 5b$$

O también,

$$m = \frac{2n - (2a - 5b)}{5}$$

Por tanto,

$$[(a,\, b)] = \{(n,\, m) \in \mathbb{Z}^2 \,:\, 2n - 5m = 2a - 5b\}$$

Finalmente,

$$\frac{\mathbb{Z}^2}{\sim} = \{[(a,\, b)] \,:\, (a,\, b) \in \mathbb{Z}^2\}$$

Ya hemos visto que las clases de equivalencia son los puntos del plano entero sobre las rectas que nos han aparecido, pero observemos que dadas dos rectas

$$Ax + By = C,\, Ax + By = D$$

estas son paralelas, y que serán iguales si y solo si $C = D$. Por tanto, la relación de equivalencia nos divide el plano en rectas paralelas a la recta de la gráfica anterior.

Ejercicio 4.3.2.11. Sobre $\mathbb{R}^2$ se define la relación

$$(x_1,\, y_1) \sim (x_2,\, y_2) \Leftrightarrow x_1^2 - x_2^2 = \frac{9}{4}(y_2^2 - y_1^2)$$

(i) Demostrar que es una relación de equivalencia.

(ii) Analizar cuál es la clase $[(0, 2)]$ y qué representa geométricamente. Dibujarla.

(iii) ¿Cuál es el conjunto $\frac{\mathbb{R}^2}{\sim}$?

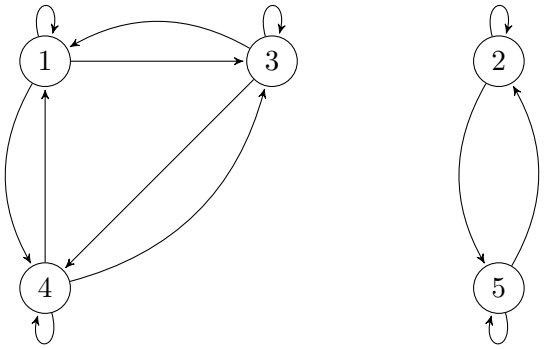
4.3.3. Relaciones de equivalencia, grafos y particiones

Ya hemos visto en esta unidad cómo representar relaciones sobre conjuntos finitos mediante grafos. Ahora vamos a ver qué tienen de especiales los grafos asociados a las relaciones de equivalencia. Terminaremos esta sección con una caracterización de las particiones de un conjunto como relaciones de equivalencia.

Sea $X = \{1, 2, 3, 4, 5\}$ y definamos sobre X la siguiente relación, que se puede demostrar que es de equivalencia:

$R = \{(1, 1), (1, 3), (1, 4), (2, 2), (2, 5), (3, 1), (3, 3), (3, 4), (4, 1), (4, 3), (4, 4), (5, 2), (5, 5)\}$

Si dibujamos su grafo asociado nos queda lo siguiente:



En este grafo podemos observar varias características:

(i) Cada vértice tiene un bucle. Esto significa que cada vértice está relacionado consigo mismo, por lo que es equivalente a afirmar que se satisface la propiedad reflexiva.

(ii) Para cada arista (i, j) existe una arista (j, i). En términos coloquiales, toda arista de ida tiene una arista de vuelta. Esta propiedad es equivalente a la propiedad simétrica.

(iii) Para todo par de aristas (i, j) y (j, k), existe una arista (i, k). En términos coloquiales, si existe una arista de i a j y una arista de j a k, entonces existe una arista que ataja de i a k.

Todo grafo que reúna estas tres propiedades representará a una relación de equivalencia, como es este caso.

(iv) Existen dos conjuntos de vértices, $\{1, 3, 4\}$ y $\{2, 5\}$, *disconexos* entre sí, es decir, que no existen aristas entre los vértices de uno y otro conjunto. Esto representa que el conjunto cociente está formado por dos clases de equivalencia:

$$[1] = \{1, 3, 4\},\ [2] = \{2, 5\}$$

El ejemplo anterior podemos generalizarlo a cualquier conjunto finito.

Proposición 4.3.3.1. Dado cualquier conjunto finito sobre el que se ha definido una relación, si su grafo asociado satisface las propiedades (i), (ii) y (iii), se tiene que la relación es de equivalencia. Además, las clases de equivalencia del conjunto cociente serán aquellos conjuntos de vértices como en la propiedad (iv).

Volvamos al ejemplo anterior. Si escribimos la matriz de adyacencia, esta queda

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

De nuevo, podemos observar las siguientes características:

(i') Toda entrada de la diagonal es 1. Esto quiere decir que todo vértice está relacionado consigo mismo, por lo que es equivalente a la propiedad reflexiva.

(ii') Cada entrada (i, j) es igual a (j, i), es decir, la matriz es simétrica. Esto implica que se satisface la propiedad simétrica.

(iii') Si la entrada (i, j) es 1 y la entrada (j, k) es igual a 1, entonces la entrada (i, k) es 1. Computacionalmente, es la propiedad más costosa de calcular. Esta propiedad es equivalente a la propiedad transitiva.

Toda matriz cuadrada formada por ceros y unos que reúna estas tres propiedades representará a una relación de equivalencia.

(iv') Existen dos conjuntos de filas (o columnas), de forma que en cada conjunto las filas son iguales y dada una fila de cada conjunto, son distintas. Además, estas tienen la particularidad de que los unos de la fila de un conjunto son ceros en la fila del otro conjunto y viceversa, pero esto solo sucede porque solo hay dos conjuntos de filas. De nuevo, esto representa que el conjunto cociente está formado por dos clases de equivalencia.

Proposición 4.3.3.2. Dada una matriz de adyacencia asociada a un conjunto finito sobre el que se ha definido una relación, si la matriz satisface las propiedades (i'), (ii') y (iii'), se tiene que la relación es de equivalencia. Además, las clases de equivalencia del conjunto cociente serán aquellos conjuntos de filas como en la propiedad (iv').

Proposición 4.3.3.3. Sea X un conjunto, y sea $P = \{X_i \in \mathcal{P}(X) : i \in I\}$ una partición de X[1] Entonces, esta partición define, de manera natural, una relación de equivalencia sobre X.

Demostración. Antes de comenzar con la demostración, observemos que cada conjunto X_i no comparte ningún otro elemento con el resto de conjuntos de la partición, y que la unión de todos los conjuntos X_i forma el conjunto X. Por ello, cada X_i representará una clase de equivalencia, y la familia de conjuntos de la partición será el conjunto de todas las clases de equivalencia, luego será el conjunto cociente. Así, de manera natural, dados $x, y \in X$, podemos definir la relación

$$x \sim y \Leftrightarrow \text{ tanto } x \text{ como } y \text{ pertenecen a } X_i, \text{ con } X_i \in P$$

[1]Recordemos que una partición de X es una familia de subconjuntos de X disjuntos entre sí y cuya unión es X.

Es decir, dos elementos están relacionados si y solo si pertenecen al mismo conjunto de la partición P. Comprobemos que, efectivamente, esta es una relación de equivalencia:

(R) $x \sim x$, ya que $x \in X \Leftrightarrow x \in X$.

(S) Supongamos que $x \sim y$. Entonces, está claro que tanto y como x pertenecen al mismo conjunto de P, por lo que $y \sim x$.

(T) Si $x \sim y$, entonces $x, y \in X_i$. Por otra parte, si $y \sim z$, entonces $y, z \in X_j$. Pero como $X_i \cap X_j = \emptyset$ si y solo si $i \neq j$, entonces se tiene que $X_i = X_j$ y, de este modo, $x, z \in X_i$. Por tanto, $x \sim z$.

Podemos concluir que esta relación es de equivalencia. □

También se tiene el recíproco de esta proposición.

Proposición 4.3.3.4. Sea X un conjunto sobre el que está definida una relación de equivalencia $\sim$. Entonces, esta relación define, de manera natural, una partición de X.

Demostración. La demostración es muy sencilla. Llamemos

$$P = \frac{X}{\sim}$$

Por el recíproco de la proposición 4.3.2.6, sabemos que las clases de equivalencia son disjuntas entre sí y, como cada elemento de X pertenece a una única clase de equivalencia, al unir todos los elementos de P, el resultado es X. Por tanto, P es una partición de X. □

4.4. Relaciones de orden

4.4.1. Introducción

Comparar es una actividad habitual en nuestro día a día. Utilizamos diversos criterios como el tamaño, el color o el orden alfabético (lexicográfico) para comparar y ordenar elementos. En esta sección veremos que el orden es un tipo de relación, que existen varios tipos de relaciones de orden y estudiaremos sus propiedades. Finalmente, veremos cómo representar gráficamente las relaciones de orden definidas sobre un conjunto finito.

Pensemos en estas dos relaciones definidas sobre $\mathbb{N}$:

(i) $n < m$

(ii) $n \leq m$

Ya hemos comentado que $<$ es una relación que no satisface las propiedades reflexiva ni simétrica, pero sí la transitiva. Sin embargo, $\leq$ sí que satisface la propiedad reflexiva además de la transitiva, pero la propiedad simétrica solo la satisface si y solo si $n = m$. Esto ejemplifica que existen diferentes tipos de relaciones de orden.

4.4.2. Órdenes parciales y orden total

Nota 4.4.2.1. Una relación de orden la denotaremos como $\preceq$ si es de orden no estricto y $\prec$ si el orden es estricto.

Definición 4.4.2.2. Sea X un conjunto. Decimos que una relación $\preceq$ definida sobre X es de orden parcial no estricto, o, directamente, orden parcial, si se satisfacen las siguientes propiedades:

(i) $x \preceq x$, $\forall x \in X$.

(ii) Si $x \preceq y$ e $y \preceq x$, entonces $x = y$, $\forall x, y \in X$.

(iii) Si $x \preceq y$ e $y \preceq z$, entonces $x \preceq z$, $\forall x, y, z \in X$.

La primera propiedad es la reflexiva y la tercera es la transitiva, que ya conocemos. La segunda propiedad se llama antisimétrica.

Al par $(X, \preceq)$ se le llama conjunto parcialmente ordenado no estricto, o, directamente, conjunto parcialmente ordenado.

Ejemplo 4.4.2.3.

(i) $(\mathbb{R}, \leq)$ es un conjunto parcialmente ordenado.

(ii) Sea X un conjunto no vacío. Entonces, $(\mathcal{P}(X), \subseteq)$ es un conjunto parcialmente ordenado. Veámoslo:

(R) Sea $A \in \mathcal{P}(X)$. Entonces, $A \subseteq A$ trivialmente.

(An) Sean A, $B \in \mathcal{P}(X)$ tales que $A \subseteq B$ y $B \subseteq A$. Como en el tema de conjuntos vimos que dos conjuntos eran iguales si y solo si se daba la doble inclusión, concluimos que $A = B$.

(T) Sean A, B, $C \in \mathcal{P}(X)$ tales que $A \subseteq B$ y $B \subseteq C$. Entonces, es evidente que $A \subseteq B \subseteq C$, luego $A \subseteq C$.

(iii) Sea $\mathbb{N}^+ = \mathbb{N} - \{0\}$, y sean n, $m \in \mathbb{N}^+$. Decimos que n divide a m, y lo denotamos $n|m$, si existe $k \in \mathbb{N}^+$ tal que $m = kn$. En terminos coloquiales, n divide a m si $\frac{m}{n}$ es una división exacta.

$(\mathbb{N}^+, |)$ es un conjunto parcialmente ordenado. Vamos a demostrarlo:

(R) $n|n$, ya que $n = 1n$.

(An) Si $n|m$ y $m|n$ entonces existen k_1, $k_2 \in \mathbb{N}^+$ tales que $m = k_1 n$ y $n = k_2 m$. Entonces, $n = k_2 k_1 n$, pero como k_1, $k_2 \geq 1$, se tiene que $k_1 = k_2 = 1$, luego $n = m$.

(T) Supongamos que $n|m$ y $m|r$. Entonces, existen k_1, $k_2 \in \mathbb{N}^+$ tales que $m = k_1 n$ y $r = k_2 m$. Por tanto, $r = k_2 k_1 n$. Si llamamos $k = k_2 k_1$, hemos encontrado $k \in \mathbb{N}^+$ tal que $r = kn$, luego $n|r$.

Observación 4.4.2.4. Que un conjunto sea parcialmente ordenado no quiere decir que todo elemento pueda compararse entre sí. Por ejemplo, si $X = \{1, 2\}$, en $(\mathcal{P}(X), \subseteq)$ se tiene que $\{1\} \not\subseteq \{2\}$ y $\{2\} \not\subseteq \{1\}$.

Proposición 4.4.2.5. Sea $(X, \preceq)$ un conjunto parcialmente ordenado, y sea $A \subseteq X$. Entonces, $(A, \preceq)$ es un conjunto parcialmente ordenado.

Definición 4.4.2.6. Sea $(X, \preceq)$ un conjunto parcialmente ordenado. Se dice que $\preceq$ es una relación de orden total, o lineal, si satisface la propiedad de comparación:

$$x \preceq y \vee y \preceq x, \forall x, y \in X$$

Si $\preceq$ es una relación de orden total, se dice que $(X, \preceq)$ es un conjunto totalmente ordenado.

Ejemplo 4.4.2.7.

(i) $(\mathbb{R}, \leq)$ es un conjunto totalmente ordenado.

(ii) Sea X un conjunto no vacío. Entonces $(\mathcal{P}(X), \subseteq)$ no es un conjunto totalmente ordenado por lo visto en la observación 4.4.2.4.

(iii) $(\mathbb{N}^+, |)$ no es un conjunto totalmente ordenado. Por ejemplo, $2 \nmid 3$ y $3 \nmid 2$.

Proposición 4.4.2.8. Sea $(X, \preceq)$ un conjunto totalmente ordenado, y sea $A \subseteq X$. Entonces, $(A, \preceq)$ es un conjunto totalmente ordenado.

Definición 4.4.2.9. Sea X un conjunto. Decimos que una relación $\prec$ definida sobre X es de orden parcial estricto si se satisfacen las siguientes propiedades:

(i) $x \not\prec x, \forall x \in X$.

(ii) Si $x \prec y$, entonces $y \not\prec x, \forall x, y \in X$.

(iii) Si $x \prec y$ e $y \prec z$, entonces $x \prec z, \forall x, y, z \in X$.

La tercera propiedad es la transitiva. La primera propiedad se llama irreflexiva y la segunda se llama asimétrica.

Si $\prec$ es una relación de orden parcial estricto sobre X, al par $(X, \prec)$ se le llama conjunto parcialmente ordenado estricto.

Ejemplo 4.4.2.10.

(i) $(\mathbb{R}, <)$ es un conjunto parcialmente ordenado estricto.

(ii) Sean A, B dos conjuntos. Decimos que A es un subconjunto estricto de B, y lo denotamos como $A \subsetneq B$, si $A \subseteq B$ y $A \neq B$.

Sea X un conjunto no vacío. Entonces, $(\mathcal{P}(X), \subsetneq)$ es un conjunto parcialmente ordenado estricto.

Proposición 4.4.2.11. Sea $(X, \prec)$ un conjunto parcialmente ordenado estricto, y sea $A \subseteq X$. Entonces, $(A, \prec)$ es un conjunto parcialmente ordenado estricto.

4.4.3. Cotas superiores e inferiores

Definición 4.4.3.1. Dado un conjunto parcialmente ordenado $(X, \preceq)$, se dice que $M \in X$ es un elemento maximal si para todo $x \in X$ tal que $M \preceq x$ se tiene que $x = M$. Es decir, es un elemento del conjunto que siempre es mayor o igual que todos aquellos elementos del conjunto con los que se puede comparar.

Análogamente, se dice que $m \in X$ es un elemento minimal si para todo $x \in X$ tal que $x \preceq m$ se tiene que $x = m$.

Observación 4.4.3.2. Los maximales y los minimales pueden no ser únicos.

Ejemplo 4.4.3.3. Sea $X = \{a, b, c, d, e, f, g\}$ y la siguiente relación de orden parcial:

$$a \preceq a,\ a \preceq c,\ a \preceq d,\ a \preceq f,\ a \preceq g,\ b \preceq b,\ b \preceq e,\ b \preceq g,$$

$$c \preceq c,\ c \preceq f,\ d \preceq d,\ d \preceq f,\ d \preceq g,\ e \preceq e,\ e \preceq g,\ f \preceq f,\ g \preceq g$$

Entonces, existen dos elementos maximales: f y g; y existen dos elementos minimales a y b.

Ejercicio 4.4.3.4. Sea $A = [0, 1] \times [0, 1] \subseteq \mathbb{R}^2$, y definamos la relación

$$(x_1, y_1) \preceq (x_2, y_2) \Leftrightarrow x_1 \leq x_2 \text{ e } y_1 \leq y_2$$

Comprobar que es una relación de orden parcial pero no total. ¿Cuáles son los elementos maximales? ¿Y minimales?

Proposición 4.4.3.5. Todo conjunto finito parcialmente ordenado tiene, al menos, un maximal y un minimal.

Definición 4.4.3.6. Dado un conjunto parcialmente ordenado $(X, \preceq)$, se dice que M es una cota superior de X si $x \preceq M$ para todo $x \in X$. Es decir, es un que es mayor o igual que todos los elementos del conjunto.

Análogamente, se dice que m es una cota inferior de X si $m \preceq x$ para todo $x \in X$.

Observación 4.4.3.7. Una cota superior o inferior no tiene por qué ser un elemento del conjunto. Por ejemplo, para el intervalo $[0, 1]$, una cota superior es 1, que sí es un elemento del conjunto, pero también lo son 2, π y 10.

Definición 4.4.3.8. Dado un conjunto parcialmente ordenado $(X, \preceq)$, se dice que $M \in X$ es un máximo si $x \preceq M$ para todo $x \in X$. Es decir, es un elemento del conjunto que es mayor o igual que el resto de elementos. Se denota $\max X$.

Análogamente, se dice que $m \in X$ es un mínimo si $m \preceq x$ para todo $x \in X$. Se denota $\min X$.

Observación 4.4.3.9. La diferencia entre maximal y máximo (de igual modo minimal y mínimo) radica en que un maximal es mayor o igual que todos los elementos comparables con él, mientras que el máximo es mayor o igual que todos los elementos. Esto implica que el máximo es un elemento comparable con todos los del conjunto y, además, que es único. También podríamos decir que es una cota superior del conjunto que pertenece al conjunto.

Podemos concluir que si un elemento es máximo, entonces es maximal, pero no el recíproco.

Ejemplo 4.4.3.10. El conjunto del ejemplo 4.4.3.3 no tiene máximo ni mínimo. Sin embargo, si añadimos al conjunto los elementos h e i de forma que $h \preceq x$, $\forall x \in \{a, b, c, d, f, g, h, i\}$, $x \preceq i$, $\forall x \in \{a, b, c, d, f, g, h, i\}$, entonces el mínimo es h y el máximo es i.

Definición 4.4.3.11. Dado un conjunto parcialmente ordenado $(X, \preceq)$, se dice que M es el supremo de X si, para todo u tal que $x \preceq u$, para todo $x \in X$, se tiene que $M \preceq u$, . Es decir, es la menor de todas las cotas superiores de X. Se denota $\sup X$.

Análogamente, se dice que m es el ínfimo de X si, para todo l tal que $l \preceq x$, para todo $x \in X$, se tiene que $l \preceq m$. Se denota $\text{ínf}\, X$.

Observación 4.4.3.12. La diferencia entre máximo y supremo (de igual modo mínimo e ínfimo) consiste en que el supremo no necesita pertenecer al conjunto. Por tanto, si un elemento es máximo, entonces es supremo, pero no se tiene el recíproco.

Proposición 4.4.3.13. Sea $X \subseteq \mathbb{N}^+$ un conjunto finito y consideremos el conjunto parcialmente ordenado $(X, |)$. Entonces:

(i) El conjunto de cotas superiores de X es el conjunto formado por los múltiplos de los maximales de X. Además, $\sup X$ es el mínimo común múltiplo de los maximales.

(ii) El conjunto de cotas inferiores de X es el conjunto formado por los divisores de los minimales de X. Además, $\text{ínf}\, X$ es el máximo común divisor de los minimales.

Demostración.

(i) Sea M_1 el conjunto de maximales de X, y sea a un número múltiplo de todos los elementos de M_1. Por definición de divisibilidad, para todo $x \in M_1$ se tendrá que $x \,|\, a$. Por otra parte, como cada elemento de X es menor o igual que alguno de los maximales, se sigue que $x \,|\, a$, $\forall x \in X$, luego a es una cota superior de X. Además, el mínimo común múltiplo de dos o más números se define como el múltiplo más pequeño de todos estos números. Como los múltiplos de los maximales son las cotas superiores de X, el mínimo común múltiplo es la menor de todas ellas. Por tanto, el mínimo común múltiplo es el supremo de X.

(ii) El razonamiento es completamente análogo.

□

Ejemplo 4.4.3.14. Sea $X = \{2, 3, 4, 6, 12, 15, 24, 90, 180\}$ y consideremos el conjunto parcialmente ordenado $(X, |)$.

(i) El conjunto de cotas inferiores de X es $A = \{1\}$, ya que es el conjunto de divisores de sus minimales, 2 y 3. Por tanto, $\text{ínf}\, X = 1$.

(ii) Como los maximales de X son 24 y 180, el conjunto de cotas superiores de X es el conjunto formado por todos los números que son múltiplos de 24 y 180. Si factorizamos ambos números nos queda $24 = 2^3 \cdot 3$ y $180 = 2^2 \cdot 3^2 \cdot 5$. Así, el conjunto de cotas superiores es

$$B = \{2^3 \cdot 3^2 \cdot 5k \,:\, k \in \mathbb{N}^+\} = \{360k \,:\, k \in \mathbb{N}^+\}$$

Por tanto, $\sup X = 360$.

Proposición 4.4.3.15. Sea $(X, \preceq)$ un conjunto finito parcialmente ordenado que tiene máximo (respectivamente mínimo) x_0. Entonces, $\sup X = x_0$ (respectivamente $\text{ínf}\, X = x_0$).

Proposición 4.4.3.16. Sea X un conjunto no vacío y consideremos el conjunto parcialmente ordenado $(\mathcal{P}(X), \subseteq)$. Entonces:

(i) $\sup \mathcal{P}(X) = X$.

(ii) $\inf \mathcal{P}(X) = \emptyset$.

4.4.4. Diagramas de Hasse

Sea $X = \{2, 3, 4, 6, 12, 15, 24, 90, 180\}$ el conjunto del ejercicio 4.4.3.14, y consideremos el conjunto parcialmente ordenado $(X, |)$.

(i) Llamemos nivel 0, N_0, al conjunto de minimales de X. Por tanto,

$$N_0 = \{2, 3\}$$

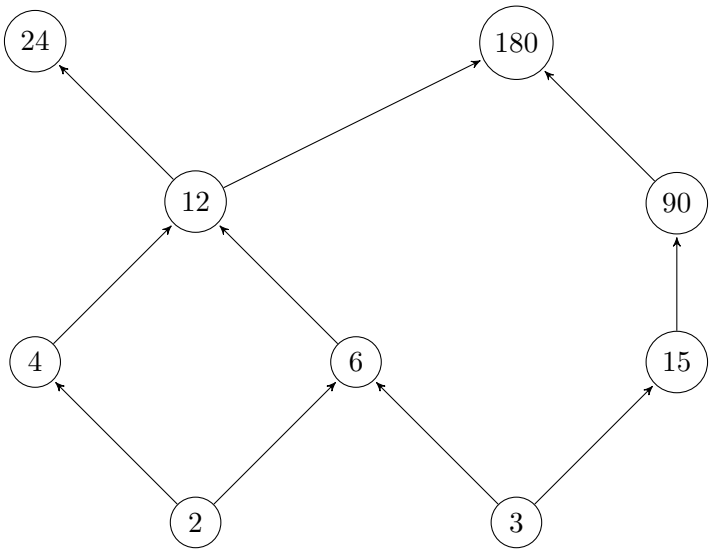
(ii) Llamemos nivel 1, N_1, al conjunto de minimales de $X - N_0$. Por tanto,

$$N_1 = \{4, 6, 15\}$$

(iii) Si repetimos el proceso, llegaremos a los siguientes niveles:

$$N_2 = \{12, 90\},\ N_3 = \{24, 180\}$$

Vamos a considerar a los elementos de X como vértices, los vamos a situar por niveles y vamos a unir los vértices x de un nivel con los vértices y del siguiente nivel mediante aristas en caso de que $x \,|\, y$. En nuestro ejemplo:



A esto es a lo que se conoce como **diagrama de Hasse**. En general, para dibujar un diagrama de Hasse necesitamos un conjunto finito parcialmente ordenado.

Proposición 4.4.4.1. Sea $(X, \preceq)$ un conjunto finito parcialmente ordenado cuyo diagrama de Hasse llega hasta el nivel N_r. Entonces:

(i) Los minimales de X se encuentran en el nivel N_0 de su diagrama de Hasse asociado, y los maximales se encuentran en el nivel N_r.

(ii) X tiene mínimo si y solo si existe un único vértice en el nivel N_0 del diagrama.

(iii) X tiene máximo si y solo si existe un único vértice en el nivel N_r del diagrama.

Proposición 4.4.4.2. Sea $(X, \preceq)$ un conjunto totalmente ordenado. Entonces, en cada nivel de su diagrama de Hasse asociado hay un único vértice.

4.5. Cuestionario

Ejercicio 33. La matriz

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

representa una relación de equivalencia.

(a) Verdadero

(b) Falso

Ejercicio 34. Sobre $\mathbb{R}$, la relación

$$x \sim y \Leftrightarrow \cos x = \cos y$$

es de equivalencia.

(a) Verdadero

(b) Falso

Ejercicio 35. Sobre $\mathbb{Z}$ se define la relación de equivalencia

$$n \sim m \Leftrightarrow \exists k \in \mathbb{Z} \text{ tal que } m - n = 3k$$

Entonces, [0] es igual a:

(a) $\{0\}$

(b) $\{k \in \mathbb{Z} : m = 3k\}$

(c) $\{m \in \mathbb{Z} : \exists k \in \mathbb{Z} \text{ tal que } m = 3k\}$

(d) El conjunto de múltiplos de 3.

Ejercicio 36. Dada la relación de equivalencia

$$R = \{(0, 0), (0, 1), (1, 0), (1, 1), (2, 2)\}$$

la clase [2] es igual a:

(a) $\{0, 1\}$

(b) $\{0, 2\}$

(c) $\{2\}$

(d) $\{0, 1, 2\}$

Ejercicio 37. Dada la relación de equivalencia

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

su matriz de adyacencia asociada es:

(a) $\begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$

(b) $\begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

(c) $\begin{pmatrix} 1 & 2 & 0 \\ 2 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$

(d) $\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$

Ejercicio 38. En el juego de piedra-papel-tijera, la relación

$$x \prec y \Leftrightarrow x \text{ gana a } y$$

es una relación de orden parcial estricto.

(a) Verdadero

(b) Falso

Ejercicio 39. Sobre $\mathbb{R}^2$, la relación

$$(a, b) \preceq (c, d) \Leftrightarrow a \leq c$$

es de orden total

(a) Verdadero

(b) Falso

Ejercicio 40. Sobre $\mathbb{N}$ definimos la relación

$$n \preceq m \Leftrightarrow \text{ en binario, el número de unos de } n \text{ es menor que el número de unos de } m$$

Entonces, $4 \preceq 3$:

(a) Verdadero

(b) Falso

Ejercicio 41. Sobre $\mathbb{R}^2$, definimos la relación de orden parcial

$$(a,\, b) \preceq (c,\, d) \Leftrightarrow a \leq c \wedge b \leq d$$

¿Cuál es el supremo de $(0,\, 1) \times (0,\, 1)$?

(a) No tiene

(b) Todos los puntos de $[0,\, 1] \times \{1\}$

(c) Todos los puntos de $\{1\} \times [0,\, 1]$

(d) $(1,\, 1) \in \mathbb{R}^2$

Ejercicio 42. Sobre $\mathbb{R}^2$, definimos la relación de orden parcial

$$(a,\, b) \preceq (c,\, d) \Leftrightarrow a \leq c \wedge b \leq d$$

Entonces, el conjunto $[0,\, 1] \times (0,\, 1)$ tiene mínimo.

(a) Verdadero

(b) Falso

Capítulo 5

Aritmética modular

5.1. Introducción

En esta unidad vamos a estudiar algunos de los conceptos básicos tanto de la aritmética (teoría de números) sobre los números enteros como de la aritmética modular. Esta segunda es una rama de la aritmética que bien podría llamarse la aritmética del reloj (analógico), pues su objeto de estudio son las propiedades y las relaciones entre los números enteros cuando los cocientamos con un cierto número entero distinto de 0. En el caso del reloj, establecemos una primera hora, el 0, y dividimos la esfera en 12 intervalos temporales. cuando han pasado 12 horas, la aguja vuelve a señalar el 0, cuando han pasado 13, el 1, cuando han pasado 257, el 5, etc. En la primera sección nos centraremos en la relación de divisibilidad en los números enteros, centrando nuestra atención en el algoritmo de la división de Euclides y en la identidad de Bézout. En la segunda sección veremos el concepto de congruencia, que formaliza la idea que hemos dado de la aritmética del reloj. Una versión divulgativa de la aritmética modular puede leerse en https://elescritoriodeenrique.com/2020/04/07/congruencias-las-matematicas-de-la-semana/

5.2. Divisivilidad en los números enteros

5.2.1. Introducción

En este primer apartado vamos a estudiar cuestiones básicas relacionadas con la divisibilidad de los números enteros. Recordemos que $m|n$ si n es múltiplo de m. En este contexto jugará un papel muy importante el máximo común divisor de dos números. Tras estudiar algunas propiedades y resultados, veremos cómo calcularlo utilizando el algoritmo de la división de Euclides. A continuación veremos que, aunque no sea de manera única, existen dos enteros u y v de tal forma que el máximo común divisor de n y m se puede escribir como $nu + mv$ y estudiaremos la identidad de Bézout como algoritmo para encontrar estos u y v.

5.2.2. Cuestiones fundamentales de aritmética

Definición 5.2.2.1. Sean n, $m \in \mathbb{Z}$. Se dice que m divide a n si existe $k \in \mathbb{Z}$ tal que $n = km$. Se escribe $m|n$.

Observación 5.2.2.2. La relación de divisibilidad es de orden parcial, pero no total, en $\mathbb{N}$. Sin embargo, no es una relación de orden parcial en $\mathbb{Z}$, ya que no cumple la propiedad antisimétrica. En efecto, si $n \neq 0$, $-n|n$ y $n|-n$, pero $n \neq -n$.

Teorema 5.2.2.3. Sean n, $m \in \mathbb{Z}$ tales que $m \neq 0$. Entonces, existen un único $c \in \mathbb{Z}$ y un único $r \in \{0, \ldots, |m|-1\}$ tales que $n = m \cdot c + r$. A c se le llama cociente y a r resto.

Demostración. Primero veamos que existen dichos c y r. Para ello, separaremos los casos en los que $m > 0$ y $m < 0$.

(i) Si $m > 0$, para todo $c \in \mathbb{Z}$,

$$n = mc + (n - mc)$$

Sea

$$S = \{n - mx \,:\, x \in \mathbb{Z}\}$$

Se comprueba que $S \cap \mathbb{N} \neq \emptyset$. Sea

$$S_0 = \{n - mx \geq 0 \,:\, x \in \mathbb{Z}\}$$

Sea

$$r = n - mc = \text{mín}\, S_0,\ c \in \mathbb{Z}$$

Supongamos $r \geq m$. Entonces,

$$0 \leq r - m = (n - mc) - m = n - m(c+1) = r - m < r$$

Luego $n - m(c+1) \in S_0$ es menor que r. Pero esto contradice lo que habíamos supuesto. Así, $0 \leq r < m$.

(ii) Si $m < 0$, Rehacemos el apartado anterior para $-m$, ya que $n = (-m)c + r = m(-c) + r$.

Para ver la unicidad, supongamos que

$$n = mc_1 + r_1 = mc_2 + r_2$$

tales que $0 \leq r_1,\ r_2 < |m|$, con $c_1 \neq c_2$, $r_1 \neq r_2$. Entonces,

$$m(c_1 - c_2) = r_2 - r_1$$

y

$$|r_2 - r_1| < |m|$$

Por otra parte,

$$|m(c_1 - c_2)| = |m|\,|c_1 - c_2| \geq |m|$$

Pero

$$|m| \leq |m|\,|c_1 - c_2| = |r_1 - r_2| < |m|!!$$

Por tanto, $r_1 = r_2$ y $c_1 = c_2$. □

Definición 5.2.2.4. Sean n, $m \in \mathbb{Z} - \{0\}$. Se define el máximo común divisor de n y m como

$$\text{mcd}(n, m) = \text{mín}\{k \in \mathbb{N} : k|n, k|m\}$$

Si $\text{mcd}(n, m) = 1$ se dice que n y m son coprimos o primos entre sí.

Observación 5.2.2.5. Al definirse el máximo común divisor como el mínimo de un conjunto, se concluye que este valor es único.

Proposición 5.2.2.6. Sean a, b, c, $d \in \mathbb{Z}$ tales que $a = b + c$, $d|a$ y $d|b$. Entonces $d|c$.

Demostración. Como $d|a$ y $d|b$, existen k, $k_1 \in \mathbb{Z}$ tales que $a = dk$ y $b = dk_1$. Al dividir c entre d, existen $k_2 \in \mathbb{Z}$ y $0 < r < |d| - 1$ tales que $c = dk_2 + r$. Por tanto,

$$a = b + c \Leftrightarrow dk = dk_1 + dk_2 + r = d(k_1 + k_2) + r \Leftrightarrow k_1 + k_2 = k,\ r = 0$$

Por tanto, $d|c$. □

Corolario 5.2.2.7. Sean n, m, c, $r \in \mathbb{Z}$ tales que $n = mc + r$. Entonces, $\text{mcd}(n, m) = \text{mcd}(m, r)$.

Proposición 5.2.2.8 (Algoritmo de Euclides)**.** Sean a, $b \in \mathbb{Z}$ tales que $a \geq b$ y $b \neq 0$ (si no, intercambiamos los papeles de a y b).

(i) El primer paso consiste en hacer la división de a entre b y escribirla de forma que

$$a = bc_1 + r_1$$

(ii) El siguiente paso es ver si el resto es 0.

- Si lo es, entonces $a = bc_1$ y b sería $\text{mcd}(a, b)$ (porque b sería divisor de a y no hay mayor divisor de b que b).
- Si $r_1 \neq 0$, dividimos b entre r_1 y lo escribimos como

$$b = r_1c_2 + r_2$$

(iii) Este proceso se repite hasta encontrar un $r_n = 0$, y el máximo común divisor será r_{n-1}.

El esquema que se sigue es el siguiente:

$$a = bc_1 + r_1\ (0 \leq r_1 < b)$$

$$b = r_1c_2 + r_2\ (0 \leq r_2 < r_1)$$

$$r_1 = r_2c_3 + r_3\ (0 \leq r_3 < r_2)$$

$$\vdots$$

$$r_{n-3} = r_{n-2}c_{n-1} + r_{n-1}\ (0 \leq r_{n-2} < r_{n-1})$$

$$r_{n-2} = r_{n-1}c_n\ (r_n = 0)$$

Entonces, $\text{mcd}(a, b) = r_{n-1}$.

Ejemplo 5.2.2.9 (Implementación del algoritmo de Euclides en Python)**.**

In [1]:
```
def AlgoritmoEuclides(n,m): #Hace un print en cada iteracion y devuelve mcd(n,m)
    if n<=m:
        a=m
        b=n
    else:
        a=n
        b=m
    c=a//b
    r=a%b
    print(str(a)+'='+str(b)+'x'+str(c)+'+'+str(r))
    while r!=0:
        a=b
        b=r
        c=a//b
        r=a%b
        print(str(a)+'='+str(b)+'x'+str(c)+'+'+str(r))
    print('mcd('+str(n)+','+str(m)+') = '+str(b))
    return(b)

AlgoritmoEuclides(135,1467)
```

```
1467=135x10+117
135=117x1+18
117=18x6+9
18=9x2+0
mcd(135,1467) = 9
```

Out[1]: 9

Observación 5.2.2.10. El algoritmo siempre termina en una cantidad finita de pasos, pues los restos sucesivamente irán decreciendo.

Proposición 5.2.2.11 (Identidad de Bézout)**.** Una vez calculado el máximo común divisor de n y m, podemos encontrar dos números enteros k_1, k_2 tales que

$$\text{mcd}(n, m) = n \cdot k_1 + m \cdot k_2$$

aunque no siempre van a ser únicos. Una forma de hallarlos es mediante la Identidad de Bézout, que consiste en ir despejando los restos obtenidos mediante el algoritmo de Euclides y sustituirlos en los pasos previos.

Ejemplo 5.2.2.12 (Implementación de la Identidad de Bézout en Python)**.**

In [2]:
```
def IdBezout(n,m):
    if n<=m:
        a=m
        b=n
    else:
        a=n
        b=m
    c=a//b
    r=a%b
    aS=[]
    bS=[]
    cS=[]
    rS=[]
    while r!=0:
        aS.append(a)
        bS.append(b)
        cS.append(c)
        rS.append(r)
        a=b
        b=r
        c=a//b
        r=a%b
    rs=[aS[0],aS[1]]+rS
    x=[(1,0),(0,1)]
    for i in range(len(cS)):
        aux1=tuple([k*cS[i] for k in x[i+1]])
        aux=(x[i][0]-aux1[0],x[i][1]-aux1[1])
        x.append(aux)
    print(str(rS[-1])+'='+str(aS[0])+'*('+str(x[-1][0])+')+'+str(aS[1])+'*('+str(x[-1][1])+')')
    return(x[-1])


IdBezout(267,1452)
#1467*7+135*(-76)
```

```
3=1452*(16)+267*(-87)
```

Out[2]: (16, -87)

Definición 5.2.2.13. Un número natural $p > 1$ es un número primo si sus únicos divisores naturales son 1 y p. A los naturales mayores que 1 que no son primos los llamaremos compuestos.

Proposición 5.2.2.14. Todo número natural $n > 1$ tiene algún divisor primo.

Teorema 5.2.2.15 (Teorema Fundamental de la Aritmética)**.** Todo número natural $n > 1$ se puede expresar como producto de primos de manera única.

Demostración. En 2.3.2.8. □

Proposición 5.2.2.16. El conjunto de números primos es infinito.

Demostración. Como ejercicio. □

Proposición 5.2.2.17. Sean $n, m \in \mathbb{Z} - \{0\}$ y $a \in \mathbb{Z} - \{0\}$ primo con n. Si $a|nm$, entonces $a|m$.

Demostración. Como a y n son primos entre sí, $\text{mcd}(a, n) = 1$. Por la identidad de Bézout, existen $u, v \in \mathbb{Z}$ tales que

$$1 = au + nv$$

Si multiplicamos por m a ambos lados de la igualdad obtenemos

$$m = amu + nmv$$

De aquí se tiene que $a|amu$ trivialmente, y también $a|nmv$, pues $a|nm$. Por tanto, $a|(amu+nmv)$, por lo que $a|m$. □

Observación 5.2.2.18. Si $d|ab$ en general, no tiene por qué darse $d|a$ o $d|b$. Por ejemplo, $6|8\cdot 9$, pero $6 \not| 8$ y $6 \not| 9$.

Corolario 5.2.2.19. Sean n, $m \in \mathbb{Z} - \{0\}$ y p un primo tal que $p|nm$. Entonces, $p|n$ o $p|m$.

Demostración. Sin pérdida de generalidad, si $p \not| n$, como p es primo, $\text{mcd}(p, n) = 1$ y, por la proposición 5.2.2.17, $p|m$. □

5.3. Relaciones de congruencia

5.3.1. Introducción

Como ya hemos adelantado en la introducción de esta unidad, la aritmética modular generaliza la forma que un reloj analógico tiene de marcar las horas. Una vez han pasado 12 horas, marcase la hora que marcase la aguja al comienzo de contar, la aguja volvería a marcar la misma hora. Sea

$$\{0, 1, \ldots, 11\}$$

el conjunto de las horas que tiene un reloj (en realidad en lugar del 0 suele tener un 12). Si comenzamos a contar horas en el momento en el que la aguja marca el 0 y pasan 12 horas, la aguja volverá a marcar 0. Si pasan 13 horas, la aguja volverá a marcar 1. De hecho, $13 = 12\cdot 1+1$, donde el cociente 1 significa que la aguja ha dado 1 vuelta completa, y el resto 1 significa que, después de esa vuelta, la aguja ha recorrido una hora más. Si pasan 14 horas, la aguja marcará 2, pues $14 = 12 \cdot 1 + 2$. Si pasan 30 horas, la aguja marcará 6, pues $30 = 12 \cdot 2 + 6$. En general, si pasan n horas, la aguja marcará la hora r, donde $n = 12\cdot c+r$. El cociente c significa que la aguja ha dado c vueltas completas y luego ha recorrido $0 \leq r < 12$ horas. De aquí podemos definir una relación de equivalencia sobre los números enteros que relaciona dos de ellos si equivalen a la misma hora en nuestro reloj. Por tanto, las clases de equivalencia son precisamente las horas que aparecen en nuestro reloj.

En esta unidad vamos a estudiar la *aritmética del reloj* para un reloj con, en general, m horas.

5.3.2. Congruencias

Definición 5.3.2.1. Sea $m \in \mathbb{Z} - \{0\}$. Dados a, $b \in \mathbb{Z}$, definimos la relación

$$a \sim_m b \Leftrightarrow \exists k \in \mathbb{Z} \text{ tal que } a - b = m \cdot k$$

Esta es una relación de equivalencia que se denota $a \equiv b \mod m$.

Veamos que, efectivamente, es una relación de equivalencia.

(R) $a \equiv a \mod m$, pues $a - a = 0 = m \cdot 0$.

(S) Si $a \equiv b \mod m$, entonces existe $k \in \mathbb{Z}$ tal que $a-b = mk$. Por otra parte, $b-a = -mk = m \cdot (-k)$, luego $b \equiv a \mod m$.

(T) Si $a \equiv b \mod m$ y $b \equiv c \mod m$, entonces existen k_1 y k_2 enteros tales que $a - b = mk_1$ y $b - c = mk_2$. Por tanto,

$$a - c = a - b + b - c = mk_1 + mk_2 = m(k_1 + k_2)$$

Así, $a \equiv c \mod m$.

Observación 5.3.2.2. La clase de equivalencia de $a \in \mathbb{Z}$ es

$$[a] = \{n \in \mathbb{Z} : a \equiv n \mod m\} = \{n \in \mathbb{Z} : \exists k \in \mathbb{Z} \text{ tal que } n - a = mk\} =$$

$$\{n \in \mathbb{Z} : \exists k \in \mathbb{Z} \text{ tal que } n = mk + a\}$$

Por tanto,

$$\frac{\mathbb{Z}}{\sim_m} = \{[0], [1], \ldots, [m-1]\} \text{ o, simplemente, } \{0, 1, \ldots, m-1\}$$

Proposición 5.3.2.3. Sean $m \in \mathbb{Z} - \{0\}$ y $a, b \in \mathbb{Z}$. Entonces:

(i) Si $a \equiv b \mod m$ y $a_1 \equiv b_1 \mod m$, entonces $a + a_1 \equiv b + b_1 \mod m$.

(ii) $ak \equiv bk \mod m$, $\forall k \in \mathbb{Z}$.

(iii) $a^n \equiv b^n \mod m$, $\forall n \in \mathbb{N}$.

Demostración. Como ejercicio. □

Proposición 5.3.2.4. Sean $a = a_1 d$, $b = b_1 d$, $m = m_1 d$. Entonces, $a \equiv b \mod m$ si y solo si $a_1 \equiv b_1 \mod m_1$.

Demostración.

($\Rightarrow$) Como

$$a \equiv b \mod m$$

entonces existe k tal que

$$a - b = mk$$

luego

$$a_1 d - b_1 = m_1 dk$$

Esto implica que

$$a_1 - b_1 = m_1 k$$

Así,

$$a_1 \equiv b_1 \mod m_1$$

($\Leftarrow$) Similar. □

5.3.3. Congruencias lineales

Definición 5.3.3.1. Sean $a \in \mathbb{Z} - \{0\}$, b, $m \in \mathbb{Z}$. A la ecuación $ax \equiv b \mod m$ se le llama congruencia lineal.

Proposición 5.3.3.2. Si α es solución de $ax \equiv b \mod m$ y $\beta \equiv \alpha \mod m$, entonces β también es solución.

Demostración. Como α es solución de

$$ax \equiv b \mod m$$

se tiene que

$$a\alpha \equiv b \mod m$$

Por otra parte, como

$$\beta \equiv \alpha \mod m$$

por el apartado (ii) de la proposición 5.3.2.3 se tiene que

$$a\beta \equiv a\alpha \mod m$$

Por tanto,

$$a\beta \equiv b \mod m$$

y β es solución de la congruencia lineal. □

Teorema 5.3.3.3. $ax \equiv b \mod m$ tiene solución si y solo si $\text{mcd}(a, m)|b$. En este caso, el número de soluciones en $\mathbb{Z}_m$ es $\text{mcd}(a, m)$.

Demostración. Llamemos $d = \text{mcd}(a, m)$. Primero veamos la doble implicación:

($\Leftarrow$) Como $d|b$, existe k tal que $b = dk$. Además, por la Identidad de Bézout, existen u, v tales que $d = au + mv$. Por tanto,

$$b = auk + mvk$$

Así, $b \equiv auk \mod m$, luego uk es solución de la congruencia lineal.

($\Rightarrow$) Supongamos que α es solución de

$$ax \equiv b \mod m$$

Entonces,

$$a\alpha \equiv b \mod m$$

Por tanto, existe k tal que

$$a\alpha - b = mk \Leftrightarrow b = a\alpha - mk$$

Por tanto, como $d|(a\alpha - mk)$, se tiene que $d|b$.

Ahora probemos la segunda parte de la demostración. Para ello distingamos los casos en los que $d = 1$ y $d > 1$.

(i) Si $d = 1$, supongamos que existen dos soluciones α, $\beta \in \mathbb{Z}_m$. Entonces,

$$a\alpha \equiv b \mod m$$

y

$$a\beta \equiv b \mod m$$

Por tanto,

$$a\alpha \equiv a\beta \mod m \Rightarrow a(\alpha - \beta) \equiv 0 \mod m$$

Esto quiere decir que existe k tal que $a(\alpha - \beta) = mk$. Pero como $d = 1$, $\alpha - \beta$ es múltiplo de m. Por otra parte, α, $\beta \in \mathbb{Z}_m$, luego $\alpha - \beta = 0$, lo que implica que $\alpha = \beta$.

(ii) Si $d > 1$, entonces $a = a_1 d$, $m = m_1 d$ y, por tanto, $b = b_1 d$. Como $\text{mcd}(a, m_1)$, se tiene que, por el apartado anterior,

$$a_1 x \equiv b_1 \mod m_1$$

tiene solución única $\alpha \in \mathbb{Z}_{m_1}$. Por tanto, como por la proposición 5.3.2.4 se tiene que

$$ax \equiv b \mod m \text{ si y solo si } a_1 x \equiv b_1 \mod m_1$$

las soluciones de la congruencia original son

$$\alpha,\ \alpha + m_1,\ \alpha + 2m_1,\ \ldots,\ \alpha + (d-1)m_1$$

pues $\alpha \equiv \alpha + km_1 \mod m_1$, $\forall k \in \mathbb{Z}$. Además, $\alpha + dm_1 = \alpha + dm \notin \mathbb{Z}_m$. Por tanto, hay un total de d soluciones en $\mathbb{Z}_m$.

□

Ejercicio 5.3.3.4. Encontrar todas las soluciones de $56x \equiv 42 \mod 105$.

Corolario 5.3.3.5. Dado $a \in \mathbb{Z}_m$, existe $a^{-1} \in \mathbb{Z}_m$ solución de $ax \equiv 1 \mod m$ si y solo si $\text{mcd}(a, m) = 1$. A a^{-1} se le llama inverso de a módulo m.

Teorema 5.3.3.6 (Teorema chino del resto)**.** Si m_1, m_2 son primos entre sí y cada congruencia lineal del sistema

$$\begin{cases} a_1 x \equiv b_1 \mod m_1 \\ a_2 x \equiv b_2 \mod m_2 \end{cases}$$

tiene solución, entonces el sistema tiene solución en $\mathbb{Z}_{m_1 m_2}$. Además, si $\text{mcd}(a_i, m_i) = 1$, $i = 1, 2$, la solución es única.

Demostración. Sea α_i solución de $a_i x \equiv b_i \mod m_i$, $i = 1, 2$. Como $\text{mcd}(m_1, m_2) = 1$, por la identidad de Bézout, existen u, v tales que

$$1 = m_1 u + m_2 v$$

Vamos a demostrar que

$$\alpha = \alpha_2 m_1 u + \alpha_1 m_2 v$$

es solución común a ambas congruencias.

Es solución de la primera congruencia porque

$$\alpha = \alpha_2 m_1 u + \alpha_1 m_2 v = \alpha_2 m_1 u + \alpha_1(1 - m_1 u) = \alpha_1 + m_1(\alpha_2 u - \alpha_1 u)$$

Es solución de la segunda congruencia porque

$$\alpha = \alpha_2 m_1 u + \alpha_1 m_2 v = \alpha_2(1 - m_2 v) + \alpha_1 m_2 v = \alpha_2 + m_2(\alpha_1 v - \alpha_2 v)$$

Así, α es solución de ambas congruencias. Además, si $\alpha \equiv \beta \mod m_1 m_2$ y $\beta \in \mathbb{Z}_{m_1 m_2}$, se tiene que β es solución de ambas congruencias en $\mathbb{Z}_{m_1 m_2}$.

La segunda parte de la demostración queda como ejercicio. □

Ejercicio 5.3.3.7. Encontrar las soluciones de

$$\begin{cases} a_1 x \equiv b_1 \mod m_1 \\ a_2 x \equiv b_2 \mod m_2 \end{cases}$$

en $\mathbb{Z}_{m_1 m_2}$.

Teorema 5.3.3.8 (Pequeño teorema de Fermat)**.** Si p es primo y a no es múltiplo de p, entonces $a^{p-1} \equiv 1 \mod p$.

5.4. Ejercicios

Ejercicio 43. Si $m|ab$ entonces $m|a$ o $m|b$.

(a) Verdadero

(b) Falso

Ejercicio 44. mcd(176, 24) es:

(a) 2

(b) 3

(c) 4

(d) 8

Ejercicio 45. Dados n, m cuyo máximo común divisor es d, los enteros u, v tales que $d = nu + mv$ no son únicos:

(a) Verdadero

(b) Falso

Ejercicio 46. Existe un único $b \in \mathbb{Z}_m$ tal que $a \equiv b \mod m$:

(a) Verdadero

(b) Falso

Ejercicio 47. El número de soluciones de $px \equiv b \mod m$ en $\mathbb{Z}_m$ donde p es primo y $p \neq m$ es:

(a) p

(b) No tiene

(c) 1

(d) No se puede saber

Capítulo 6

Grafos

6.1. Introducción

Los grafos son otro concepto fundamental de la Matemática Discreta, especialmente en cuestiones relacionadas con la Informática y las Ciencias Sociales. En la unidad anterior vimos, sin entrar en demasiado detalle, en qué consistían los grafos dirigidos y cómo representarlos gráficamente y por medio de las matrices de adyacencia. En esta unidad profundizaremos mucho más en estos conceptos, y ampliaremos la definición de grafo a grafos no dirigidos. Exploraremos todas las posibilidades que nos ofrecen las distintas representaciones de los grafos para estudiar sus propiedades fundamentales.

El estudio de la unidad nos llevará a la parte más importante de la unidad: los grafos eulerianos y hamiltonianos. Estos dos tipos de grafos surgen en problemas para los cuales debemos encontrar ciertos caminos especiales que comienzan y terminan en un mismo punto. A lo largo de todo el tema, veremos algoritmos que nos permitirán obtener la solución a determinados problemas.

6.2. Tipos de grafos

6.2.1. Introducción

En esta sección vamos a conocer los dos grandes tipos de grafos que existen: dirigidos y no dirigidos. Veremos cómo representar gráfica y matricialmente estos grafos y toda la terminología relacionada con ellos, como los conceptos de vértice, arista, bucle, etc. Estudiaremos las propiedades básicas de los grafos y acabaremos aprendiendo a saber cuándo dos grafos son *iguales* gracias al concepto de isomorfismo (misma forma).

6.2.2. Conceptos básicos. Representación gráfica de grafos

Definición 6.2.2.1. Un grafo dirigido (u orientado), también llamado digrafo, es un par $G = (V, E)$, donde

$$V = \{v_i : i \in I\}$$

y $E \subseteq V \times V$. Es decir,

$$E = \{(u, v) : u, v \in V\}$$

A los elementos de V se les llama vértices o nodos y a los de E aristas o arcos. A los vértices que forman una arista se les llama extremos de la arista. Si $(u, v) \in E$, a u se le llama vértice de partida y a v se le llama vértice de llegada.

Ejemplo 6.2.2.2. Sean

$$V = \{1, 2, 3, 4\}$$

y

$$E = \{(1, 1), (1, 2), (2, 1), (2, 3), (2, 4), (3, 1), (4, 1), (4, 2), (4, 4)\}$$

Entonces, $G = (V, E)$ es un grafo dirigido.

Definición 6.2.2.3. Una arista de la forma (v, v) se llama bucle.

Un grafo dirigido se puede representar de manera gráfica utilizando círculos etiquetados con los nombres de los vértices y flechas entre círculos a modo de aristas con la punta de la flecha apuntando al vértice de entrada.

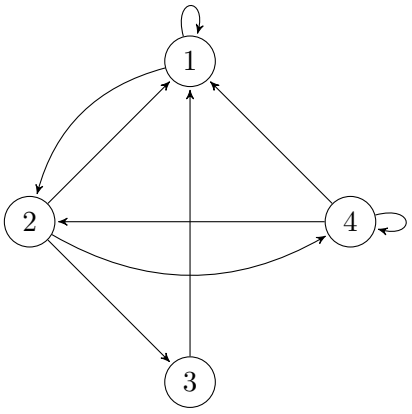
Ejemplo 6.2.2.4. Volviendo al grafo $G = (V, E)$, donde

$$V = \{1, 2, 3, 4\}$$

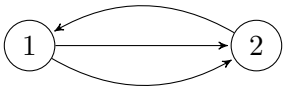
y

$$E = \{(1, 1), (1, 2), (2, 1), (2, 3), (2, 4), (3, 1), (4, 1), (4, 2), (4, 4)\}$$

lo representaríamos gráficamente como



Observación 6.2.2.5. Existen grafos dirigidos que tienen varias aristas repetidas que se llaman multigrafos, en este caso, multigrafos dirigidos como el siguiente:



En este caso, el modelo de E como subconjunto de $V \times V$ ya no tiene sentido, ya que en un conjunto, los elementos no aparecen repetidos. Para ello, existe el concepto de **multiconjunto**,

que difiere del de conjunto en que los elementos pueden aparecer repetidos. La notación de un multiconjunto es la misma que la de conjunto. Aunque no nos preocupemos demasiado por la formalidad en este aspecto en las definiciones y los resultados, conviene saber que se formalizaría de este modo.

Definición 6.2.2.6. Un grafo no dirigido (o no orientado) es un par $G = (V, E)$, donde

$$V = \{v_i : i \in I\}$$

y

$$E = \{\{v, w\} : v, w \in V\}$$

A los elementos de V se les llama vértices y a los de E aristas. A los vértices que forman una arista se les llama extremos de la arista. Dos vértices unidos por una arista se dice que son adyacentes.

Ejemplo 6.2.2.7. Sean

$$V = \{1, 2, 3, 4\}$$

y

$$E = \{\{1, 1\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{4, 4\}\}$$

Entonces, $G = (V, E)$ es un grafo no dirigido.

Observación 6.2.2.8. En un grafo no dirigido, se tiene que $\{u, v\} = \{v, u\}$. Sin embargo, en un grafo dirigido, $(u, v) \neq (v, u)$.

Un grafo dirigido se puede representar de manera gráfica utilizando círculos etiquetados con los nombres de los vértices y líneas sin flechas entre círculos a modo de aristas.

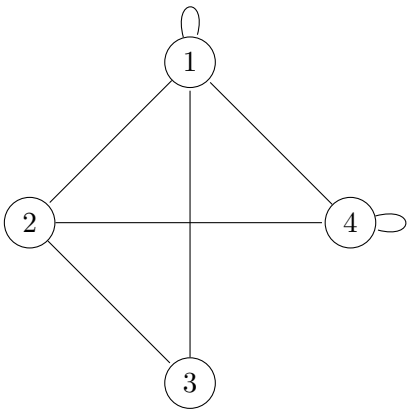
Ejemplo 6.2.2.9. Volviendo al grafo $G = (V, E)$, donde

$$V = \{1, 2, 3, 4\}$$

y

$$E = \{\{1, 1\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{4, 4\}\}$$

lo representaríamos gráficamente como



Observación 6.2.2.10. Al igual que para grafos dirigidos, también existen multigrafos no dirigidos.

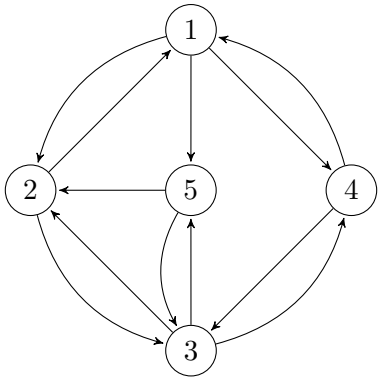
Definición 6.2.2.11. Sea $G = (V, E)$ un grafo dirigido no multigrafo. Se define el grafo no dirigido subyacente de G, $G' = (V', E')$, como un grafo no dirigido tal que:

(i) $V' = V$

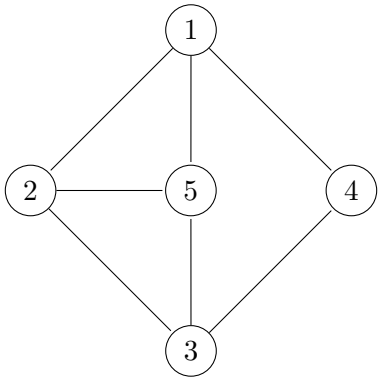
(ii) $E' = \{\{u, v\} : (u, v) \in E\}$

Es decir, consiste en en el grafo dirigido de forma que a cada arista se le elimina la flecha y si hay una arista de u a v y otra arista de v a u, se eliminan las flechas y permanece una sola de las aristas.

Ejemplo 6.2.2.12. Consideremos el siguiente grafo dirigido:



Entonces, su grafo no dirigido subyacente es



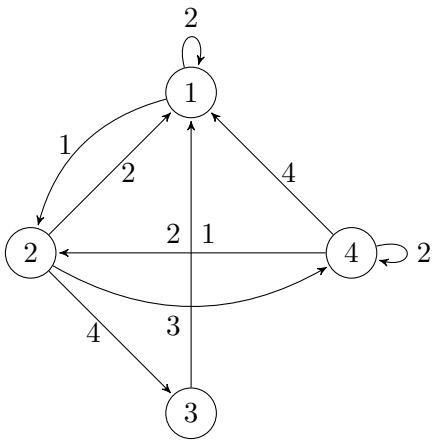
Nota 6.2.2.13. En un grafo no multigrafo, para simplificar la notación de las aristas, llamaremos e_{ij} a $\{v_i, v_j\}$, en caso de que el grafo sea no dirigido, o a (v_i, v_j), en caso de que el grafo sea dirigido.

Definición 6.2.2.14. Se dice que un grafo es simple si no tiene bucles ni aristas repetidas.

Definición 6.2.2.15. Se dice que un grafo (V, E) es valorado si cada arista $e \in E$ tiene asociado un valor $p \in \mathbb{R}$ llamado peso.

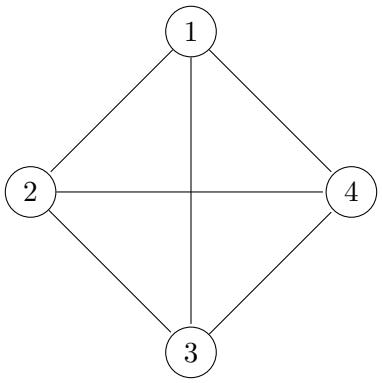
Ejemplo 6.2.2.16. El siguiente es un grafo valorado[1]:

[1]Se ha elegido el criterio de situar las etiquetas de los pesos de las aristas que no son bucles a la derecha de la arista, tomando como referencia la flecha apuntando hacia arriba. Así, por ejemplo, la arista $e_{3,1}$ tiene peso 1 y la arista $e_{4,2}$ tiene peso 2.



Definición 6.2.2.17. Se dice que un grafo es completo si cada par de vértices está unido por una arista.

Ejemplo 6.2.2.18. El siguiente grafo es completo:



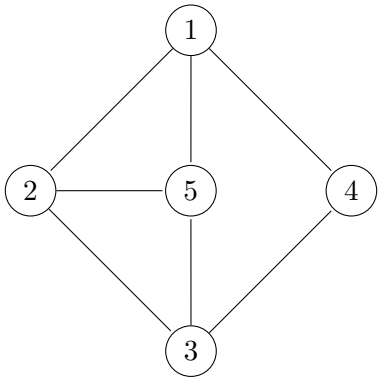
Definición 6.2.2.19. Sea $G = (V, E)$ un grafo. Se dice que $G' = (V', E')$ es subgrafo de G si:

(i) $V' \subseteq V$

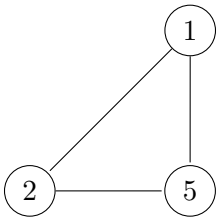
(ii) $E' = \{e_{ij} \in E : v_i, v_j \in V'\}$

Es decir, es un grafo formado por algunos vértices de G y cuyas aristas son aquellas con extremos en V' que pertenecen a E.

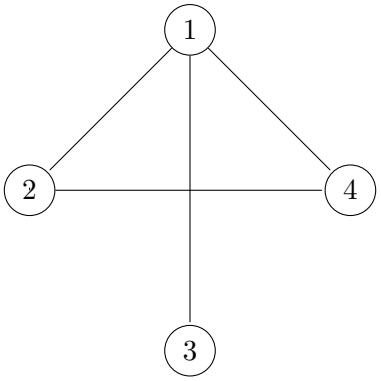
Ejemplo 6.2.2.20. Sea el grafo G

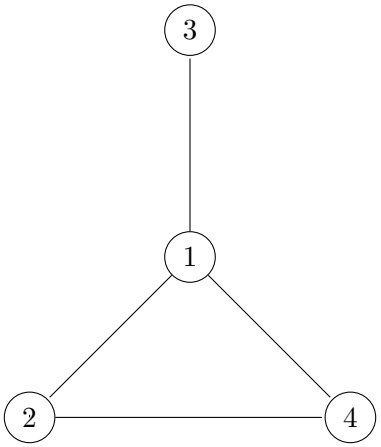


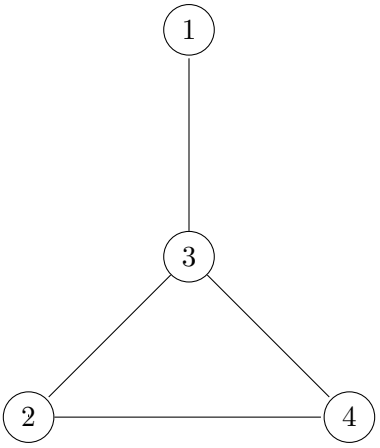
Entonces, el subgrafo formado por los vértices $V' = \{1, 2, 5\}$ es



Dados los siguientes grafos, ¿se puede decir que son el mismo grafo?







Evidentemente, se puede ver que el primer grafo y el segundo están dispuestos en otras posiciones pero poseen los mismos vértices y las mismas aristas entre ellos, por lo que sí se puede decir que son el mismo grafo. Por otra parte, el segundo grafo y el tercero cambian solamente en el nombre de los vértices 1 y 3, por lo que, salvo renombramiento, siguen siendo el mismo grafo. De esta forma, las tres representaciones hacen referencia al mismo grafo.

El concepto que justifica dicha igualdad es el de isomorfismo de grafos. Básicamente, dos grafos son iguales (isomorfos) si sucede una de las dos situaciones que acabamos de exponer. Para definir rigurosamente isomorfismo necesitamos dar otras definiciones previas.

Definición 6.2.2.21. Sea

$$f : X \longrightarrow Y$$

una función entre dos conjuntos X e Y. Se dice que f es:

(i) Inyectiva, si para todo x, $y \in X$ tal que $f(x) = f(y)$ implica que $x = y$.

(ii) Sobreyectiva, si para todo $y \in Y$ existe $x \in X$ tal que $f(x) = y$.

(iii) Biyectiva, si es inyectiva y sobreyectiva.

En conclusión, una función es biyectiva si los elementos de X e Y están relacionados uno a uno por f.

Ejemplo 6.2.2.22.

(i) La función identidad $f(x) = x$ es biyectiva en cualquier conjunto X.

(ii) $f(x) = x^2$ no es biyectiva en $\mathbb{R}$, ya que no es ni inyectiva ni sobreyectiva. No es inyectiva porque $f(x) = f(-x)$, $\forall x \in \mathbb{R}$. No es sobreyectiva porque, si $x \in \mathbb{R}$, no existe ningún número negativo y tal que $y = x^2$.

(iii) La función

$$\begin{aligned} f : X &\longrightarrow Y \\ x &\longmapsto x + 2 \end{aligned}$$

no es biyectiva si $X = Y = \mathbb{N}$, ya que no es sobreyectiva. Pero sí es biyectiva si $X = \mathbb{N}$ e $Y = \{n \in \mathbb{N} : n \geq 2\}$.

Definición 6.2.2.23. Sean $G = (V, E)$, $G' = (V', E')$ dos grafos y

$$f : V \longrightarrow V'$$

una función. Se dice que f es un isomorfismo entre G y G' si se satisfacen las siguientes propiedades:

(i) f es biyectiva.

(ii) Si u, $v \in V$ son adyacentes, entonces $f(u)$, $f(v) \in V'$ son adyacentes.

Si existe un isomorfismo entre G y G', entonces se dice que G y G' son isomorfos, y se escribe $G \approx G'$.

Ejemplo 6.2.2.24. Los tres grafos con los que hemos introducido el tema de isomorfismos son isomorfos. Entre el primero y el segundo no hay nada que comentar, ya que la única diferencia es su representación geométrica, pero el isomorfismo es la función identidad. Entre el segundo y el tercero, el isomorfismo viene dado por la función

$$f(1) = 3,\ f(2) = 2,\ f(3) = 1,\ f(4) = 4$$

Evidentemente, es una función biyectiva. Para ver la segunda condición, nos fijamos en que el conjunto de vértices adyacentes a 1 es $\{2, 3, 4\}$, a 2 es $\{1, 4\}$, a 3 es $\{1\}$ y a 4 es $\{1, 2\}$. El conjunto de vértices adyacentes a $f(1)$ es $\{f(2), f(3), f(4)$, a $f(2)$ es $\{f(1), f(4)\}$, a $f(3)$ es $\{f(1)\}$ y a $f(4)$ es $\{f(1), f(2)\}$. Por tanto, se puede concluir que la segunda propiedad de isomorfismo se satisface.

De la definición de isomorfismo y del ejemplo anterior podemos deducir el siguiente resultado.

Corolario 6.2.2.25. Sea G un grafo. Entonces, un renombramiento de los vértices de V da lugar a un grafo isomorfo a G.

Observación 6.2.2.26. El corolario anterior justifica que un conjunto de vértices $\{v_1, v_2, \ldots, v_n\}$ lo podamos reescribir como $\{1, 2, \ldots, n\}$.

6.2.3. Representación matricial de grafos

Para terminar la sección, vamos a representar grafos utilizando matrices. Ya vimos en la anterior unidad cómo un grafo dirigido podía ser representado por su matriz de adyacencia. Ahora vamos a profundizar más en ello y veremos que los grafos no dirigidos admiten representación por una matriz de adyacencia y cómo ambos tipos de grafos pueden representarse por otro tipo de matrices llamadas matrices de incidencia.

Definición 6.2.3.1. Sea $G = (V, E)$ un grafo sin aristas repetidas tal que $V = \{v_1, v_2, \ldots, v_n\}$. Como un grafo queda completamente determinado por sus vértices y sus aristas, podemos representar las aristas e_{ij} en una matriz, llamada matriz de adyacencia, $A = (a_{ij})_{i,j=1}^{n}$, de tal forma que

$$a_{ij} = \begin{cases} 1 & e_{ij} \in E \\ 0 & \text{otro caso} \end{cases}$$

Ejemplo 6.2.3.2. Sean $V = \{1, 2, 3, 4\}$ y $E = \{\{1, 2\}, \{1, 4\}, \{2, 2\}, \{2, 3\}, \{2, 4\}, \{3, 3\}, \{3, 4\}\}$. Entonces, la matriz de adyacencia del grafo $G = (V, E)$ es

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

Observación 6.2.3.3.

(i) Si un grafo es no dirigido, su matriz de adyacencia será simétrica, mientras que si el grafo es dirigido, la matriz de adyacencia no tiene por qué serlo.

(ii) Las matrices de adyacencia no permiten representar multigrafos.

Definición 6.2.3.4. Sea $G = (V, E)$ un grafo no dirigido tal que $V = \{v_1, v_2, \ldots, v_n\}$ y $E = \{e_1, e_2, \ldots, e_m\}$. Se define la matriz de incidencia de G como una matriz[2]

$$I = (a_{ij})_{i=1\ldots n,\, j=1\ldots m}$$

de forma que las filas representan los vértices, las columnas las aristas y

$$a_{ij} = \begin{cases} 1 & v_i \text{ es un extremo de la arista } e_j \\ 0 & \text{otro caso} \end{cases}$$

Ejemplo 6.2.3.5. Sean $V = \{1, 2, 3, 4\}$ y $E = \{\{1, 2\}, \{1, 4\}, \{2, 2\}, \{2, 3\}, \{2, 4\}, \{3, 3\}, \{3, 4\}\}$. Entonces, la matriz de incidencia del grafo $G = (V, E)$ es

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

Definición 6.2.3.6. Sea $G = (V, E)$ un grafo dirigido tal que $V = \{v_1, v_2, \ldots, v_n\}$ y $E = \{e_1, e_2, \ldots, e_m\}$. Se define la matriz de incidencia de G como una matriz

$$I = (a_{ij})_{i=1\ldots n,\, j=1\ldots m}$$

de forma que

$$a_{ij} = \begin{cases} -1 & e_j \text{ es una arista que parte de } v_i \\ 1 & e_j \text{ es una arista que llega a } v_i \\ 0 & \text{otro caso} \end{cases}$$

Observación 6.2.3.7. Las matrices de incidencia sí permiten representar multigrafos.

6.3. Más sobre grafos

6.3.1. Introducción

En esta sección apartado introduciremos el concepto de aridad, o grado, de un vértice en un grafo no dirigido como el número de aristas que tienen a dicho vértice como extremos. En el caso de un grafo dirigido diferenciaremos el grado de entrada y el de salida, definiendo el grado como la suma de dichos grados. Aprenderemos a calcular estos valores utilizando la representación matricial de los grafos. Posteriormente, estudiaremos en qué consiste un grafo bipartito y expondremos resultados que los caracterizan a partir de su representación matricial. Finalmente, veremos qué significa que un grafo sea $k-$coloreable y mostraremos un algoritmo para aproximar dicho valor.

6.3.2. Aridad

Definición 6.3.2.1. Sea $G = (V, E)$ un grafo no dirigido simple y sea $v \in V$. Se define el grado (o aridad, o valencia) de v como

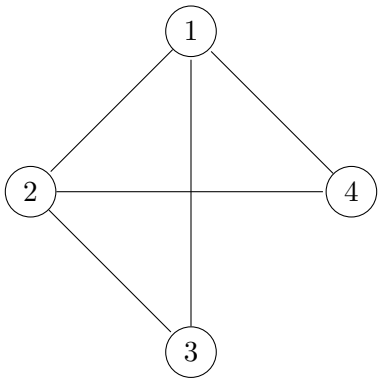
$$g(v) = |\{\{u, v\} \in E\}|$$

[2]Hemos utilizado la notación I para denotar a la matriz de incidencia, lo que podría dar lugar a confusiones, ya que es la notación habitualmente empleada para la matriz identidad. Sin embargo, en este curso no vamos a trabajar en ningún momento con matrices identidad y no habrá solapamiento de notaciones.

Es decir, es la cantidad de aristas de G que tienen a v como extremo.

Se dice que v es par si $g(v)$ es par, y se dice que es impar si $g(v)$ es impar.

Ejemplo 6.3.2.2. Sea el grafo



Entonces, $g(1) = g(2) = 3$ y $g(3) = g(4) = 2$.

Definición 6.3.2.3. Sea $G = (V, E)$ un grafo dirigido simple y sea $v \in V$.

(i) Se define el grado de entrada de v como

$$g^+(v) = |\{(u, v) \in E\}|$$

Es decir, es la cantidad de aristas de G que llegan a v.

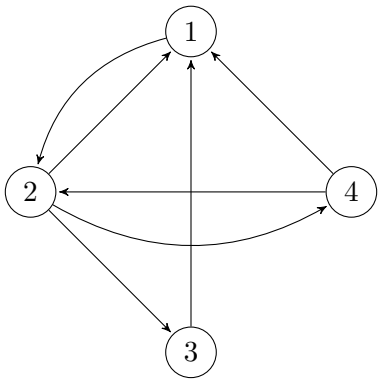
(ii) Se define el grado de salida de v como

$$g^-(v) = |\{(v, u) \in E\}|$$

Es decir, es la cantidad de aristas de G que parten de v.

(iii) Se define el grado de v como $g(v) = g^+(v) + g^-(v)$.

Ejemplo 6.3.2.4. Sea el grafo



Entonces $g^+(1) = 3$, $g^+(2) = 2$, $g^+(3) = g^+(4) = 1$ y $g^-(1) = 1$, $g^-(2) = 3$, $g^-(3) = 1$, $g^-(4) = 2$.

También podemos calcular el grado de un vértice a partir de las matrices de adyacencia e incidencia.

Proposición 6.3.2.5. Sea $G = (V, E)$ un grafo no dirigido tal que $V = \{v_1, v_2, \ldots, v_n\}$, y sean A e I sus matrices de adyacencia e incidencia respectivamente. Entonces:

(i) En la matriz de adyacencia A, $g(v_i) = \sum_{j=1}^{n} a_{ij}$. Es decir, contamos los 1 de la fila i.

(ii) En la matriz de incidencia I, $g(v_i) = \sum_{j=1}^{n} a_{ij}$. Es decir, contamos los 1 de la fila i.

Proposición 6.3.2.6. Sea $G = (V, E)$ un grafo dirigido tal que $V = \{v_1, v_2, \ldots, v_n\}$, y sean A e I sus matrices de adyacencia e incidencia respectivamente. Entonces:

(i) En la matriz de adyacencia A, $g^+(v_i) = \sum_{j=1}^{n} a_{ji}$ y $g^-(v_i) = \sum_{j=1}^{n} a_{ij}$. Es decir, para el grado de entrada contamos los 1 de la columna i y para el grado de salida contamos los 1 de la fila i.

(ii) En la matriz de incidencia I, $g^+(v_i) = \sum_{\substack{j=1 \\ a_{ij}>0}}^{n} a_{ij}$ y $g^-(v_i) = \sum_{\substack{j=1 \\ a_{ij}<0}}^{n} |a_{ij}|$. Es decir, para el grado de entrada contamos los 1 de la fila i y para el grado de salida contamos los -1 de la fila i.

Proposición 6.3.2.7. Sea $G = (V, E)$ un grafo sin bucles tal que $V = \{v_1, v_2, \ldots, v_n\}$ y $|E| = m$. Entonces,

$$\sum_{i=1}^{n} g(v_i) = 2m$$

Es decir, la suma de los grados de todos los vértices es igual al doble del número de aristas.

Demostración. Vamos a distinguir los casos en que el grafo es no dirigido y dirigido.

(i) Como en un grafo no dirigido sin bucles cada arista une dos vértices, si escribimos la matriz de incidencia de G comprobaremos que cada columna tiene exactamente dos 1. Así, como la suma de los grados de todos los vértices no es más que contar todos los 1 que tiene la matriz, habrá dos veces el número de columnas de la matriz. Como cada columna es una arista, habrá dos veces el número de aristas, esto es, $2m$.

(ii) Como en un grafo dirigido sin bucles cada arista une dos vértices, si escribimos la matriz de incidencia de G comprobaremos que cada columna tiene exactamente un 1 y un -1. Así, como la suma de los grados de todos los vértices no es más que contar todos los 1 y -1 que tiene la matriz, habrá dos veces el número de columnas de la matriz. Como cada columna es una arista, habrá dos veces el número de aristas, esto es, $2m$.

□

El siguiente resultado toma su nombre de la siguiente analogía: en una fiesta, el número de personas que estrecha la mano a una cantidad impar de personas es siempre par. En términos matemáticos lo reescribimos como:

Proposición 6.3.2.8 (Lema del apretón de manos)**.** Dado un grafo sin bucles, la cantidad de vértices impares es par.

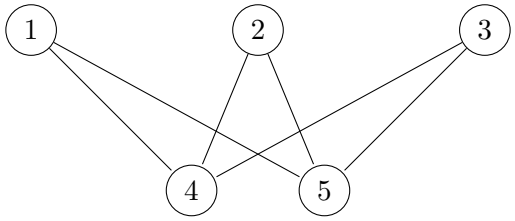
Demostración. Supongamos que hay r vértices impares. Denotemos por p a la suma de los grados de todos los vértices pares y por q a la suma de los grados de todos los vértices impares. Por la proposición anterior, $p+q$ es par, digamos $2m$. Además, p es un número par, ya que los vértices pares tienen grado par y la suma de grados pares es par. Por tanto, $q = 2m - p$ y la resta de números pares es par, luego q es par también. Pero q es la suma de grados impares, luego para que sea par esa suma, tiene que haber una cantidad par de vértices impares, es decir, r es par. □

6.3.3. Grafos bipartitos

Definición 6.3.3.1. Se dice que un grafo $G = (V, E)$ no dirigido simple es bipartito si existe una partición de V en dos conjuntos V_1 y V_2 de tal forma que

$$E = \{\{v_1, v_2\} : v_1 \in V_1, v_2 \in V_2\}$$

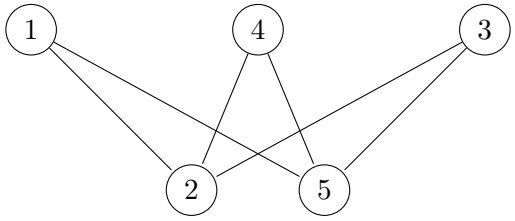
Ejemplo 6.3.3.2. El siguiente grafo es bipartito:



En efecto, existe una partición de $V = \{1, 2, 3, 4, 5\}$ formada por los conjuntos $V_1 = \{1, 2, 3\}$ y $V_2 = \{4, 5\}$ tal que los vértices de V_1 no son adyacentes entre sí, los vértices de V_2 no son adyacentes entre sí y para cada vértice de V_1 todos los vértices de V_2 son adyacentes a él. Observemos la forma que tiene la matriz de adyacencia asociada a este grafo:

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

Sin embargo, aunque el ser bipartito es una propiedad que se conserva bajo isomorfismos, el siguiente grafo, isomorfo al primero, que tiene la forma



tiene por matriz de adyacencia

$$A' = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

El siguiente resultado nos garantiza una forma de decidir si un grafo es bipartito o no en términos de su matriz de adyacencia.

Proposición 6.3.3.3. Sea $G = (V, E)$ un grafo no dirigido simple y A su matriz de adyacencia asociada. Entonces, son equivalentes:

(i) G es bipartito y la partición es $\{v_1, v_2, \ldots, v_r\}$, $\{v_{r+1}, v_{r+2}, \ldots, v_n\}$.

(ii)
$$A = \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix} = \begin{pmatrix} 0 & \cdots & 0 & 1 & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & 1 & \cdots & 1 \\ 1 & \cdots & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \cdots & 1 & 0 & \cdots & 0 \end{pmatrix},$$

donde A_1 tiene r filas y columnas, A_2 tiene r filas y $n - r$ columnas, A_3 tiene $n - r$ filas y r columnas y A_4 tiene $n - r$ filas y columnas.

Como hemos visto en el ejemplo anterior, no siempre la partición de V viene dada de manera lineal. La siguiente proposición generaliza este hecho.

Proposición 6.3.3.4. Sea $G = (V, E)$ un grafo no dirigido simple y A su matriz de adyacencia asociada. Entonces, son equivalentes:

(i) G es bipartito y la partición es $\{v_{i_1}, v_{i_2}, \ldots, v_{i_r}\}$, $\{v_{i_{r+1}}, v_{i_{r+2}}, \ldots, v_{i_n}\}$.

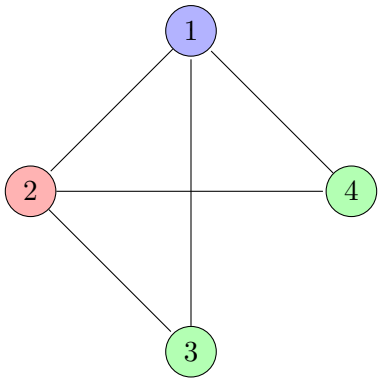
(ii) En A existen dos grupos de filas, $I_1 = \{i_1, i_2, \ldots, i_r\}$, $I_2 = \{i_{r+1}, i_{r+2}, \ldots, i_n\}$, de forma que
$$a_{ij} = \begin{cases} 1 & i \in I_1 \text{ y } j \in I_2 \\ 0 & i, j \in I_1 \text{ o } i, j \in I_2 \end{cases}$$

6.3.4. Coloración de grafos

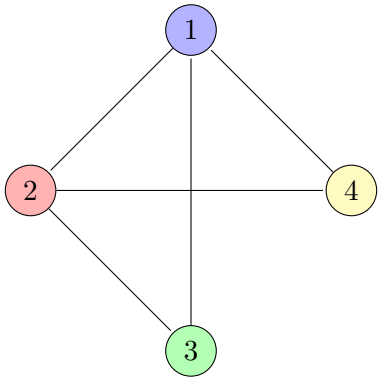
Definición 6.3.4.1. Sea $G = (V, E)$ un grafo no dirigido simple. Se dice que una coloración de G es una asignación de colores a cada vértice de G de forma que a cada vértice le corresponde un único color y dos vértices adyacentes no comparten el mismo color.

Si el grafo admite una coloración con k colores distintos, se dice que es k-coloreable.

Ejemplo 6.3.4.2. El siguiente grafo es 3-coloreable



Evidentemente, si es 3-coloreable, también es 4 coloreable



Definición 6.3.4.3. Dado un grafo simple G, se define el número cromático del grafo, y se denota $\chi(G)$, como

$$\chi(G) = \text{mín}\{k \in \mathbb{N} : G \text{ es } k\text{-coloreable}\}$$

Es decir, es el número mínimo de colores para su coloración.

Ejemplo 6.3.4.4. El grafo del ejemplo anterior tiene número cromático 3.

Observación 6.3.4.5. Sea $G = (V, E)$ un grafo no dirigido simple con $|V| = n$. Entonces,

(i) $E = \emptyset$ si y solo si G es 1-coloreable.

(ii) Si G es completo, entonces es n-coloreable.

(iii) Si G es bipartito, entonces es 2-coloreable.

Encontrar el número cromático de un grafo es un problema NP. Sin embargo, existen algoritmos heurísticos que permiten aproximarlo (en algunos casos incluso lo calculan exactamente). A este número lo llamamos número cromático aproximado, y lo denotamos $\chi'(G)$.

Proposición 6.3.4.6 (Algoritmo del más largo primero / Matula-Marble-Isaacson)**.** Sea $G = (V, E)$ un grafo no dirigido simple.

1. Calcular $g(v)$ para todo $v \in V$.
2. Reordenar V de manera decreciente según los grados de los vértices calculados en el paso 1.

3. Definir v como el primer vértice de V.

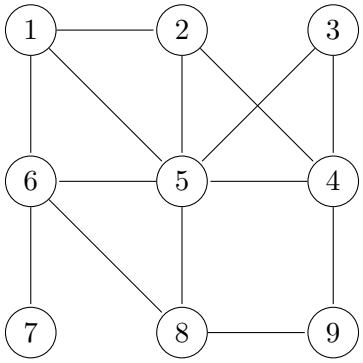
4. Obtener el conjunto $A = \{v_{i_1}, \ldots, v_{i_m}\}$ formado por todos los vértices de V que no son adyacentes a v.

5. Si v_{i_j} es adyacente a algún vértice $v_{i_1}, \ldots, v_{i_{j-1}}$, eliminarlo de A.

6. Colorear v y los vértices de A de un mismo color que no se haya utilizado previamente. Hacer $V = V - A$.

7. Si $V \neq \emptyset$, repetir los pasos 1-6. Si $V = \emptyset$, el número cromático aproximado, $\chi'(G)$, será el número de colores utilizados en el algoritmo.

Ejemplo 6.3.4.7. Consideremos el siguiente grafo:



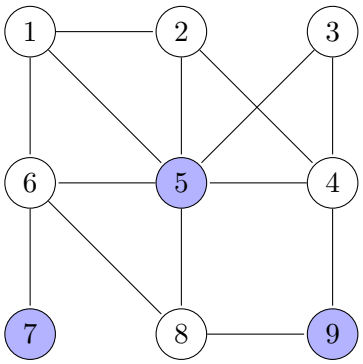
Vamos a aplicar el algoritmo del más largo primero para obtener el número cromático aproximado.

(i) Calculamos el grado de todos los vértices: $g(1) = 3$, $g(2) = 3$, $g(3) = 2$, $g(4) = 4$, $g(5) = 6$, $g(6) = 4$, $g(7) = 1$, $g(8) = 3$, $g(9) = 2$.

(ii) Reordenamos vértices de mayor a menor según su grado: $V = \{5, 4, 6, 1, 2, 8, 3, 9, 7\}$.

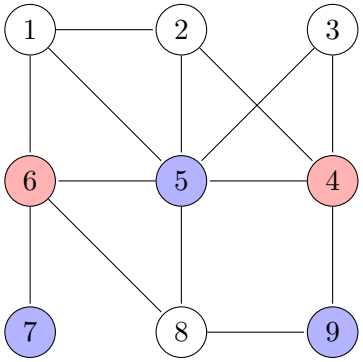
(iii) El conjunto de vértices adyacentes a 5 es, ordenado, $\{4, 6, 1, 2, 8, 3\}$. Por tanto, el conjunto de vértices no adyacentes a 5 es $\{9, 7\}$.

(iv) Asignamos un color, digamos azul, a 5. Al 9, al ser el primer elemento del conjunto del paso anterior le asignamos también este color. Como 7 no es adyacente a 9, también le asignamos el mismo color.



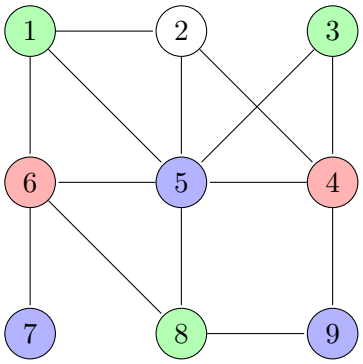
(v) Repetimos los pasos anteriores, desde (iii), con el subgrafo formado por los vértices {4, 6, 1, 2, 8, 3} sin repetir los colores ya utilizados. El conjunto de vértices no adyacentes a 4 es {6, 1, 8}.

(vi) Asignamos un color a 4, digamos rojo. Al 6 le asignamos el mismo color. El 1 es adyacente a 6, luego no le asignamos color. El 8 es adyacente a 6, por lo que no le asignamos color.

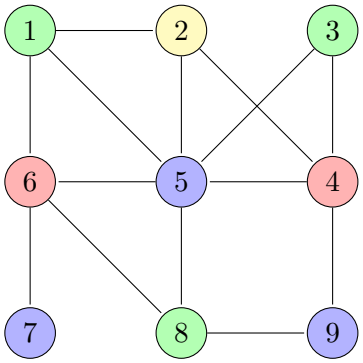


(vii) De nuevo, repetimos los pasos anteriores con el subgrafo formado por los vértices {1, 2, 8, 3} sin repetir los colores ya utilizados. El conjunto de vértices no adyacentes a 1 es {8, 3}.

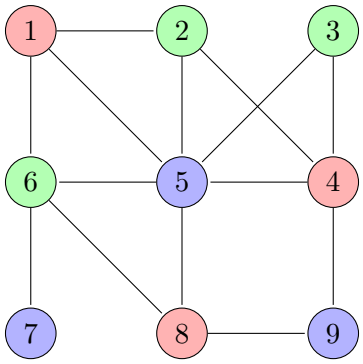
(viii) Asignamos un color a 1, digamos verde. Al 8 y al 3 les asignamos el mismo color.



(ix) Como ya solo queda el vértice 2, le asignamos un color no utilizado. Digamos el amarillo.



Por tanto, el número cromático aproximado es 4. Sin embargo, el número cromático es 3, ya que podemos encontrar la coloración



6.4. Caminos

6.4.1. Introducción

Dedicaremos esta sección a los caminos en grafos. Un camino es una secuencia ordenada de aristas que parten de un vértice y terminan en otro. Gracias a los caminos, definiremos un grafo conexo como un grafo para el que todo par de vértices está conectado por un camino. Dentro de los caminos, los que juegan un papel más importante en esta unidad son los caminos cerrados, es decir, caminos que comienzan y terminan en el mismo vértice. Hay dos tipos muy importantes de caminos cerrados: los circuitos y los ciclos. Los circuitos no repiten aristas y los ciclos no repiten vértices. Los circuitos más importantes son los eulerianos, que pasan por todas las aristas del grafo exactamente una vez y dan lugar a los grafos eulerianos. Los ciclos más importantes son los hamiltonianos, que pasan por todos los vértices del grafo exactamente una vez y dan lugar a los grafos hamiltonianos.

6.4.2. Caminos, circuitos y ciclos

Definición 6.4.2.1. Dado un grafo no dirigido $G = (V, E)$ y dados dos vértices $v, v' \in V$, se dice que un camino de longitud r entre v y v' es una secuencia ordenada de aristas de E, $(a_1, a_2, \ldots, a_r)$, de forma que

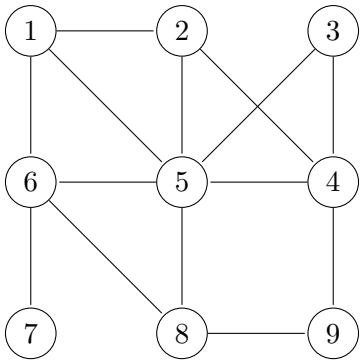
$$a_1 = \{v, v_{i_1}\}, a_2 = \{v_{i_1}, v_{i_2}\}, \ldots, a_{r-1} = \{v_{i_{r-2}}, v_{i_{r-1}}\}, a_r = \{v_{i_{r-1}}, v'\}$$

A veces el camino entre v y v' se denota

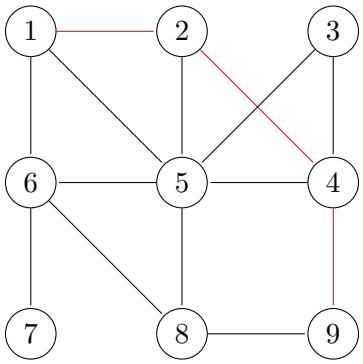
$$v \to v_{i_1} \to v_{i_2} \to \ldots \to v_{i_{r-2}} \to v_{i_{r-1}} \to v'$$

Nótese que algunos vértices del camino pueden estar repetidos.

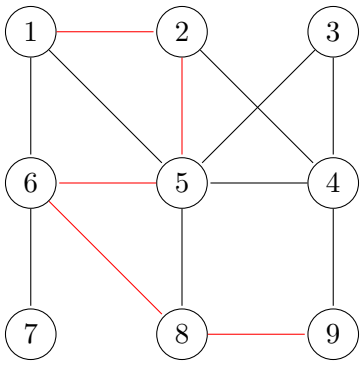
Ejemplo 6.4.2.2. Sea el grafo



Entonces, un camino entre 1 y 9 es el siguiente:



Pero otro camino puede ser:



Esto pone de manifiesto que un camino entre dos vértices no es único.

Proposición 6.4.2.3. Sea $G = (V, E)$ un grafo no dirigido sin aristas repetidas, y sea A su matriz de adyacencia. Entonces, la entrada (i, j) de A^k, $k \geq 1$, es el número de caminos de longitud k entre v_i y v_j. Además, la entrada (i, i) de A^2 es $g(v_i)$.

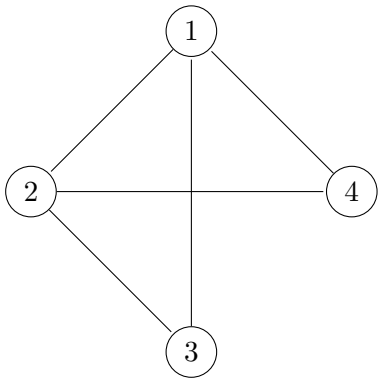
Definición 6.4.2.4. Dado un grafo no dirigido $G = (V, E)$, se dice que un camino es simple si todos los vértices del camino son distintos.

Definición 6.4.2.5. Dado un grafo no dirigido $G = (V, E)$, se dice que G es conexo si existe un camino entre cada par de vértices.

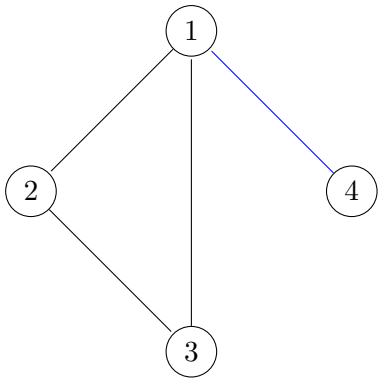
Una arista que, al ser eliminada del grafo (solo la arista, no sus extremos), hace que el grafo deje de ser conexo, se llama puente.

Ejemplo 6.4.2.6.

(i) El siguiente grafo es conexo:



(ii) Dado el siguiente grafo, la arista $\{1, 4\}$ es una arista puente:

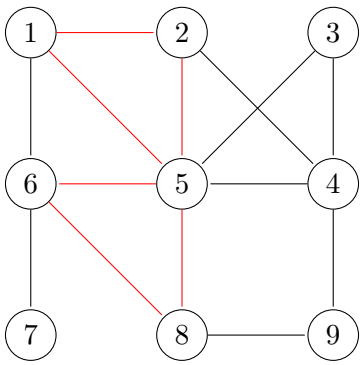


Definición 6.4.2.7. Dado un grafo no dirigido simple $G = (V, E)$, se dice que un camino es cerrado si el vértice inicial y el vértice final son el mismo.

Definición 6.4.2.8. Dado un grafo no dirigido simple $G = (V, E)$, se dice que un camino cerrado es un circuito si todas las aristas son distintas.

Definición 6.4.2.9. Dado un grafo no dirigido simple $G = (V, E)$, se dice que un camino cerrado es un ciclo si todos los vértices, salvo el inicial, son distintos.

Ejemplo 6.4.2.10. El camino cerrado $1 \to 2 \to 5 \to 8 \to 6 \to 5 \to 1$ es un circuito:



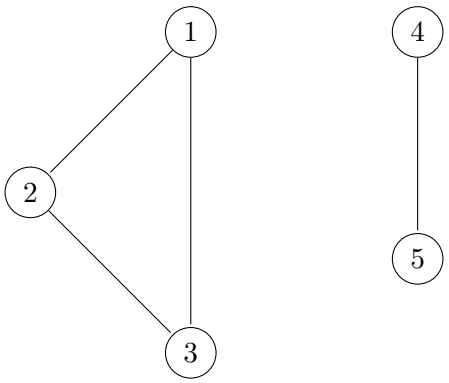
Sin embargo, no es un ciclo, ya que repite el vértice 5.

Observación 6.4.2.11. Un circuito no tiene por qué ser un ciclo, ya que puede repetir vértices como hemos visto en el ejemplo anterior. Sin embargo, todo ciclo es un circuito, ya que al no repetir vértices, condiciona que no pueda repetir aristas. En efecto, si suponemos que la arista $\{v_i, v_j\}$ aparece repetida en el ciclo, esto quiere decir que tanto v_i como v_j aparecen repetidos, y está garantizado que al menos uno de ellos no es el vértice inicial.

Dado un grafo no dirigido $G = (V, E)$ y dos vértices $v, v' \in V$, que v y v' estén conectados por un camino es una relación de equivalencia. Lo interesante de que sea una relación de equivalencia radica en que la clase de v, $[v]$, es el conjunto de todos los vértices para los que existe un camino entre v y ellos, y eso motiva la siguiente definición.

Definición 6.4.2.12. Dado un grafo no dirigido $G = (V, E)$ y un vértice $v \in V$, consideremos el conjunto de todos los vértices $v' \in V$ tales que existe un camino entre v y v', es decir, la clase de equivalencia de v. La denotamos $K(v)$ y se denomina componente conexa del vértice v.

Ejemplo 6.4.2.13. El siguiente grafo tiene dos componentes conexas:



Estas componentes son $K(1) = K(2) = K(3)$ y $K(4) = K(5)$.

Observación 6.4.2.14. Si el grafo no dirigido es conexo, habrá una única componente conexa que será el propio grafo.

Definición 6.4.2.15. Dado un grafo dirigido $G = (V, E)$ y dados dos vértices $v, v' \in V$, se dice que un camino de longitud r de v a v' es una secuencia ordenada de aristas de E, $(a_1, a_2, \ldots, a_r)$, de forma que

$$a_1 = (v, v_{i_1}),\ a_2 = (v_{i_1}, v_{i_2}),\ \ldots,\ a_{r-1} = (v_{i_{r-2}}, v_{i_{r-1}}),\ a_r = (v_{i_{r-1}}, v')$$

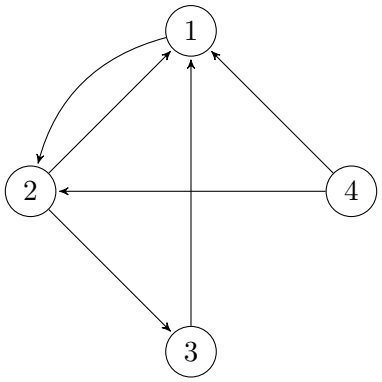
A veces el camino de v a v' se denota

$$v \to v_{i_1} \to v_{i_2} \to \ldots \to v_{i_{r-2}} \to v_{i_{r-1}} \to v'$$

Nótese que algunos vértices del camino pueden estar repetidos.

Definición 6.4.2.16. Dado un grafo dirigido $G = (V, E)$ y dados dos vértices $v, v' \in V$, se dice que el par formado por v y v' es fuertemente conexo si existe un camino de v a v' y un camino de v' a v.

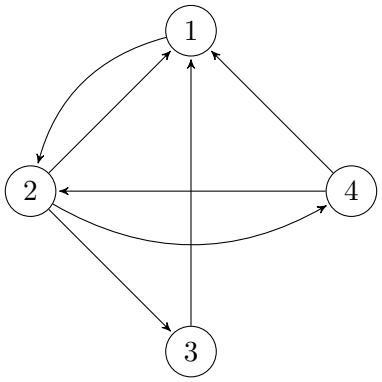
Ejemplo 6.4.2.17. Consideremos el siguiente grafo:



El par formado por 1 y 3 es fuertemente conexo, pues existen los caminos $1 \to 2 \to 3$ y $3 \to 1$. Sin embargo, el par formado por 1 y 4 no es fuertemente conexo, ya que no existe camino de 1 a 4.

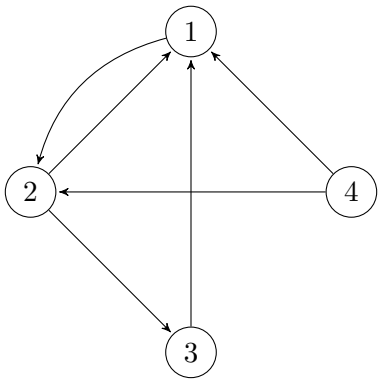
Definición 6.4.2.18. Dado un grafo dirigido $G = (V, E)$, se dice que es fuertemente conexo si todo par de vértices v, $v' \in V$ es fuertemente conexo.

Ejemplo 6.4.2.19. El siguiente grafo es fuertemente conexo:

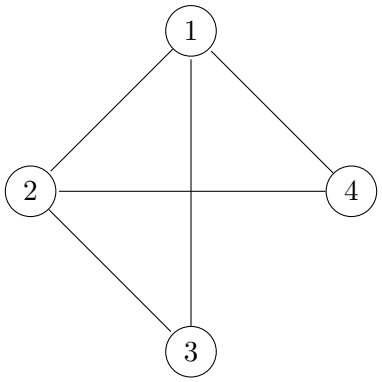


Definición 6.4.2.20. Dado un grafo dirigido $G = (V, E)$, se dice que es débilmente conexo si su grafo no dirigido subyacente es conexo.

Ejemplo 6.4.2.21. Consideremos el grafo:



Este grafo es débilmente conexo, pues su grafo subyacente es conexo:



Sin embargo, no es fuertemente conexo, ya que el par formado por 1 y 4 no lo es.

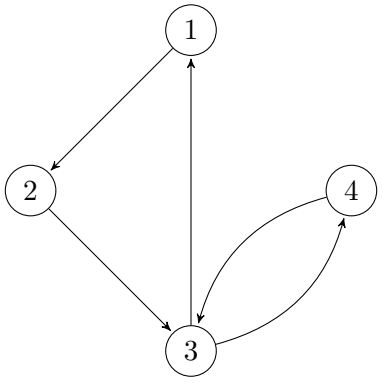
Observación 6.4.2.22. Si un grafo es fuertemente conexo, entonces, en particular, es débilmente conexo. Sin embargo, como hemos visto en el ejemplo anterior, un grafo débilmente conexo no tiene por qué ser fuertemente conexo.

Definición 6.4.2.23. Dado un grafo dirigido $G = (V, E)$, se dice que un camino es cerrado si el vértice inicial y el vértice final son el mismo.

Definición 6.4.2.24. Dado un grafo dirigido $G = (V, E)$, se dice que un camino cerrado es un circuito si todas las aristas son distintas.

Definición 6.4.2.25. Dado un grafo dirigido $G = (V, E)$, se dice que un camino cerrado es un ciclo si todos los vértices son distintos.

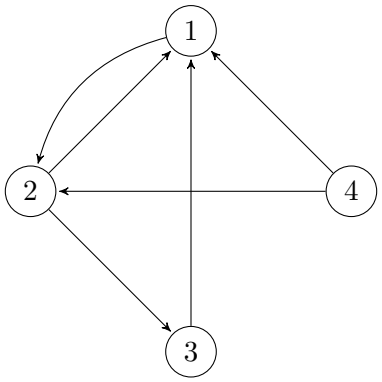
Observación 6.4.2.26. Como para grafos no dirigidos, tenemos de nuevo que todo ciclo es un circuito y que no todo circuito es necesariamente un ciclo. Por ejemplo, en el circuito $1 \to 2 \to 3 \to 4 \to 3 \to 1$ observamos que se pasa dos veces por el vértice 3:



Dado un grafo dirigido $G = (V, E)$ y dos vértices v, $v' \in V$, que v y v' sean un par fuertemente conexo es una relación de equivalencia. Esto motiva la siguiente definición.

Definición 6.4.2.27. Dado un grafo $G = (V, E)$ y un vértice $v \in V$, consideremos el conjunto de todos los vértices $v' \in V$ tales que v y v' son un par fuertemente conexo, es decir, la clase de equivalencia de v. La denotamos $K(v)$ y se denomina componente fuertemente conexa del vértice v.

Ejemplo 6.4.2.28. Sea el grafo:



Este grafo tiene dos componentes fuertemente conexas: $K(1) = K(2) = K(3)$ y $K(4)$.

Observación 6.4.2.29. Si el grafo es fuertemente conexo, habrá una única componente fuertemente conexa que será el propio grafo.

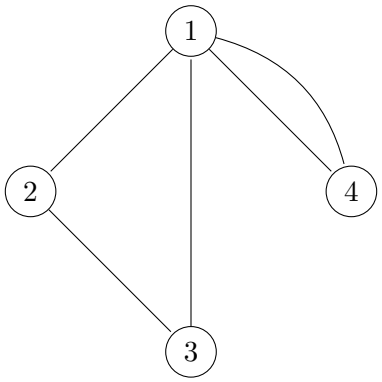
Proposición 6.4.2.30. Sea $G = (V, E)$ un grafo dirigido sin aristas repetidas, y sea A su matriz de adyacencia. Entonces, la entrada (i, j) de A^k, $k \geq 1$, es el número de caminos de longitud k de v_i a v_j.

6.4.3. Grafos eulerianos

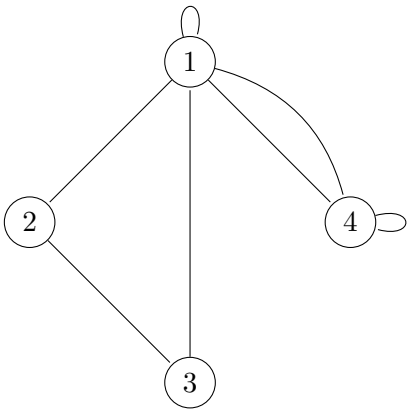
Definición 6.4.3.1. Sea $G = (V, E)$ un grafo no dirigido. Se dice que un camino es euleriano si cada arista de E aparece exactamente una vez en el camino. Si el camino euleriano es cerrado se dice que es un circuito euleriano.

Si G tiene un circuito euleriano, se dice que es un grafo euleriano.

Ejemplo 6.4.3.2. El siguiente grafo es euleriano, porque tiene un ciclo que pasa por todas las aristas exactamente una vez: $1 \to 4 \to 1 \to 2 \to 3 \to 1$.



Observación 6.4.3.3. Si el grafo tuviese bucles y el grafo resultante de eliminar los bucles es euleriano, entonces el grafo inicial es euleriano. Utilizando el ejemplo anterior podemos ver por qué.

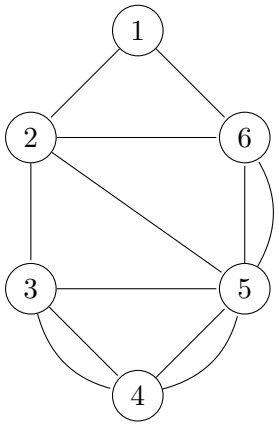


En efecto, si utilizamos el mismo camino que hemos encontrado antes y añadimos, tras la primera visita al vértice con bucle, dicho bucle, habremos pasado una vez ya por esta arista. En nuestro caso, el ciclo sería: $1 \to 1 \to 4 \to 4 \to 1 \to 2 \to 3 \to 1$.

Proposición 6.4.3.4. Un grafo conexo no euleriano tiene un camino euleriano si y solo si tiene exactamente dos vértices de grado impar.

Proposición 6.4.3.5. Un grafo conexo y sin bucles es euleriano si y solo si cada vértice tiene grado par.

Ejemplo 6.4.3.6. Consideremos el siguiente grafo:



Este grafo tiene todos sus vértices de grado par y, en este caso, a simple vista nos damos cuenta de que es conexo. Por tanto, el grafo es euleriano.

Observación 6.4.3.7. En la próxima unidad veremos dos algoritmos que, dado un grafo, nos permiten determinar si es o no conexo. No obstante, para casos como el grafo del ejemplo anterior, una breve justificación de su conexión, si el objetivo del problema no es garantizar que el grafo sea conexo, es suficiente.

El siguiente algoritmo nos permite encontrar el circuito euleriano de un grafo en caso de que este sea euleriano.

Proposición 6.4.3.8 (Algoritmo de Fleury)**.**

1. Comprobar que el grafo es conexo y cada vértice es de grado par.

2. Tomar un vértice v cualquiera.

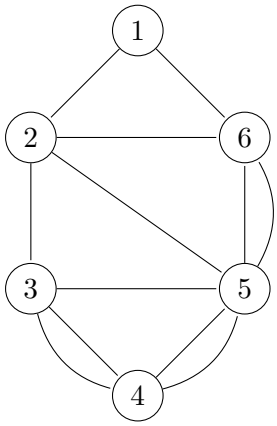
3. Elegir una arista $\{v, v'\}$ que no sea puente a menos que no quede alternativa.

4. Eliminar la arista.

5. Hacer $v = v'$ y repetir los pasos 3-5 hasta que nos quedemos sin aristas.

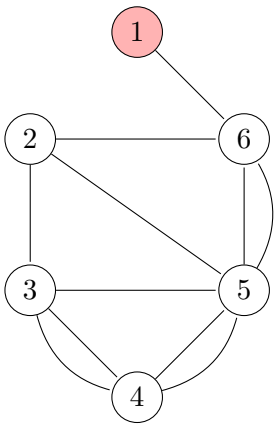
6. El circuito euleriano es el formado por las aristas en el orden en el que las hemos eliminado.

Ejemplo 6.4.3.9. Consideremos el grafo del último ejemplo y apliquemos el algoritmo de Fleury para encontrar un circuito euleriano.

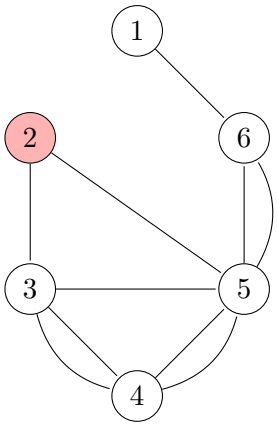


(i) El grafo es conexo y todos los vértices tienen grado par.

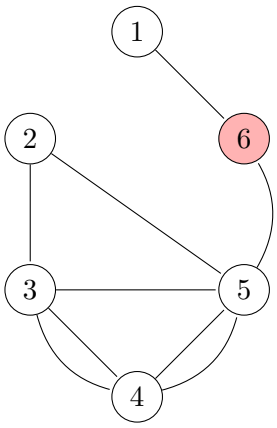
(ii) Elegimos como primer vértice el vértice 1. Como ninguna arista es puente, tomamos $e_{1,2}$.



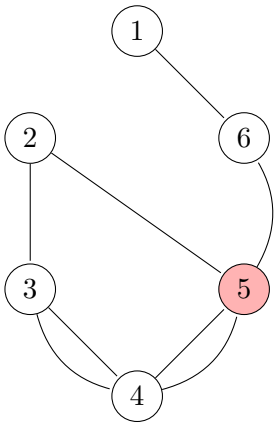
(ii) Nos situamos sobre el vértice 2. Como ninguna arista es puente, tomamos cualquiera que no hayamos utilizado anteriormente. En general, tomaríamos la arista $e_{2,3}$, pero para mostrar que no importa la arista que tomemos, cojamos $e_{2,6}$.



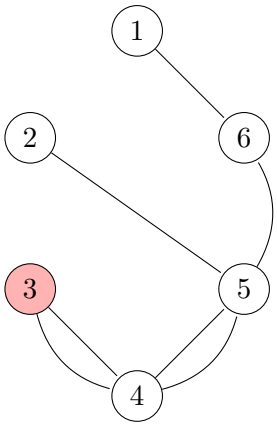
(iii) La arista $e_{1,6}$ es puente, así que, como hay otras aristas que inciden en el vértice 6, debemos tomar otra. Por ejemplo, $e^1_{5,6}$.



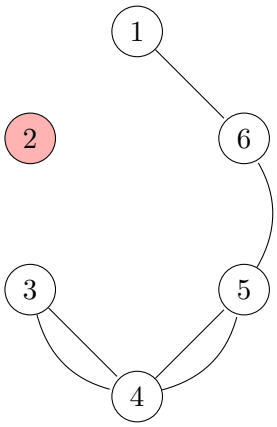
(iv) Seguimos el proceso sin detenernos demasiado unos cuantos pasos más.



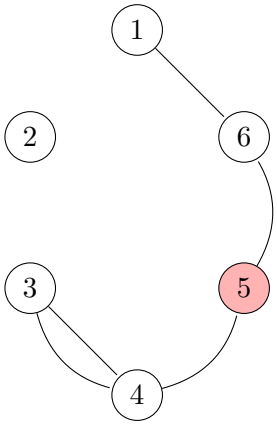
(v)



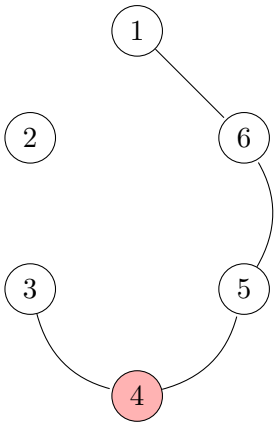
(vi) Como desde el vértice 2 ya solo queda una arista puente, la tomamos.



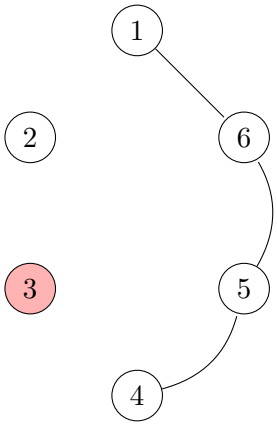
(vii)



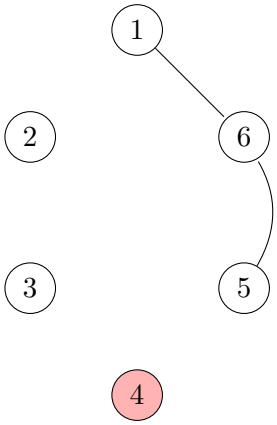
(viii)



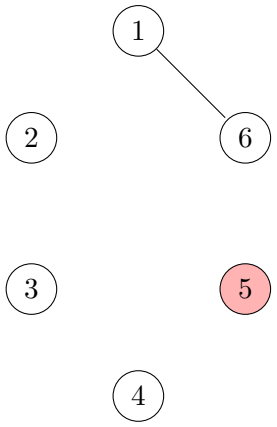
(ix)



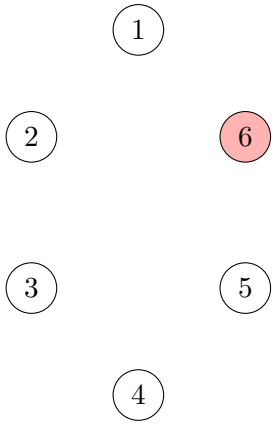
(x)



(xi)



(xii)



(xiii) Como ya tenemos un grafo sin aristas, el algoritmo ha terminado. El circuito euleriano encontrado es:

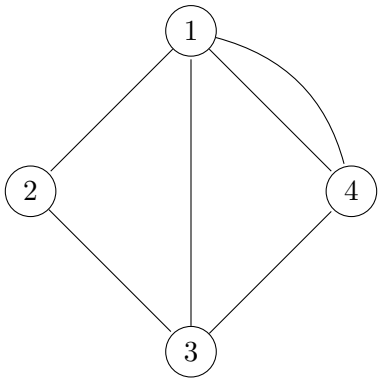
$$1 \to 2 \to 6 \to 5 \to 3 \to 2 \to 5 \to 4 \to 3 \to 4 \to 5 \to 6 \to 1$$

6.4.4. Grafos hamiltonianos

Definición 6.4.4.1. Sea $G = (V, E)$ un grafo no dirigido. Se dice que un camino es hamiltoniano si pasa por cada vértice de V exactamente una vez. Si el camino hamiltoniano es cerrado, se dice que es un ciclo hamiltoniano.

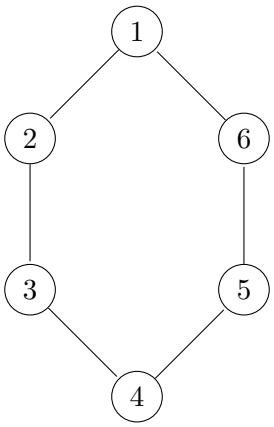
Si G tiene un ciclo hamiltoniano, se dice que es un grafo hamiltoniano.

Ejemplo 6.4.4.2. El siguiente grafo es hamiltoniano, pues contiene al ciclo hamiltoniano $1 \to 2 \to 3 \to 4 \to 1$.



Teorema 6.4.4.3 (Dirac)**.** Sea $G = (V, E)$ un grafo no dirigido simple tal que $|V| = n \geq 3$ y tal que para todo $v \in V$, $g(v) \geq \frac{n}{2}$. Entonces, G es hamiltoniano.

Ejemplo 6.4.4.4. El grafo del ejemplo anterior tiene todos sus vértices de grado mayor o igual que 2, que es la mitad del número de vértices. Por tanto, por el teorema de Dirac, podríamos haber concluido que el grafo es hamiltoniano sin necesidad de encontrar un ciclo hamiltoniano. No obstante, un grafo puede ser hamiltoniano y no satisfacer las hipótesis de dicho teorema, como, por ejemplo, el siguiente grafo:



Tiene 6 vértices, luego la mitad de 6 es 3. Sin embargo, el grado de cada vértice es $2 < 3$. Pero evidentemente es un grafo hamiltoniano.

6.5. Cuestionario

Ejercicio 48. El grafo cuyo conjunto de aristas es

$$E = \{\{1, 2\}, \{2, 2\}\}$$

es dirigido.

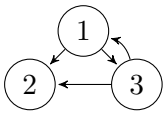
(a) Verdadero

(b) Falso

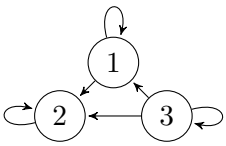
Ejercicio 49. ¿Con qué grafo se corresponde la siguiente matriz de adyacencia?

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

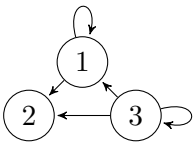
(a)



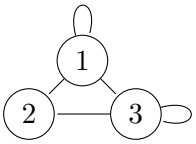
(b)



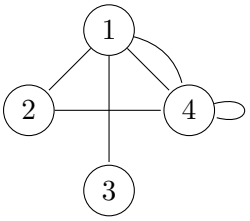
(c)

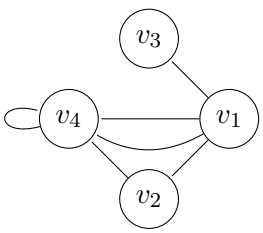


(d)



Ejercicio 50. Los siguientes grafos son isomorfos:





(a) Verdadero

(b) Falso

Ejercicio 51. Según lo que hemos visto en la unidad, una matriz de incidencia no puede representar multigrafos.

(a) Verdadero

(b) Falso

Ejercicio 52. Según la siguiente matriz de adyacencia

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

el grado de entrada del vértice 3 es:

(a) 0

(b) 1

(c) 2

(d) 3

Ejercicio 53. Si la suma de los grados de todos los vértices de un grafo sin bucles es 14, ¿cuántas aristas tiene el grafo?

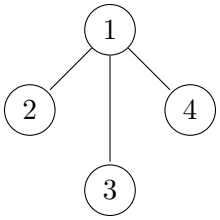
(a) 28

(b) 14

(c) Depende de si el grafo es dirigido o no dirigido

(d) 7

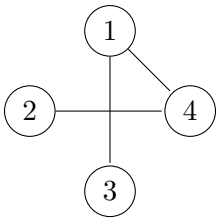
Ejercicio 54. El siguiente grafo es bipartito:



(a) Verdadero

(b) Falso

Ejercicio 55. ¿Cuál es el número cromático del siguiente grafo?



(a) 1

(b) 2

(c) 3

(d) 4

Ejercicio 56. Sea el grafo $G = (V, E)$, donde

$$V = \{1, 2, 3, 4, 5, 6\}$$

y

$$E = \{\{1, 1\}, \{1, 2\}, \{1, 4\}, \{2, 4\}, \{3, 3\}, \{3, 6\}, \{3, 6\}, \{4, 5\}, \{6, 6\}\}$$

¿Cuántas componentes conexas tiene?

(a) 0

(b) 1

(c) 2

(d) 3

Ejercicio 57. El siguiente camino sobre un grafo no dirigido simple es un ciclo euleriano:

$$1 \to 2 \to 4 \to 3 \to 5 \to 2 \to 5 \to 1$$

(a) Verdadero

(b) Falso

Capítulo 7

Árboles. Algoritmos en grafos

7.1. Introducción

En esta unidad vamos a estudiar tres tipos de algoritmos para resolver algunos de los problemas más importantes de la teoría de grafos. Para ello, dedicaremos el comienzo de la primera sección a estudiar en qué consiste un árbol, es decir, un grafo conexo que no contiene ciclos, y los conceptos más importantes relacionados con estos, como el de árbol generador de un grafo G, que consiste en un grafo con los mismos vértices de G que es árbol. Tras ello, veremos dos algoritmos, *DFS* y *BFS* (búsqueda en profundidad y búsqueda en anchura respectivamente), que nos permitirán decidir si un grafo es conexo o no y, en caso de que no lo sea, encontrar todas sus componentes conexas. En el segundo apartado estudiaremos el concepto de árbol generador mínimo para un grafo valorado, es decir, un árbol generador cuya suma de pesos de las aristas es la mínima posible, y veremos dos algoritmos para obtener este árbol generador mínimo: Kruskal y Prim. Finalmente, veremos el algoritmo de Dijkstra, que nos permitirá encontrar el camino mínimo entre dos vértices de un grafo valorado.

7.2. Algoritmos para comprobar la conexión

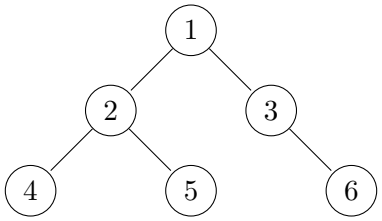
7.2.1. Introducción

En esta primera sección dedicaremos la primera parte a ver en qué consiste un árbol y todos los conceptos relacionados con éste, como los niveles, la altura, la raíz y las hojas. También veremos que, dado un grafo, un árbol generador es un árbol con el mismo conjunto de vértices que el grafo y cuyo conjunto de aristas es subconjunto del del grafo. El resto de la sección la dedicaremos a estudiar los dos algoritmos que nos permiten decidir si un grafo es conexo o no y, en caso de que no lo sea, encontrar todas sus componentes conexas. Estos dos algoritmos son el *DFS*, de búsqueda en profundidad, y el *BFS*, de búsqueda en anchura. Ambos algoritmos son exhaustivos, pues exploran todos los vértices del grafo.

7.2.2. Árboles

Definición 7.2.2.1. Sea G un grafo. Se dice que G es un árbol (o árbol no dirigido) si es conexo y no tiene ciclos (es acíclico).

Ejemplo 7.2.2.2. El siguiente grafo es un árbol:



Proposición 7.2.2.3. Sobre un grafo simple $G = (V, E)$, son equivalentes:

(i) G es un árbol.

(ii) G es conexo y $|E| = |V| - 1$.

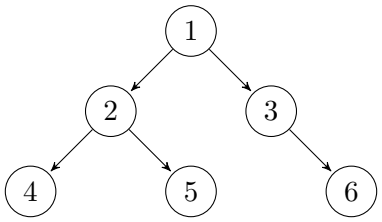
(iii) G es acíclico y $|E| = |V| - 1$.

(iv) G es conexo y cada arista es puente.

(v) Existe un único camino simple entre cada par de vértices de G.

Definición 7.2.2.4. Se dice que un grafo dirigido G es un árbol dirigido si su grafo no dirigido subyacente es un árbol.

Ejemplo 7.2.2.5. El siguiente grafo es un árbol dirigido:



Definición 7.2.2.6. Sea G un árbol dirigido. Se dice que un vértice v es raíz del árbol si el grado de entrada $g^+(v) = 0$.

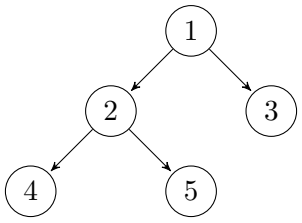
Definición 7.2.2.7. Sea G un árbol dirigido. Se dice que un vértice v es una hoja del árbol si el grado de salida $g^-(v) = 0$.

Definición 7.2.2.8. Sea G un árbol. Se dice que un vértice v está en el nivel k si el número de aristas que hay en el camino que va desde la raíz a v es k.

Definición 7.2.2.9. Sea G un árbol dirigido. Se dice que un vértice v está en el nivel k si el número de aristas que hay en el camino que va desde la raíz a v es k.

Definición 7.2.2.10. Sea G un árbol dirigido. Se llama altura de G al mayor de todos los niveles.

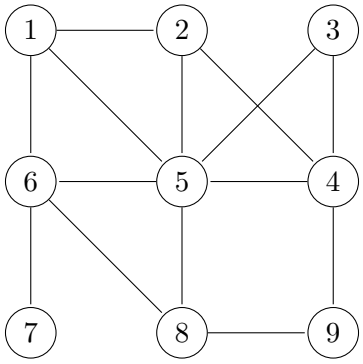
Ejemplo 7.2.2.11. Consideremos el árbol dirigido del ejemplo 7.2.2.5:



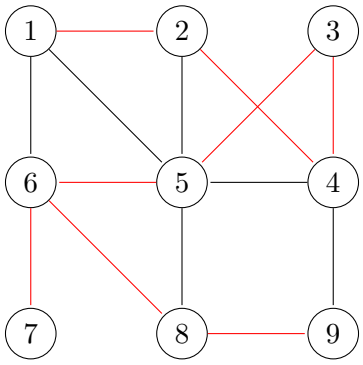
Este árbol tiene altura 3. En el nivel 0 se encuentra el vértice 1. Este vértice es la única raíz del árbol. En el nivel 1 se encuentran los vértices 2 y 3. En el nivel 2 se encuentran los vértices 4 y 5. Los vértices 3, 4 y 5 son las hojas del árbol.

Definición 7.2.2.12. Sea $G = (V, E)$ un grafo simple y $T = (V, E')$ un grafo tal que $E' \subseteq E$. Se dice que T es un árbol generador (o recubridor, o de expansión) de G si T es un árbol.

Ejemplo 7.2.2.13. Consideremos el siguiente grafo simple G:



Entonces, el grafo cuyas aristas están en color rojo es un árbol generador de G:



7.2.3. Algoritmo DFS

El algoritmo *DFS* (*depth first search*) sirve, principalmente, para comprobar si un grafo es conexo buscando en profundidad.

Proposición 7.2.3.1 (Algoritmo *DFS*)**.** Sea $G = (V, E)$ un grafo no dirigido.

1. Tomar un vértice $v \in V$ cualquiera que no haya sido visitado.

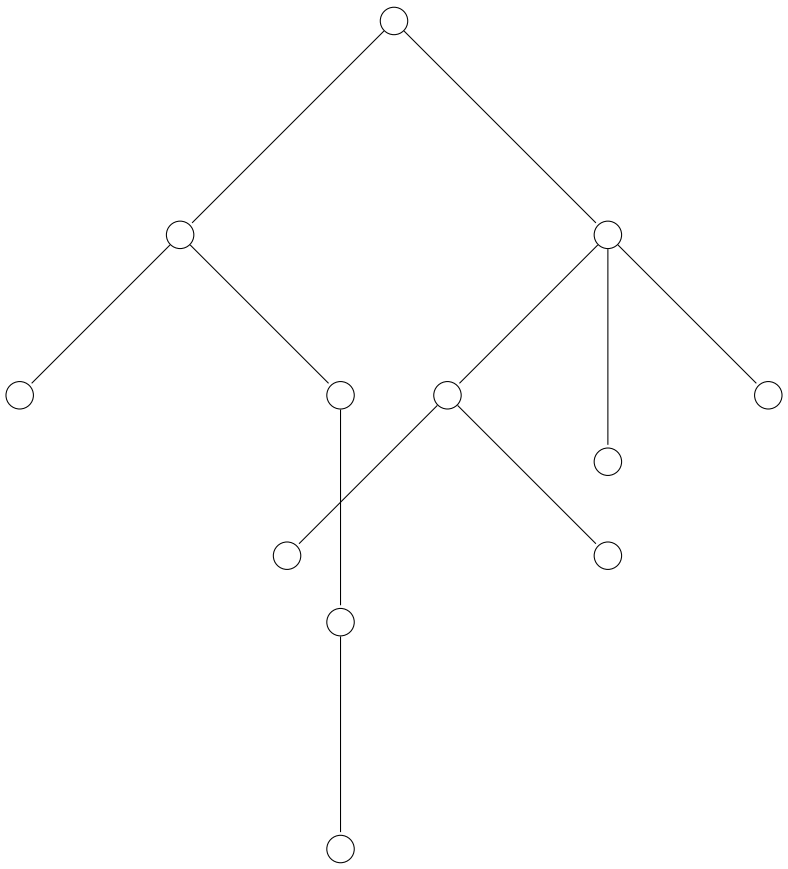
2. Encontrar todos los vértices no visitados adyacentes a v y escoger uno de ellos, u. Si no hay vértices adyacentes, volver al último vértice visitado para el cuál queden vértices adyacentes no visitados y escoger uno de ellos, u. Si no quedan vértices adyacentes a ningún vértice visitado, ir al paso 5.

3. Marcar la arista $\{v, u\}$ y considerar u como visitado.

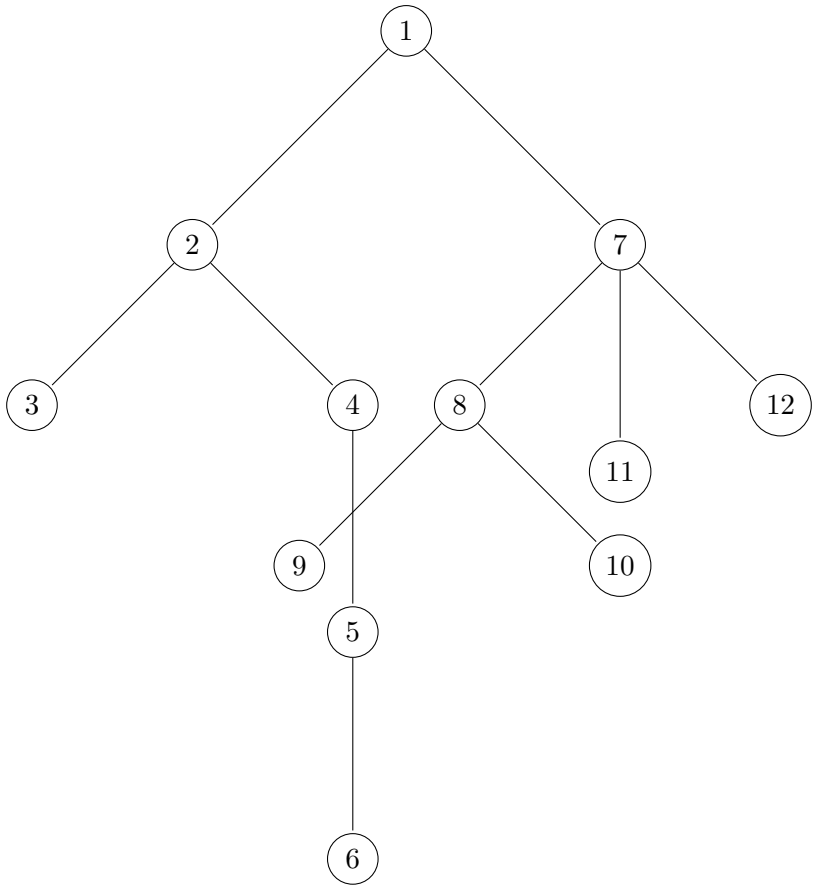
4. Si el conjunto de vértices no visitados adyacentes a u no es vacío, hacer $v = u$ y volver al paso 2. Si es vacío, volver al paso 2.

5. Si todos los vértices de V han sido visitados, G es conexo. Si no todos han sido visitados, G no es conexo. Para encontrar todas las componentes conexas bastará con volver al paso 1. Las veces que hagamos el paso 1 será la cantidad de componentes conexas del grafo.

Ejemplo 7.2.3.2. Consideremos el siguiente grafo:



Si marcamos los vértices según el orden que recorremos al aplicar el algoritmo *DFS*, nos queda de la siguiente manera:



Al haber podido marcar todos los vértices, el grafo es conexo.

7.2.4. Algoritmo BFS

El algoritmo *BFS* (*breadth first search*) sirve, principalmente, para comprobar si un grafo es conexo buscando en anchura.

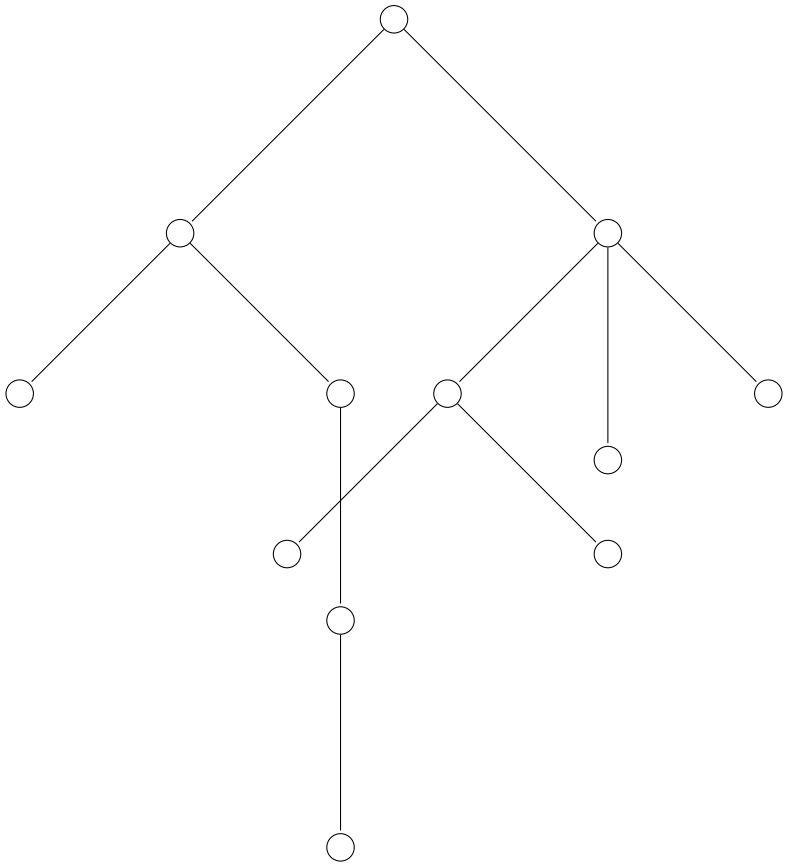
Proposición 7.2.4.1 (Algoritmo *BFS*)**.** Sea $G = (V, E)$ un grafo no dirigido.

1. Tomar un vértice $v \in V$ cualquiera y definir el conjunto $A = \{v\}$. Eliminar v de V.

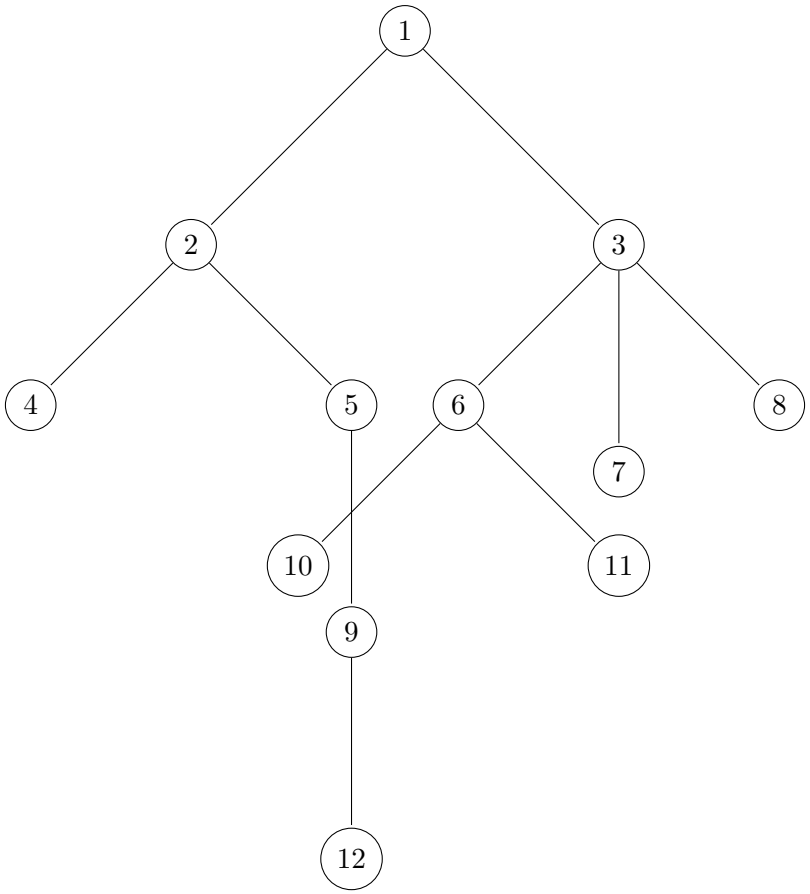
2. Encontrar todos los vértices adyacentes a los vértices de A, digamos $\{v_1, v_2, \ldots, v_k\}$ y redefinir A como $A = \{v_1, v_2, \ldots, v_k\}$. Eliminar $v_1, v_2, \ldots, v_k$ de V. Si $A = \emptyset$, ir al paso 3. Si no, repetir el paso 2.

3. Si $V = \emptyset$, G es conexo. Si no, G no es conexo. Para encontrar todas las componentes conexas bastará con volver al paso 1. Las veces que hagamos el paso 1 será la cantidad de componentes conexas del grafo.

Ejemplo 7.2.4.2. Consideremos el siguiente grafo:



Si marcamos los vértices según el orden que recorremos al aplicar el algoritmo *BFS*, nos queda de la siguiente manera:



Al haber podido marcar todos los vértices, el grafo es conexo.

7.3. Algoritmos para encontrar el árbol generador mínimo

7.3.1. Introducción

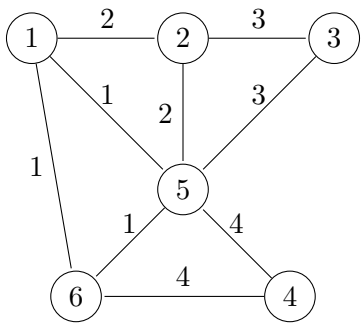
En esta sección mostraremos que una matriz de pesos es una matriz similar a la de adyacencia para grafos valorados cuyas entradas consisten en los pesos de cada arista. Definiremos el árbol generador mínimo asociado a un grafo como el árbol generador cuyo peso, es decir, la suma de pesos de todas sus aristas, es mínimo. Finalmente, veremos dos algoritmos que nos permiten obtener un árbol generador mínimo asociado a un grafo no dirigido, valorado, conexo y simple: el algoritmo de Kruskal y el algoritmo de Prim.

7.3.2. Conceptos preliminares

Definición 7.3.2.1. Sea $G = (V, E)$ un grafo valorado (es decir, un grafo en el que cada arista $e \in E$ tiene asociado un peso $p \in \mathbb{R}$), y sea $M = (a_{ij})$ la matriz asociada al grafo. Se define la matriz de pesos asociada al grafo como una matriz P cuya entrada

$$p_{ij} = \begin{cases} p & a_{ij} \in \{-1, 1\} \text{ en la matriz de adyacencia/incidencia} \\ \infty & a_{ij} = 0 \end{cases}$$

Ejemplo 7.3.2.2. Consideremos el siguiente grafo:



La matriz de pesos asociada al grafo es:

$$P = \begin{pmatrix} \infty & 2 & \infty & \infty & 1 & 1 \\ 2 & \infty & 3 & \infty & 2 & \infty \\ \infty & 3 & \infty & \infty & 3 & \infty \\ \infty & \infty & \infty & \infty & 4 & 4 \\ 1 & 2 & 3 & 4 & \infty & 1 \\ 1 & \infty & \infty & 4 & 1 & \infty \end{pmatrix}$$

Definición 7.3.2.3. Sea $G = (V, E)$ un grafo no dirigido valorado, y sea T un árbol generador. El peso de T se define como la suma de los pesos de todas sus aristas.

Definición 7.3.2.4. Sea $G = (V, E)$ un grafo no dirigido valorado. Se define el árbol generador mínimo de G como el árbol generador cuyo peso sea menor o igual que el peso del resto de árboles generadores de G.

7.3.3. Algoritmo de Kruskal

Proposición 7.3.3.1 (Algoritmo de Kruskal)**.** El algoritmo de Kruskal nos permite obtener un árbol generador mínimo para un grafo no dirigido conexo, valorado y simple. Sea $G = (V, E)$ un grafo con estas características y con $|V| = n$.

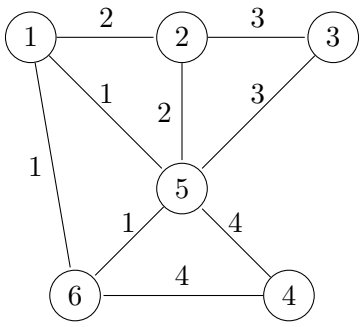
1. Ordenar E de manera no decreciente en función de los pesos de las aristas y definir $A = \emptyset$.

2. Si la primera arista de E forma un ciclo con los vértices definidos por los extremos de las aristas de A, eliminar de E. Si no, eliminar dicha arista de E y añadirla a A.

3. Repetir el paso 2 hasta que A tenga $n - 1$ elementos (lo cual garantiza que conforma un árbol de recubrimiento por un resultado visto anteriormente).

El subgrafo $T = (V, A)$ es el árbol de recubrimiento mínimo para G.

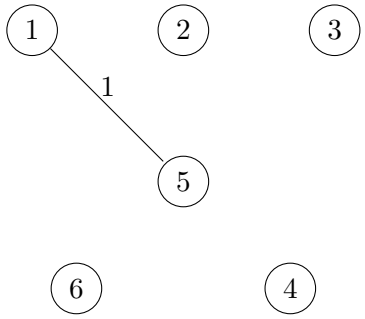
Ejemplo 7.3.3.2. Consideremos el siguiente grafo no dirigido conexo, valorado y simple del cuál queremos encontrar un árbol generador mínimo utilizando el algoritmo de Kruskal:



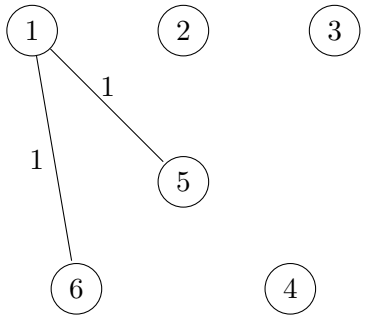
(i) El conjunto E lo ordenamos de la siguiente forma:

$$E = \{e_{1,5},\ e_{1,6},\ e_{5,6},\ e_{1,2},\ e_{2,5},\ e_{2,3},\ e_{3,5},\ e_{4,5},\ e_{5,6}\}$$

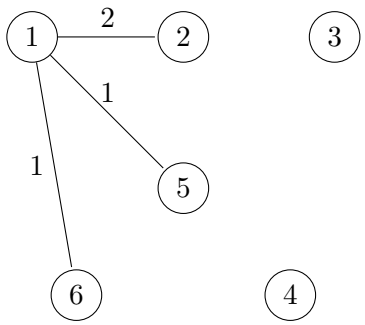
(ii) Escogemos la primera arista de E pues no forma ciclos al no haber elegido previamente ninguna otra arista.



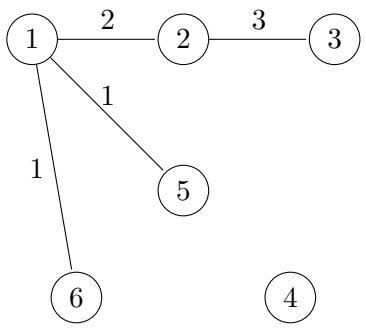
(iii) Elegimos la segunda arista por no formar ciclos.



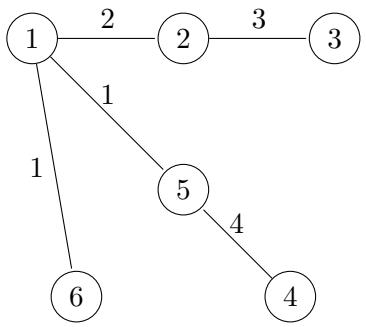
(iv) La tercera arista no la elegimos, pues forma un ciclo entre los vértices 1, 5 y 6. Por tanto, elegimos la cuarta arista.



(v) No elegimos la quinta arista, pues forma ciclo entre los vértices 1, 2 y 5. Elegimos la sexta arista.



(vi) No elegimos la séptima arista, pues forma ciclo entre los vértices 2, 3 y 5. Elegimos la octava arista.



(vii) Al tener 5 aristas y haber 6 vértices, el algoritmo termina.

Notemos que el árbol generador mínimo encontrado tiene peso 11.

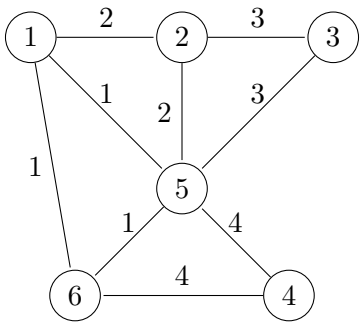
7.3.4. Algoritmo de Prim

Proposición 7.3.4.1 (Algoritmo de Prim)**.** El algoritmo de Prim nos permite obtener un árbol generador mínimo para un grafo no dirigido conexo, valorado y simple. Sea $G = (V, E)$ un grafo con estas características y con $|V| = n$.

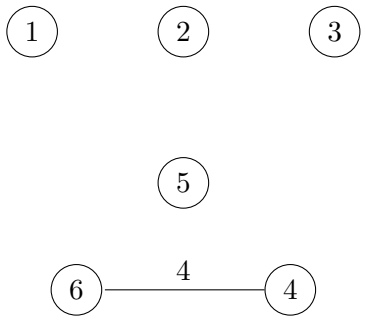
1. Tomar un vértice $v \in V$ cualquiera y definamos $A = \emptyset$.
2. Encontrar el vértice $u \in V$ tal que $\{v, u\}$ tenga el mínimo peso, añadir dicha arista a A, siempre y cuando no forme un ciclo con los vértices definidos por los extremos de las aristas de A, y hacer $v = u$.
3. Repetir el paso 2 hasta que A tenga $n - 1$ elementos.

El subgrafo $T = (V, A)$ es el árbol de recubrimiento mínimo para G.

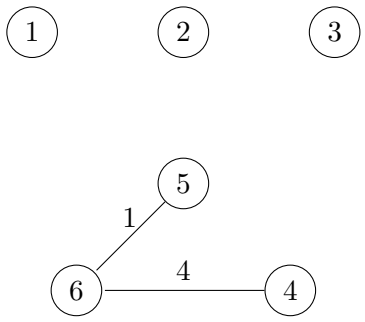
Ejemplo 7.3.4.2. Consideremos el siguiente grafo no dirigido, valorado, conexo y simple del cuál queremos encontrar un árbol generador mínimo utilizando el algoritmo de Prim:



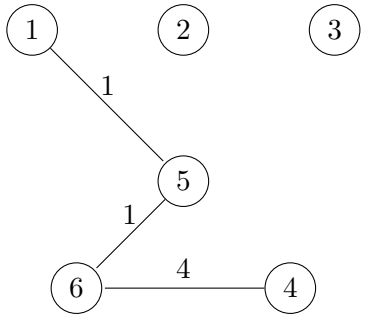
(i) Para demostrar que el algoritmo no depende de la elección del vértice inicial, empecemos tomando un vértice distinto del 1, digamos el 4. Seleccionemos la arista con menor peso que tiene a 4 por extremo. Hay dos aristas de igual peso: $e_{4,5}$ y $e_{4,6}$. Tomemos, digamos, $e_{4,6}$.



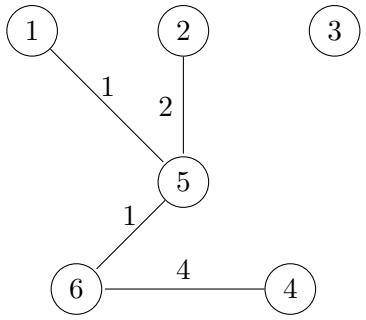
(ii) Las posibles aristas que podemos seleccionar ahora son $e_{1,6}$, $e_{4,5}$, $e_{5,6}$. La primera y la última tienen igual peso, así que elegimos una de las dos.



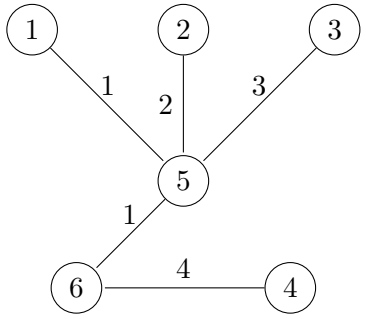
(iii) Las aristas que podemos elegir ahora son $e_{1,5}$, $e_{1,6}$, $e_{2,5}$, $e_{3,5}$, $e_{4,5}$. De estas, eliminamos las que forman ciclos con las que ya hemos elegido y nos quedan $e_{1,5}$, $e_{1,6}$, $e_{2,5}$, $e_{3,5}$. Las dos primeras tienen peso 1, elegimos una de ellas.



(iv) Las aristas que podemos seleccionar ahora son $e_{1,2}$, $e_{1,6}$, $e_{2,5}$, $e_{3,5}$. Si eliminamos las aristas que forman ciclos con las seleccionadas nos quedan $e_{1,2}$, $e_{2,5}$, $e_{3,5}$. Las dos primeras tienen menor peso, 2. Elegimos una.



(v) Las aristas que podemos seleccionar ahora son $e_{1,2}$, $e_{2,3}$, $e_{3,5}$. Si eliminamos las aristas que forman ciclos con las seleccionadas nos quedan $e_{2,3}$, $e_{3,5}$. Como tienen el mismo peso, elegimos una de las dos.



(vi) Al tener 5 aristas y haber 6 vértices, el algoritmo termina.

Notemos que el árbol generador mínimo encontrado tiene peso 11 y, aunque sea un árbol distinto del encontrado con el algoritmo de Kruskal, el peso es el mismo.

7.4. Algoritmo de búsqueda del camino más corto

7.4.1. Introducción

Dedicaremos la última sección al, probablemente, algoritmo más importante del curso, el algoritmo de Dijkstra, para encontrar el camino más corto entre dos vértices. No solo encuentra este camino, sino que, además, calcula la distancia mínima entre ambos y encuentra el camino más corto entre un vértice y todos los demás.

7.4.2. Algoritmo de Dijkstra

Definición 7.4.2.1. Sea $G = (V, E)$ un grafo valorado. Se define el camino mínimo entre dos vértices u y v como el camino cuya suma de pesos es mínima.

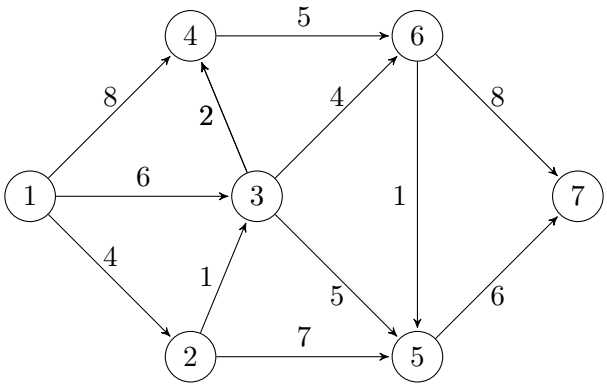
Observación 7.4.2.2. Sea $G = (V, E)$ un grafo dirigido y valorado, con $|V| = n$, tal que $p_{ij} \geq 0$. El algoritmo va a consistir en dos partes: la primera sirve para encontrar la distancia más corta entre un vértice y el resto y la segunda sirve para encontrar el camino que recorre esa distancia. La idea va a ser empezar en dicho vértice y recorrer la arista de menor peso. A continuación, para el resto de vértices, llevaremos la cuenta de las distancias mínimas estimadas desde los vértices ya visitados hasta el vértice al cual estamos calculando dicha distancia mínima y comprobando si desde el vértice actual la distancia mínima estimada es menor que las calculadas anteriormente o no.

- $L(i)$ denotará la distancia mínima recorrida desde el vértice inicial hasta el vértice v_i.
- $L'(i)$ será una cota superior de la distancia mínima entre el vértice inicial y el vértice v_i.
- p_{ij} representa el peso (o distancia) de la arista e_{ij}.

Proposición 7.4.2.3 (Algoritmo de Dijkstra para el camino más corto)**.** Sea $G = (V, E)$ un grafo dirigido y valorado con $V = \{v_1, \ldots, v_n\}$. Queremos calcular la distancia mínima de v_1 al resto de vértices. Para ello:

1. Definir $v = v_1$, $L(1) = 0$, retirar v de V y calcular $L'(i) = p_{1i}$ para todo $v_i \in V$.
2. Recorrer la arista (v, v_k) tal que $L'(k)$ sea mínimo. Definir $v = v_k$, $L(k) = L'(k)$ y retirar v de V.
3. Calcular $L'(i) = \text{mín}\{L'(i), L'(k) + p_{ki}\}$ y volver al paso 2.
4. Si $V = \emptyset$, el algoritmo termina. La distancia más corta entre v_1 y v_i es $L(i)$.

Ejemplo 7.4.2.4. Dado el siguiente grafo, queremos calcular la distancia mínima desde el vértice 1 hasta el resto de vértices utilizando el algoritmo de Dijkstra:



(i) Hacemos $v = 1$ e imponemos $L(1) = 0$. Calculamos las distancias mínimas estimadas desde 1 hasta el resto de vértices. Tenemos: $L'(2) = 4$, $L'(3) = 6$, $L'(4) = 8$, $L'(5) = L'(6) = L'(7) = \infty$. Como el mínimo de estos valores se alcanza para el vértice 2, nos quedamos con este vértice.

(ii) Hacemos $v = 2$ e imponemos $L(2) = L'(2) = 4$. Calculamos las distancias mínimas estimadas. Tenemos:

- $L'(3) = \text{mín}\{L'(3), L(2) + p_{2,3}\} = \text{mín}\{6, 4 + 1\} = 5$.

- $L'(4) = \text{mín}\{L'(4),\, L(2) + p_{2,4}\} = \text{mín}\{8,\, 4 + \infty\} = 8.$
- $L'(5) = \text{mín}\{L'(5),\, L(2) + p_{2,5}\} = \text{mín}\{\infty,\, 4 + 7\} = 11.$
- $L'(6) = \text{mín}\{L'(6),\, L(2) + p_{2,6}\} = \text{mín}\{\infty,\, 4 + \infty\} = \infty.$
- $L'(7) = \text{mín}\{L'(7),\, L(2) + p_{2,7}\} = \text{mín}\{\infty,\, 4 + \infty\} = \infty.$

Como el mínimo de estos valores se alcanza para el vértice 3, nos quedamos con este vértice.

(iii) Hacemos $v = 3$ e imponemos $L(3) = L'(3) = 5$. Calculamos las distancias mínimas estimadas. Tenemos:

- $L'(4) = \text{mín}\{L'(4),\, L(3) + p_{3,4}\} = \text{mín}\{8,\, 5 + 2\} = 7.$
- $L'(5) = \text{mín}\{L'(5),\, L(3) + p_{3,5}\} = \text{mín}\{11,\, 5 + 5\} = 10.$
- $L'(6) = \text{mín}\{L'(6),\, L(3) + p_{3,6}\} = \text{mín}\{\infty,\, 5 + 4\} = 9.$
- $L'(7) = \text{mín}\{L'(7),\, L(3) + p_{3,7}\} = \text{mín}\{\infty,\, 5 + \infty\} = \infty.$

Como el mínimo de estos valores se alcanza para el vértice 4, nos quedamos con este vértice. Hacemos $v = 4$ e imponemos $L(4) = L'(4) = 7$. Calculamos las distancias mínimas estimadas. Tenemos:

- $L'(5) = \text{mín}\{L'(5),\, L(4) + p_{4,5}\} = \text{mín}\{10,\, 7 + \infty\} = 10.$
- $L'(6) = \text{mín}\{L'(6),\, L(4) + p_{4,6}\} = \text{mín}\{9,\, 7 + 5\} = 9.$
- $L'(7) = \text{mín}\{L'(7),\, L(4) + p_{4,7}\} = \text{mín}\{\infty,\, 7 + \infty\} = \infty.$

Como el mínimo de estos valores se alcanza para el vértice 6, nos quedamos con este vértice. Hacemos $v = 6$ e imponemos $L(6) = L'(6) = 9$. Calculamos las distancias mínimas estimadas. Tenemos:

- $L'(5) = \text{mín}\{L'(5),\, L(6) + p_{5,6}\} = \text{mín}\{10,\, 9 + 1\} = 10.$
- $L'(7) = \text{mín}\{L'(7),\, L(6) + p_{6,7}\} = \text{mín}\{\infty,\, 9 + 8\} = 17.$

Como el mínimo de estos valores se alcanza para el vértice 5, nos quedamos con este vértice. Hacemos $v = 5$ e imponemos $L(5) = L'(5) = 10$. Calculamos las distancias mínimas estimadas. Tenemos:

$$L'(7) = \text{mín}\{L'(7),\, L(5) + p_{5,7}\} = \text{mín}\{17,\, 10 + 6\} = 16$$

Como es el último vértice, tenemos que $L(7) = L'(7) = 16$.

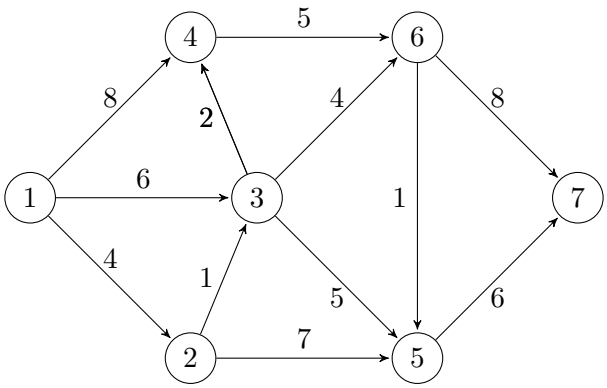
Las distancia mínima desde el vértice 1 hasta el vértice i es $L(i)$, $\forall i \in V$.

Proposición 7.4.2.5 (Algoritmo de Dijkstra para la distancia más corta)**.** Sea $G = (V,\, E)$ un grafo dirigido y valorado con $V = \{v_1,\, \ldots,\, v_n\}$. Queremos obtener el camino más corto entre v_1 y el resto de vértices habiendo obtenido las distancias más cortas. Para que una arista $(v_i,\, v_j)$ esté en el camino:

(i) $L(i) < L(j)$.

(ii) $L(i) + p_{ij} = L(j)$.

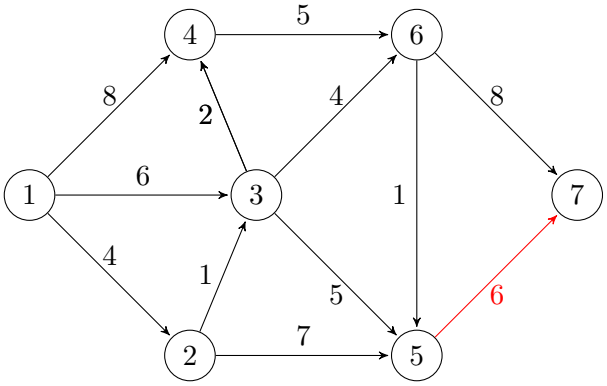
Ejemplo 7.4.2.6. Supongamos que, en el grafo del ejemplo anterior queremos encontrar el camino mínimo entre el vértice 1 y el vértice 7.



(i) Comenzando desde el vértice 7, este vértice solo es vértice de llegada para las aristas $e_{5,7}$ y $e_{6,7}$. Como $L(5) < L(7)$ y $L(6) < L(7)$, comprobamos la segunda condición del algoritmo.

- $L(5) + p_{5,7} = 10 + 6 = 16 = L(7)$.
- $L(6) + p_{6,7} = 9 + 8 = 17 \neq L(7)$.

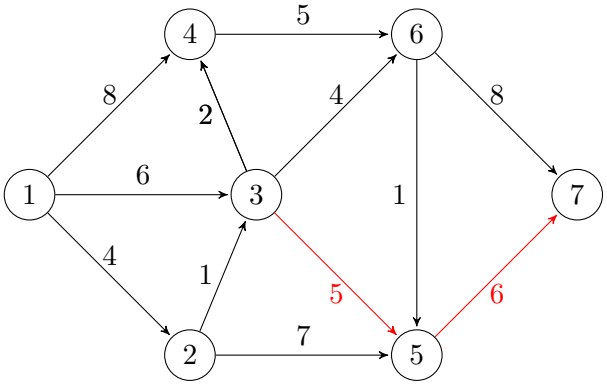
Por tanto, marcamos la arista $e_{5,7}$ como parte del camino mínimo.



(ii) El vértice 5 es vértice de llegada para las aristas $e_{2,5}$, $e_{3,5}$ y $e_{6,5}$. Como $L(2) < L(5)$, $L(3) < L(5)$, $L(6) < L(5)$, comprobamos la segunda condición del algoritmo.

- $L(2) + p_{2,5} = 4 + 7 = 11 \neq L(5)$.
- $L(3) + p_{3,5} = 5 + 5 = 10 = L(5)$.
- $L(6) + p_{6,5} = 9 + 1 = 10 = L(5)$.

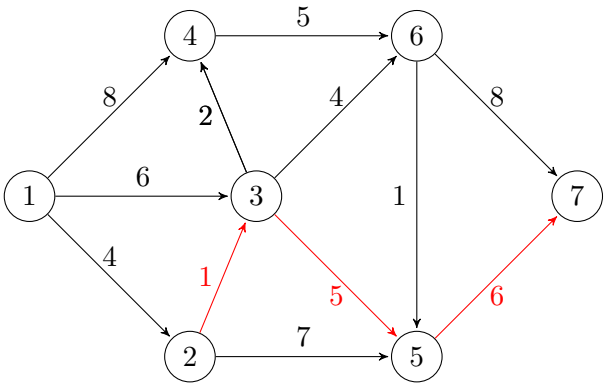
Como las aristas $e_{3,5}$ y $e_{6,5}$ hacen que el camino hasta 5 tenga igual distancia, elegimos indistintamente una de las dos. Tomemos, por ejemplo, $e_{3,5}$ como parte del camino mínimo.



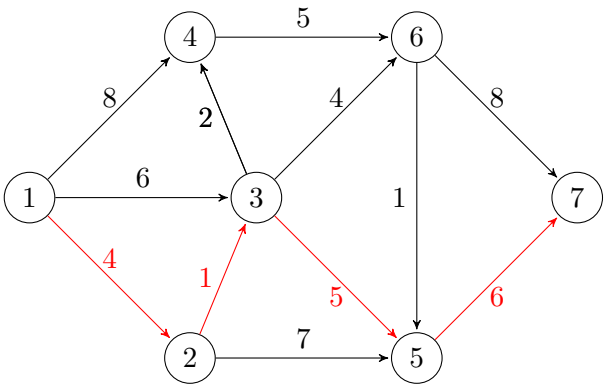
(iii) El vértice 3 es vértice de llegada para las aristas $e_{1,3}$ y $e_{2,3}$. Como $L(1) < L(3)$, $L(2) < L(3)$, comprobamos la segunda condición del algoritmo.

- $L(1) + p_{1,3} = 0 + 6 = 6 \neq L(3)$.
- $L(2) + p_{2,3} = 4 + 1 = 5 = L(3)$.

Por tanto, marcamos la arista $e_{2,3}$ como parte del camino mínimo.



(iv) El vértice 2 es vértice de llegada para la arista $e_{1,2}$, por tanto, está garantizado que esta arista forma parte del camino mínimo.



De esta forma, hemos encontrado el camino de longitud mínima desde el vértice 1 hasta el vértice 7.

7.5. Cuestionario

Ejercicio 58. Un árbol de altura 3 puede tener una hoja en el nivel 2.

(a) Verdadero

(b) Falso

Ejercicio 59. ¿Cuántos vértices tiene un árbol con 16 aristas?

(a) 15

(b) 16

(c) 17

(d) No se puede saber

Ejercicio 60. Un grafo simple con 20 vértices y 14 aristas no puede tener un árbol recubridor.

(a) Verdadero

(b) Falso

Ejercicio 61. Un árbol puede tener 2 o más componentes conexas.

(a) Verdadero

(b) Falso

Ejercicio 62. Los algoritmos *DFS* y *BFS* solo se diferencian en la forma de explorar los vértices del grafo.

(a) Verdadero

(b) Falso

Ejercicio 63. Si dos vértices v_i y v_j no son adyacentes, pero hay una arista $e_{i,k}$ de peso 2 y una arista $e_{k,j}$ de peso 3, el peso $p_{i,j}$ es:

(a) 2

(b) 3

(c) 5

(d) ∞

Ejercicio 64. En el algoritmo de Kruskal debemos ordenar los vértices en función de sus grados.

(a) Verdadero

(b) Falso

Ejercicio 65. Con el algoritmo de Prim siempre se va a obtener el mismo árbol generador minimal.

(a) Verdadero

(b) Falso

Ejercicio 66. Un camino entre dos vértices es más corto que otro si tiene un menor número de aristas.

(a) Verdadero

(b) Falso

Ejercicio 67. En el algoritmo de Dijkstra, para seleccionar un vértice, este debe tener la menor distancia estimada de todos los vértices por explorar.

(a) Verdadero

(b) Falso