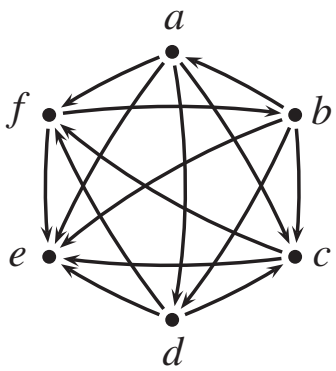
Notas de la UEA Matemáticas Discretas II

Dra. Mika Olsen



$$P(x)\cdot U(x)=\sum_{j=0,i+j=0}^{n+0} a_i \mathbf{u}(x^{i+j})=\sum_{i=0}^{n} a_i x^i = P(x).$$

Casa abierta al tiempo
UNIVERSIDAD AUTÓNOMA METROPOLITANA
Unidad Cuajimalpa

Obra ganadora del Tercer Concurso para la publicación de libros de texto y materiales de apoyo a la impartición de los programas de estudio de las licenciaturas que ofrece la Unidad Cuajimalpa

Notas de la UEA

Matemáticas Discretas II

Casa abierta al tiempo
UNIVERSIDAD AUTÓNOMA METROPOLITANA
Unidad Cuajimalpa

2) Notas de la UEA Matemáticas discretas II
Clasificación Dewey: 004.0151 O47
Clasificación LC: QA76.9.M35 O47
Olsen, Mika
Notas de la UEA : Matemáticas discretas II / Mika Olsen . – Ciudad de México : UAM, Unidad Cuajimalpa, 2017.
117 p. : il. col., diagrs. tablas ; 17x24 cm.

ISBN: 978-607-28-1097-6

1. Ciencias de la computación – Matemáticas – Libros de texto. 2. Anillos (Álgebra) – Libros de texto. 3. Teoría de grafos – Libros de texto. 4. Universidad Autónoma Metropolitana – Unidad Cuajimalpa – Planes de estudio.

Esta obra fue dictaminada positivamente por pares académicos mediante el sistema doble ciego y evaluada para su publicación por el Consejo Editorial de la UAM Unidad Cuajimalpa.

Avenida Vasco de Quiroga 4871
Col. Santa Fe Cuajimalpa, delegación Cuajimalpa de Morelos
C.P. 05348, Ciudad de México (Tel: 5814 6500)
www.cua.uam.mx

ISBN: 978-607-28-1097-6

Primera edición: 2017

Corrección de estilo: Omar Campa
Diseño editorial y portada: Literatura y Alternativas en Servicios Editoriales S.C.
Avenida Universidad 1815-c, Depto. 205, Colonia Oxtopulco,
C. P. 04318, Delegación Coyoacán, Ciudad de México.
RFC: LAS1008162Z1

Impreso y hecho en México
Printed and made in Mexico

Dra. Mika Olsen

Notas de la UEA

Matemáticas Discretas II

Casa abierta al tiempo
UNIVERSIDAD AUTÓNOMA METROPOLITANA
Unidad Cuajimalpa

UNIVERSIDAD AUTÓNOMA METROPOLITANA

Dr. Eduardo Peñalosa Castro
Rector General

Dr. José Antonio De los Reyes Heredia
Secretario General

Dr. Rodolfo Suárez Molnar
Rector de la Unidad Cuajimalpa

Dr. Álvaro Peláez Cedrés
Secretario de la Unidad Cuajimalpa

Mtro. Octavio Mercado González
Director de la División de Ciencias de la Comunicación y Diseño

Dr. Raúl Roydeen García Aguilar
Secretario Académico de la División de Ciencias de la Comunicación y Diseño

Dr. A. Mauricio Sales Cruz
Director de la División de Ciencias Naturales e Ingeniería

Dr. José Javier Valencia López
Secretario Académico de la División de Ciencias Naturales e Ingeniería

Dr. Roger Mario Barbosa Cruz
Director de la División de Ciencias Sociales y Humanidades

Dr. Jorge Lionel Galindo Monteagudo
Secretario Académico de la División de Ciencias Sociales y Humanidades

Índice

Prefacio

Las notas de curso que aquí se presentan corresponden al programa actual de la UEA Matemáticas Discretas II de la UAM Cuajimalpa. El objetivo general de la UEA es que el alumno durante el tercer trimestre de la Licenciatura madure su pensamiento matemático, aumente su capacidad de trabajar con abstracciones y claro esta que maneje técnicas de razonamiento discreto en estructuras básicas de álgebra y en teoría de gráficas. Estas notas pretenden apoyar al alumno en su estudio, reuniendo los temas de la UEA en un sólo texto, está basado en las clases que ha impartido la autora y se ajusta al modelo educativo de la UAM-Cuajimalpa. En el desarrollo del material se asume que el alumno ya tuvo un acercamiento con demostraciones sencillas y que tenga un conocimientos básicas en Lógica, Conjuntos, Números Naturales, Números Enteros, Números Complejos, Relaciones, Funciones y Conteo temas incluídas en el programa de Matemáticas Discretas I. El material incluye mas de 80 ejemplos para motivar las definiciones y 52 figuras y 18 cuadros que apoyan el desarrollo teórico de los temas, además los ejemplos y ejercicios resueltos así como ejercicios son una herramienta para que el alumno evalúe el avance de su aprendizaje. Cada capítulo cuenta con una sección de proyectos, que pueda desarrollar el alumno, con el objetivo de reafirmar los conocimientos adquiridos y relacionar los conocimientos con problemas o aplicaciones reales. Algunos de los proyectos incluye la implementación de algoritmos para relacionar los conocimientos adquiridos con la implementación de algoritmos.

Prólogo para profesor

Las notas de curso de Matemáticas Discretas II, se puede cubrir a lo largo de un trimestre, esta dividido en dos partes:

1. Estructuras Algebraícas.

2. Teoría de las Gráficas.

La primera parte tiene dos capítulos: Introducción al Álgebra Moderna Aplicada y Anillos de Polinomios. La segunda parte también tiene dos capítulos: Introducción a la Teoría de las Gráficas e Introducción a los Árboles. Las dos partes son independientes y se puede intercambiar el orden de ellos sin que afecte la cronología lógica de la teoría.

En la primera parte de las notas se introduce la estructura algebraíca de anillo. Se presentan diversos anillos en diversos áreas de las matemáticas haciendo énfasis en los conjuntos

de elementos o números que el alumno conoce de antemano que forman un anillo con operaciones conocidos, como los conjuntos de números $\mathbb{Z}$, $\mathbb{Q}$, las matrices cuadradas con entradas en un anillo y el conjunto potencia $\mathcal{P}_U$ de un conjunto no vacío U. Después, el estudio de los anillos, se centra en los anillos $\mathbb{Z}_n$ y la relación de congruencia. El primer capítulo termina con álgebra booleana que resume propiedades de la lógica y de los conjuntos (que se estudian en Matemáticas Discretas I) y se estudian alguno de sus aplicaciones, en particular su aplicación a los circuitos combinatorios. En el segundo capítulo se estudia el anillo de polinomios. Cuando los coeficientes de los polinomios pertenecen a un campo, se trazan analogías entre el anillo de los números entros $\mathbb{Z}$ y el anillo de polinomios, terminando el capítulo con el anillo de polinomios con coeficientes reales, el cual los alumnos conocen de sus estudio media-superior. En la primera parte del material se revisan dos algorítmos: el algoritmo de la división de polinomios incluyendo división sintética y el algoritmo de Euclides para encontrar el máximo común divisor de dos polinomios.

La segunda parte del temario de Matemáticas Discretas II está dedicada a la Teoría de las Gráficas. El objetivo de la introducción a la Teoría de las Gráficas es familiarizar al alumno con la teoría básica así como aplicaciones y problemas que se pueden modelar con una gráfica o digráfica. Para lograr este objetivo iniciamos el capítulo 3 con la revisión de cuatro problemas que históricamente fueron importantes para la Teoría de las Gráficas: circuitos eulerianos, ciclos hamiltonianos, gráficas planas y el Teorema de los cuatro colores. El primer problema esta completamente determinado, el segundo y el tercero son problemas $\mathcal{NP}$-Completos y el último problema fue el primer teorema matemático en el que se utilizó una computadora para probar su veracidad. Después se hace una revisión de algunos conceptos de la Teoría de las Gráficas así como sus aplicaciones. En el cuarto capítulo se estudia la clase de los árboles, una clase de gráficas con muchas aplicaciones en diversas áreas de las ciencias exactas y en ciencias sociales. En matemáticas tiene aplicaciones en el área de Conteo, Probabilidad, Teoría de Decisiones, Relaciones de Orden, Estructura de Datos y Algoritmos. En la segunda parte del material se revisan tres algorítmos en gráficas: el algoritmo de Prim y el algoritmo de Kruskal para encontrar un árbol de peso mínimo y el algoritmo de Dijkstra para encontrar la distancia mínima entre dos vértices en una gráfica o digráfica.

1 Introducción al Álgebra Moderna Aplicada

En este capítulo se introducen las estructuras algebraicas de grupo, anillo y álgebra booleana. El estudio de los anillos se centra en los enteros $\mathbb{Z}_n$, aunque también se presentan otros ejemplos tales como matrices y conjuntos. En el estudio del álgebra booleana se hace énfasis en las aplicaciones tanto a la lógica y la teoría de conjunto como a los circuitos combinatorios.

1.1 Estructuras algebraicas

Un grupo consta de un conjunto A de objetos (o números) y una operación $\star$. La operación $\star$ puede ser por ejemplo una suma, un producto, una eje de simetría, la intersección de conjuntos. Decimos que el conjunto A está **cerrado bajo la operación** $\star$ si para todo par de elementos $a, b \in A$ se tiene que $a \star b \in A$.

Definición 1.1.1. *El conjunto A con la operación $\star$ forman un* **grupo** $(A, \star)$ *si el conjunto A está cerrado bajo la operación $\star$, y para todo $a, b, c \in A$ se tiene que*

1. $a \star (b \star c) = (a \star b) \star c$ *(propiedad asociativa).*
2. *Existe $z \in A$ tal que $a \star z = z \star a = a$ (propiedad neutro).*
3. *Para todo $a \in A$ existe $(a') \in A$ tal que $a \star (a') = (a') \star a = z$ (propiedad inverso).*

Definición 1.1.2. *El grupo $(A, \star)$ es un* **grupo abeliano** *si para todo $a, b \in A$ se tiene que*

4. $a \star b = b \star a$ *(propiedad conmutativa)*

Ejemplo 1.1.1. *Considera las operaciones usuales.*

1. *El conjunto de los números enteros $\mathbb{Z}$ forma el grupo abeliano $(\mathbb{Z}, +)$.*
2. *El conjunto de los números racionales $\mathbb{Q}$ forma el grupo abeliano $(\mathbb{Q}, *)$.*
3. *El conjunto de los números enteros $\mathbb{Z}$ no forma un grupo con el producto usual ya que los inversos multiplicativos no son números enteros, por ejemplo, el inverso multiplicativo de 2 es $1/2$, pero $1/2 \notin \mathbb{Z}$.*

1.1.1 Grupo de simetrías de un triángulo equilátero

Revisamos el ejemplo donde el conjunto no es un conjunto de números sino un triángulo equilátero y la operación no es ni la suma ni el producto sino el conjunto de todas las simetrías del triángulo equilátero. Al grupo de simetrías de un polígono equilátero de n lados, también se le llama el **grupo diédrico** D_n.

Un triángulo equilátero tiene dos tipos de simetrías: rotaciones con respecto al centro del triángulo y reflecciones con respecto a las medianas, es decir, tiene seis simetrías tres rotaciones y tres reflexiones. Considera el triángulo equilátero ABC en la figura 1.1. Si

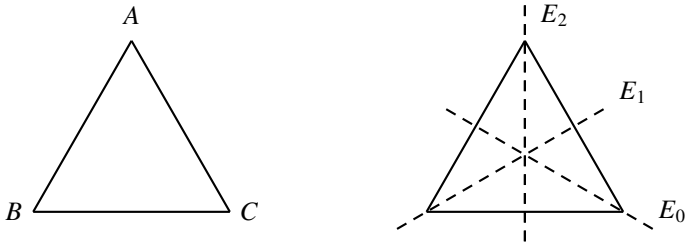


Figura 1.1: El triángulo equilátero ABC y las simetrías de un triángulo equilátero.

rotamos el triángulo ABC con 0°, 120° y 240° en contra de las manecillas del reloj, el triángulo ABC queda idéntico salvo la etiquetación. Denota por R_0, R_1 y R_2 las rotaciones con 0°, 120° y 240° respectivamente. Si reflejamos con respecto a una mediana el triángulo ABC queda idéntico salvo la etiquetación. Denota por E_0, E_1 y E_2 las medianas (ejes de simetría) según la figura 1.1. Con esta notación, el conjunto de las simetrías de un triángulo equilátero ABC es

$$\{R_0, R_1, R_2, E_0, E_1, E_2\}.$$

Primero comprobamos que al aplicar una simetría seguida por otra simetría obtenemos de nuevo una simetría del triángulo equilátero. El orden en que se aplica las operaciones se lee de derecha hacia izquierda (como en la composición de funciones).

1. Aplicamos la reflexión con respecto al eje E_1 seguida por la reflexión con respecto al eje E_0 (ver figura 1.2).

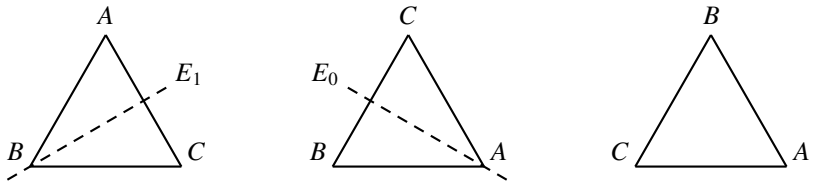


Figura 1.2: El triángulo ABC, aplicando la reflección E_1 seguida por la reflección E_0.

El resultado es la rotación del 120°, por lo que $E_0E_1 = R_1$.

2. Aplicamos la rotación de 120° seguida por la reflexión con respecto al eje E_0 (ver figura 1.3). El resultado es la reflexión con respecto al eje E_2, por lo que $E_0R_1 = E_2$.

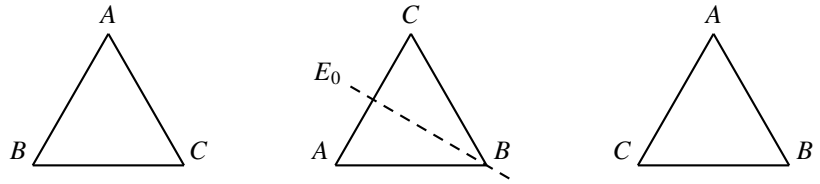


Figura 1.3: El triángulo ABC, aplicando la rotación R_1 seguida por la reflección E_0.

3. Aplicamos la reflexión con respecto al eje E_0 seguida por la reflexión con respecto al eje E_1 (ver figura 1.4). El resultado es la rotación del 240°, por lo que $E_1E_0 = R_2$.

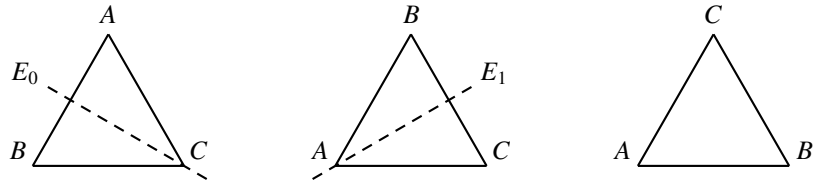


Figura 1.4: El triángulo ABC, aplicando la reflección E_0 seguida por la reflección E_1.

Observa que en los casos 1. y 3. aplicamos las mismos operaciones, pero con orden invertido y obtuvimos resultados distintos, por lo que el orden en que aplicamos las simetrías es importante y la composición de las simetrías no es conmutativa.

En el cuadro 1.1.1 representamos la simetrás resultantes al aplicar la simetría del renglón seguida por la simetría de la columna. En el cuadro 1.1.1 podemos observar que R_0 es un

Cuadro 1.1: La tabla de simetrías del triángulo equilátero.

$2 \setminus 1$	R_0	R_1	R_2	E_0	E_1	E_2
R_0	R_0	R_1	R_2	E_0	E_1	E_2
R_1	R_1	R_2	R_0	E_1	E_2	E_0
R_2	R_2	R_0	R_1	E_2	E_0	E_1
E_0	E_0	E_2	E_1	R_0	R_1	R_2
E_1	E_1	E_0	E_2	R_2	R_0	R_1
E_2	E_2	E_1	E_0	R_1	R_2	R_0

elemento neutro, cada ejes E_i es su propio inverso, R_1 es inverso de R_2 y R_2 es inverso de R_1. Para poder afirmar que D_3 en efecto es un grupo sólo falta comprobar la propiedad asociativa. Esta propiedad se deja como (ejercicio 1.1).

1.1.2 Anillos

Un anillo consta de un conjunto de objetos (o números) y dos operaciones que usualmente se denominan suma y producto aunque no lo sean. El conjunto debe estar cerrado bajo

ambas operaciones y las operaciones deben satisfacer una serie de propiedades llamadas Axiomas de anillo. Con la primera operación (denominado suma) el conjunto debe formar un grupo abeliano, mientras que para la segunda operación (denominado producto) sólo se pide que sea una operación asociativa y que cumpla una propiedad distributiva con respecto a la primera operación.

Definición 1.1.3. *Dado un conjunto A y dos operaciones, suma $+$ y producto $\cdot$, definimos las siguientes* **Axiomas de anillo**. *Para $a, b, c \in A$.*

A1 $a + b = b + a$ *(propiedad conmutativa).*

A2 $a + (b + c) = (a + b) + c$ *(propiedad asociativa).*

A3 *Existe un* **neutro aditivo z** *en A tal que para todo $a \in A$ se tiene que $a + \mathbf{z} = \mathbf{z} + a = a$ (propiedad neutro).*

A4 *Todo elemento $a \in A$ tiene* **inverso aditivo**, *denotado $(-a)$ tal que $a + (-a) = \mathbf{z}$ (propiedad inverso).*

M1 $a \cdot b = b \cdot a$ *(propiedad conmutativa).*

M2 $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ *(propiedad asociativa).*

M3 *Existe un* **neutro multiplicativo** *(unidad)* **u** *en A tal que para todo $a \in A$ se tiene que $u \cdot \mathbf{a} = a$ (propiedad inverso).*

M4 *Todo elemento $a \in A \setminus \{z\}$ tiene un* **inverso multiplicativo**, *denotado (a^{-1}), tal que $a \cdot (a^{-1}) = (a^{-1}) \cdot a = \boldsymbol{u}$ (propiedad inverso).*

D $a \cdot (b + c) = a \cdot b + a \cdot c$ *(propiedad distribuitiva).*

Definición 1.1.4. *Dado un conjunto A y dos operaciones, suma $+$ y producto $\cdot$, tales que A está cerrado bajo estas dos operaciones. Decimos que $(A; +, \cdot)$ es un* **anillo** *si los elementos de A satisfacen los axiomas de anillo $A1, A2, A3, A4, M2, D$. Si un anillo $(A; +, \cdot)$ satisface el axioma $M1$ decimos que es un anillo conmutativo y si un anillo $(A; +, \cdot)$ satisface el axioma $M3$ decimos que es un* **anillo con unidad**.

Ejemplo 1.1.2. *Los conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ forman anillos conmutativos con unidad con las operaciones usuales.*

Ejemplo 1.1.3. *Para cada entero $n \geq 2$ el conjunto $n\mathbb{Z} = \{\ldots, -2n, -n, 0, n, 2n, 3n, \ldots\}$ forma un anillo conmutativo sin unidad con las operaciones usuales. Por ejemplo.*

1. $2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$.
2. $5\mathbb{Z} = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$.

Si en un anillo $(A; \oplus, \otimes)$ con neutro aditivo **z** existen dos números $a, b \in A$ distintos del neutro aditivo **z** tales que $a \otimes b = \mathbf{z}$ decimos que a y b son divisores propios del neutro aditivo **z** (o divisores propios del cero).

Definición 1.1.5. *Un anillo conmutativo* $(A; \oplus, \otimes)$ *con unidad u y neutro aditivo* $\mathbf{z}$*, es un* **dominio entero** *si los elementos de A cumple el siguiente axioma:*

$$S\,i\; a \otimes b = \mathbf{z},\ entonces\ a = \mathbf{z}\ o\ b = \mathbf{z}.$$

Es decir, en un dominio entero el cero no tiene divisores propios.

Ejemplo 1.1.4. *Los siguientes conjuntos forman un dominio entero con la suma y el producto usual.*

1. *El conjunto de los números enteros.*
2. *El conjunto* $A = \left\{a + b\sqrt{2} : a, b \in \mathbb{Z}\right\}$.
3. *El conjunto* $A = \{7n : n \in \mathbb{Z}\}$.

En la próxima sección veremos ejemplos de anillos conmutativos con unidad que no son dominios enteros.

Definición 1.1.6. *Un anillo* $(A; +, \cdot)$ *conmutativo con unidad* $\mathbf{u}$ *que satisface* $M4$ *es un* **campo***, es decir, todo elemento* $a \in A$ *con a distinto del neutro aditivo tiene un inverso multiplicativo* (a^{-1}) *tal que* $a \cdot (a^{-1}) = \mathbf{u}$.

Ejemplo 1.1.5. *Los conjuntos* $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ *forman campos con las operaciones usuales, mientras que* $\mathbb{Z}$ *no es un campo porque los inversos multiplicativos de los números enteros no necesariamente son números enteros (por ejemplo, el inverso multiplicativo de* 2 *es* $1/2$*, pero* $1/2 \notin \mathbb{Z}$*).*

1.1.3 Ejemplos de anillos

Ejemplo 1.1.6. *Dado el conjunto de los números enteros* $\mathbb{Z}$*, definimos la suma y la multiplicación como sigue:*

$$\begin{aligned} x \oplus y &:= x + y - 1 \\ x \odot y &:= x + y - xy. \end{aligned}$$

La terna $(\mathbb{Z}; \oplus, \odot)$ *forma un anillo conmutativo con unidad.*

Por las propiedades de las operaciones en $\mathbb{Z}$*, el conjunto* $\mathbb{Z}$ *está cerrado bajo las operaciones* $\oplus$ *y* $\odot$*. Probamos que el conjunto* $\mathbb{Z}$ *con las operaciones* $\oplus$ *y* $\odot$ *satisface los axiomas de anillo. Sean* $a, b, c \in \mathbb{Z}$*.*

A1 $a \oplus b = a + b - 1 = b + a - 1 = b \oplus a$.

A2 $a \oplus (b \oplus c) = a \oplus (b + c - 1) = a + (b + c - 1) - 1 = (a + b - 1) + c - 1 = (a + b - 1) \oplus c = (a \oplus b) \oplus c$.

A3 Vamos a encontrar un número $z \in \mathbb{Z}$ *tal que para todo* $a \in A$ *se tiene que* $a = a \oplus z$*. Por la definición de la operación* $\oplus$ *tenemos que* $a = a \oplus z = a + z - 1$*. Usando propiedades de las operaciones usuales en* $\mathbb{Z}$ *tenemos que* $a = a + z - 1$ *si y sólo si* $z = 1$*. Por lo que* $z = 1$ *es neutro aditivo en* $(\mathbb{Z}; \oplus, \odot)$*.*

A4 *Dado un número $a \in A$ con $a \neq z$, vamos a encontrar un número $(-a) \in \mathbb{Z}$ tal que $z = a \oplus (-a)$. Por A3 sabemos que $z = 1$, por la definición de la operación $\oplus$, tenemos que $1 = a \oplus (-a) = a + (-a) - 1$. Usando propiedades de las operaciones usuales en $\mathbb{Z}$ tenemos que $1 = a + (-a) - 1$ si y sólo si $(-a) = -a + 2$. Por lo que el inverso aditivo de a en $(\mathbb{Z}; \oplus, \odot)$ es $-a + 2$.*

M1 $a \odot b = a + b - ab = b + a - ba = b \odot a$.

M2 $a \odot (b \odot c) = a \odot (b + c - bc) = a + b + c - bc - a(b + c - bc) = a + b + c - ab - ac - bc + abc$.

$(a \odot b) \odot c = (a + b - ab) \odot c = a + b - ab + c - (a + b - ab)c = a + b + c - ab - ac - bc + abc$.

Por lo que $a \odot (b \odot c) = (a \odot b) \odot c$.

M3 *Vamos a encontrar un número $u \in \mathbb{Z}$ tal que para todo $a \in A \setminus z$ se tiene que $a \odot u = u \odot a = a$. Por la definición de la operación $\odot$ tenemos que $a = a + u - au$. Usando propiedades por la elección de a que operaciones usuales en $\mathbb{Z}$ tenemos que $0 = u(1 - a)$ y como $z = 1$ se sigue $a \neq 1$ y $u = 0$. Por lo que $u = 0$ es neutro multiplicativo en $(\mathbb{Z}; \oplus, \odot)$.*

D $a \odot (b \oplus c) = a \odot (b + c - 1) = a + (b + c - 1) - a(b + c - 1) = 2a + b + c - ab + ac - 1$.

$(a \odot b) \oplus (a \odot c) = (a + b - ab) \oplus (a + c - ac) = (a + b - ab) + (a + c - ac) - 1 = 2a + b + c - ab + ac - 1$.

Por lo que $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$.

Con lo que concluimos que $(\mathbb{Z}; \oplus, \odot)$ es un anillo conmutativo con unidad.

Ejemplo 1.1.7. *Considera el conjunto de los números racionales $\mathbb{Q}$ con las operaciones definidas en el ejemplo 1.1.6. Prueba que $(\mathbb{Q}; \oplus, \odot)$ es un campo.*

Probar que $(\mathbb{Q}; \oplus, \odot)$ es un anillo conmutativo con unidad es análogo al ejemplo 1.1.6. Solamente falta probar que cualquier elemento en $\mathbb{Q}$ tiene inverso multiplicativo con las operaciones definidas.

M4 *Dado un número $a \in \mathbb{Q}$ con $a \neq z$, vamos a encontrar un número (a^{-1}), tal que $a \odot (a^{-1}) = u$. Como $u = 0$, por la definición de la operación $\odot$ tenemos que $0 = a \odot (a^{-1}) = a + (a^{-1}) - a(a^{-1})$. Usando propiedades de las operaciones usuales en $\mathbb{Z}$ tenemos que $0 = a + (a^{-1}) - a(a^{-1})$ si y sólo si $(a^{-1})a - (a^{-1}) = a$, si factorizamos (a^{-1}) obtenemos que $(a^{-1})(a - 1) = a$ y como $z = 1$, tenemos que $a \neq 1$ y podemos despejar (a^{-1}) obteniendo que $(a^{-1}) = \frac{a}{a-1}$. Por lo que el inverso multiplicativo de a en $(\mathbb{Q}; \oplus, \odot)$ con $a \in \mathbb{Q} \setminus \{1\}$ es $\dfrac{a}{a-1}$.*

Por el ejemplo 1.1.6 y como todo $a \in \mathbb{Q}$ con $a \neq z$ satisface M4, entonces $(\mathbb{Q}; \oplus, \odot)$ es un campo.

Ejemplo 1.1.8. *Dado un conjunto universal U no vacío y el conjunto potencia de U, denotado por $\mathcal{P}_U$, definimos la suma simétrica de dos subconjuntos de U como $A \triangle B = (A \setminus B) \cup (B \setminus A)$.*

A1 $A \triangle B = (A \setminus B) \cup (B \setminus A) = (B \setminus A) \cup (A \setminus B) = B \triangle A$.

A2 $A \triangle (B \triangle C) = (A \triangle B) \triangle C$. *Ejercicio 1.11 inciso (a).*

A3 *Vamos a encontrar un subconjunto* Z *de* U ($Z \in \mathcal{P}_U$) *tal que* $A \triangle Z = A$ *para todo* $A \in \mathcal{P}_U$.

Es decir, que $A = A \triangle Z = (A \setminus Z) \cup (Z \setminus A)$.

Como $A \setminus \emptyset = A$ *y* $\emptyset \setminus A = \emptyset$, *entonces* $(A \setminus \emptyset) \cup (\emptyset \setminus A) = A \cup \emptyset = A$ *y* $A = A \triangle \emptyset$.

Supongamos que $Z \neq \emptyset$ *y analicemos los siguientes dos casos para un elemento* $x \in Z$. *Si* $x \in A \cap Z$, *entonces* $x \notin A \triangle Z$ *y* $x \in A$. *Si* $x \in Z \setminus A$, *entonces* $x \notin A$ *y* $x \in A \triangle Z$. *En ambos casos tenemos que* $A \neq A \triangle Z$. *Por lo tanto* $Z = \emptyset$ *es neutro aditivo en* $\mathcal{P}_U$.

A4 *Dado un elemento* $A \in \mathcal{P}_U$ *con* $A \neq \emptyset$ *tenemos que encontrar un subconjunto denotado* $(-A)$ *tal que* $\emptyset = A \triangle (-A) = (A \cup (-A)) \setminus (A \cap (-A))$.

Por la definición de la operación $\triangle$ *tenemos que* $A \triangle A = \emptyset$.

Supongamos que $(-A) \neq A$ *y analicemos los siguientes dos casos. Si* $x \in A \setminus (-A)$, *entonces* $x \in A \triangle (-A)$, *análogamente si* $x \in (-A) \setminus A$, *entonces* $x \in A \triangle (-A)$, *en ambos casos tenemos que* $A \triangle A \neq \emptyset$. *Por lo que el inverso aditivo de* A *es* A *en* $\mathcal{P}_U$.

M1 $A \cap B = B \cap A$. *Ejercicio 1.11 inciso (b).*

M2 $A \cap (B \cap C) = (A \cap B) \cap C$. *Ejercicio 1.11 inciso (c).*

M3 *Vamos a encontrar un subconjunto* V *de* U ($V \in \mathcal{P}_U$) *tal que* $V \cap A = A$ *para todo* $A \in \mathcal{P}_U$.

Por propiedades de conjuntos tenemos que $U \cap A = A$ *para todo* $A \in \mathcal{P}_U$.

Supongamos que $V \neq U$ (U *es el conjunto universal*), *entonces existe un elemento* $b \in U$ *tal que* $b \notin V$. *Entonces* $\{b\} \in \mathcal{P}_U$ *y* $\{b\} \cap V = \emptyset$, *lo cual contradice que* $V \cap A = A$ *para todo* $A \in \mathcal{P}_U$. *Por lo que* U *es neutro multiplicativo en* $\mathcal{P}_U$.

D $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$. *Ejercicio 1.11 inciso (d).*

Con lo que concluimos que $(\mathcal{P}_U; \triangle, \cap)$ *es un anillo conmutativo con unidad.*

Denotaremos al conjunto de matrices de 2×2 con coeficientes enteros por $M_{2\times 2}[\mathbb{Z}]$. Si $A, B \in M_{2\times 2}[\mathbb{Z}]$ con $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ y $B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$, donde $a_{ij}, b_{ij} \in \mathbb{Z}$, definimos las operaciones suma y multiplicación para las matrices de 2×2 como sigue.

$$A + B = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix}.$$

$$AB = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}.$$

Ejemplo 1.1.9. *$M_{2\times2}[\mathbb{Z}]$ es un anillo con unidad con las operaciones usuales de matrices. Nótese que no es un anillo conmutativo.*

Por la definición de las operaciones en matrices y propiedades del anillo de los números enteros, las entradas de la matriz resultante son números enteros, y el conjunto $M_{2\times2}[\mathbb{Z}]$ está cerrado bajo la suma y el producto usual de matrices.

Primero probamos que el conjunto $M_{2\times2}[\mathbb{Z}]$ forma un grupo abeliano con la suma de matrices.

A1 La suma conmuta en $M_{2\times2}[\mathbb{Z}]$:

$$\begin{aligned} A+B &= \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} \\ a_{21}+b_{21} & a_{22}+b_{22} \end{pmatrix} \\ &\quad \text{la suma usual en } \mathbb{Z} \text{ es una operación conmutativa}, \\ &= \begin{pmatrix} b_{11}+a_{11} & b_{12}+a_{12} \\ b_{21}+a_{21} & b_{22}+a_{22} \end{pmatrix} = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} + \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \\ &= B+A. \end{aligned}$$

A2 La suma es asociativa en $M_{2\times2}[\mathbb{Z}]$:

$$\begin{aligned} A+(B+C) &= \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \left(\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} + \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} \right) \\ &= \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11}+c_{11} & b_{12}+c_{12} \\ b_{21}+c_{21} & b_{22}+c_{22} \end{pmatrix} \\ &= \begin{pmatrix} a_{11}+(b_{11}+c_{11}) & a_{12}+(b_{12}+c_{12}) \\ a_{21}+(b_{21}+c_{21}) & a_{22}+(b_{22}+c_{22}) \end{pmatrix} \\ &\quad \text{la suma usual en } \mathbb{Z} \text{ es una operación asociativa}, \\ &= \begin{pmatrix} (a_{11}+b_{11})+c_{11} & (a_{12}+b_{12})+c_{12} \\ (a_{21}+b_{21})+c_{21} & (a_{22}+b_{22})+c_{22} \end{pmatrix} \\ &= \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} \\ a_{21}+b_{21} & a_{22}+b_{22} \end{pmatrix} + \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} \\ &= \left(\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \right) + \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} \\ &= (A+B)+C. \end{aligned}$$

A3 $M_{2\times2}[\mathbb{Z}]$ tiene un elemento neutro aditivo: Sea $\mathbf{0}_{2\times2} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, entonces

$$\mathbf{0}_{2\times2} + A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} 0+a_{11} & 0+a_{12} \\ 0+a_{21} & 0+a_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = A.$$

Como la suma conmuta, $\mathbf{0}_{2\times2}$ es el neutro aditivo de $M_{2\times2}[\mathbb{Z}]$.

A4 Para cada $A \in M_{2\times2}[\mathbb{Z}]$*, existe un elemento inverso aditivo* $-A \in M_{2\times2}[\mathbb{Z}]$ *tal que*

$$A + (-A) = (-A) + A = \mathbf{0}_{2\times2}.$$

Sea $(-A) = \begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix}$*, entonces*

$$\begin{aligned} A + (-A) &= \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix} = \begin{pmatrix} a_{11} + (a_{11}) & a_{12} + (-a_{12}) \\ a_{21} + (-a_{21}) & a_{22} + (-a_{22}) \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \mathbf{0}_{2\times2} \end{aligned}$$

Como la suma conmuta, $(-A)$ *es el inverso aditivo de* A *en* $M_{2\times2}[\mathbb{Z}]$*. Por lo tanto* $M_{2\times2}[\mathbb{Z}]$ *con la suma de matrices forman un grupo abeliano.*

Ahora vamos a probar que el producto de matrices es asociativa, que hay una matriz unidad y que el producto de matrices se distribuye sobre la suma de matrices.

M2 La multiplicación es asociativa en $M_{2\times2}[\mathbb{Z}]$*.*

$A(BC) = (AB)C$*. Ejercicio 1.12.*

M3 $M_{2\times2}[\mathbb{Z}]$ *tiene un elemento neutro multiplicativo: Sea* $\boldsymbol{I}_{2\times2} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$*, entonces*

$$\begin{aligned} \boldsymbol{I}_{2\times2}A &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} 1(a_{11}) + 0(a_{21}) & 1(a_{12}) + 0(a_{22}) \\ 0(a_{11}) + 1(a_{21}) & 0(a_{12}) + 1(a_{22}) \end{pmatrix} \\ &= \begin{pmatrix} a_{11} + 0 & a_{12} + 0 \\ 0 + a_{21} & 0 + a_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = A. \end{aligned}$$

$$\begin{aligned} A\boldsymbol{I}_{2\times2} &= \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1(a_{11}) + 0(a_{12}) & 0(a_{11}) + 1(a_{12}) \\ 1(a_{21}) + 0(a_{22}) & 0(a_{21}) + 1(a_{22}) \end{pmatrix} \\ &= \begin{pmatrix} a_{11} + 0 & 0 + a_{12} \\ a_{21} + 0 & 0 + a_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = A. \end{aligned}$$

D La multiplicación se distribuye sobre la suma en $M_{2\times2}[\mathbb{Z}]$*.*

$$\begin{aligned} A(B+C) &= \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\left(\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} + \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}\right) \\ &= \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} b_{11} + c_{11} & b_{12} + c_{12} \\ b_{21} + c_{21} & b_{22} + c_{22} \end{pmatrix} \\ &= \begin{pmatrix} a_{11}(b_{11} + c_{11}) + a_{12}(b_{21} + c_{21}) & a_{11}(b_{12} + c_{12}) + a_{12}(b_{22} + c_{22}) \\ a_{21}(b_{11} + c_{11}) + a_{22}(b_{21} + c_{21}) & a_{21}(b_{12} + c_{12}) + a_{22}(b_{22} + c_{22}) \end{pmatrix} \\ &= \begin{pmatrix} (a_{11}b_{11} + a_{12}b_{21}) + (a_{11}c_{11} + a_{12}c_{21}) & (a_{11}b_{12} + a_{12}b_{22}) + (a_{11}c_{12} + a_{12}c_{22}) \\ (a_{21}b_{11} + a_{22}b_{21}) + (a_{21}c_{11} + a_{22}c_{21}) & (a_{21}b_{12} + a_{22}b_{22}) + (a_{21}c_{12} + a_{22}c_{22}) \end{pmatrix} \\ &= \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix} + \begin{pmatrix} a_{11}c_{11} + a_{12}c_{21} & a_{11}c_{12} + a_{12}c_{22} \\ a_{21}c_{11} + a_{22}c_{21} & a_{21}c_{12} + a_{22}c_{22} \end{pmatrix} \\ &= \left(\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}\right) + \left(\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}\right) \\ &= AB + AC. \end{aligned}$$

Ejemplo 1.1.10. *Dado un anillo* $(A;\oplus,\odot)$*. Se tiene que* $M_{n\times n}[A]$ *es un anillo con las operaciones usuales de matrices. Si además* $(A;\oplus,\odot)$ *tiene unidad, entonces* $M_{n\times n}[A]$ *también tiene unidad.*

1.1.4 Ejercicios

Ejercicio 1.1. *Para el grupo de simetrías del triángulo equilátero, comprueba la propiedad asociativa.*

Ejercicio 1.2. *Para el grupo de simetrías del triángulo equilátero, encuentra una expresión algebráica para las operaciones* E_iR_j, R_iE_j, E_iE_j *y* R_iR_j.

Ejercicio 1.3. *Determine y justifica si cada uno de los siguientes conjuntos forman un anillo con las operaciones (suma y producto) usuales de los números reales.*

i) $A = \left\{a + b\sqrt{2} + c\sqrt{3} : a, b, c \in \mathbb{Z}\right\}$. *ii)* *Sea* $A = \{7n : n \in \mathbb{Z}\}$.

Ejercicio 1.4. *Usando los axiomas de anillo, demuestra que si* $(A,\oplus,\odot)$ *es un anillo, con neutro aditivo* $\mathbf{0}$*, entonces para todo* $a, b, c \in A$ *se tiene las siguientes propiedades.*

i) *Si* $a \oplus b = a \oplus c$*, entonces* $b = c$.

ii) *Si* $a \oplus b = a$*, entonces* $b = \mathbf{0}$.

iii) $-(a \odot a) = (-a) \odot a$ *para todo* $a \in A$.

iv) $\mathbf{0} \odot a = \mathbf{0}$ *para todo* $a \in A$.

Ejercicio 1.5. *¿Bajo que condiciones se tiene que si* $a \odot b = a \odot c$*, entonces* $b = c$*?*

Ejercicio 1.6. *Prueba que los conjuntos del ejemplo 1.1.4 en efecto forman un dominio entero.*

Ejercicio 1.7. *Prueba que los conjuntos de de los números complejos* $\mathbb{C}$ *forman un dominio entero.*

Ejercicio 1.8. *Demuestra que en un dominio entero se cumple la siguiente propiedad de cancelación:*

$$\text{Si } ab = ac,\ a \neq 0,\ \text{entonces } b = c.$$

Ejercicio 1.9. *Sea* $\mathbf{K}$ *un campo, probar que* $\mathbf{K}$ *forma un dominio entero.*

Ejercicio 1.10. *Considere al conjunto* $\mathbb{Z}$ *con las operaciones (binarias)* $\oplus$ *y* $\odot$ *definidas para cualesquier* $x, y \in \mathbb{Z}$ *como:*

$$x \oplus y := x + y - 3, \qquad x \odot y := x + y - xy.$$

¿Qué Axiomas de anillo cumple $\mathbb{Z}$ *con las operaciones* $\oplus$ *y* $\odot$ *y cuales no? ¿Es* $(\mathbb{Z},\oplus,\odot)$ *un anillo?*

Ejercicio 1.11. *Sean* A, B, C *tres conjuntos. Para completar la prueba del ejemplo 1.1.8, prueba las siguientes:*

i) $A \triangle (B \triangle C) = (A \triangle B) \triangle C$, *(Axioma A2).*

ii) $A \cap B = B \cap A$, *(Axioma M1).*

iii) $A \cap (B \cap C) = (A \cap B) \cap C$, *(Axioma M2).*

iv) $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$, *(Axioma D).*

Ejercicio 1.12. *Prueba que la multiplicación es una operación asociativa en* $M_{2\times2}[\mathbb{Z}]$.

Ejercicio 1.13. *Verificar que la multiplicación* $M_{2\times2}[\mathbb{Z}]$ *no es una operación conmutativa, es decir, encuentra dos matrices* $A, B \in M_{2\times2}[\mathbb{Z}]$*, tales que* $AB \neq BA$.

1.2 Anillos y estructura modular

Motivamos el estudio de los anillos Z_n con la aritmética del reloj. Una vez comprendido la aritmética del reloj, definimos formalmente el anillo $\mathbb{Z}_n$, sus operaciones y estudiamos la relación entre el anillo $\mathbb{Z}_n$ y la relación de congruencia.

1.2.1 Aritmética del reloj

Ejemplo 1.2.1. *Resuelve las ecuaciones para un reloj de 5 horas (ver figura 1.5).*
i) $x + 4 = 2$. *ii*) $2 = 4x$. *iii*) $x = 2 - 4$. *iv*) $1 = 2x$.

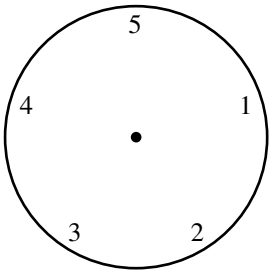


Figura 1.5: Reloj de 5 horas.

En un reloj de 5 *horas sólo tenemos los valores* 1, 2, 3, 4, 5. *Las manecillas del reloj no pueden mostrar el número* -3 *ni el número* 8. *Igual que en un reloj acrómico, cuando se pasamos de las* 5 *horas, el reloj muestra el número correspondiente sin tomar en cuenta el número de vueltas que llevamos.*

i) $x + 4 = 2$*: Como el reloj no tiene números negativos, el resultado de* x *tiene que pasar después de al menos una vuelta. El cuadro 1.2 muestra el resultado de* $x + 4$ *según el valor de* x *y podemos ver que* $x = 3$ *es un resultado para la ecuación* $x + 4 = 2$.

ii) $4x = 3$*: Como el reloj no tiene números racionales, el resultado de* x *tiene que pasar después de al menos una vuelta. El cuadro 1.3 muestra el resultado de* $4x$ *según el valor de* x *y podemos ver que* $x = 2$ *es un resultado para la ecuación* $4x = 3$.

Cuadro 1.2: El resultado de $x + 4$ en un reloj de 5 horas.

x	1	2	3	4	5
$x+4$	5	1	2	3	4

Cuadro 1.3: El resultado de $4x$ en un reloj de 5 horas.

x	1	2	3	4	5
$4x$	4	3	2	1	5

iii) $x = 2 - 4$*: Como el reloj no tiene números negativos, el resultado de x se puede obtener regresando las manecillas cuatro horas (es decir, recorrer en sentido contrario), y obtenemos que* $x = 3$.

iv) $1 = 2x$*: Igual que en el inciso ii*) *construimos un cuadro que muestre el resultado de* $2x$*. En el cuadro 1.4 podemos ver que* $x = 3$ *es un resultado para la ecuación* $1 = 2x$.

Cuadro 1.4: El resultado de $4x$ en un reloj de 5 horas.

x	1	2	3	4	5
$2x$	2	4	1	3	5

En el ejercicio 1.14, hacemos las mismas preguntas que en el ejemplo 1.2.1 para un reloj de 6 horas. Podemos preguntar cuáles son las características del número $a \in \{1, 2, 3, 4, 5, 6\}$ para que la ecuación $ax = 1$ tenga solución en el reloj de 6. También podemos preguntar cuáles son las características del número de horas de un reloj para que la ecuación $ax = 1$ siempre tenga solución. Estas preguntas serán respondidas en la seguiente sección.

1.2.2 Estructura modular y el anillo $\mathbb{Z}_n$

Sea $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ y sean $a, b \in \mathbb{Z}_n$. Definimos las operaciones suma y producto en $\mathbb{Z}_n$ como sigue.

$$\begin{aligned} a \oplus b &= r, \quad \text{donde } a + b = nq + r \text{ y } 0 \leq r < n. \\ a \otimes b &= r, \quad \text{donde } ab = nq + r \text{ y } 0 \leq r < n. \end{aligned}$$

Nótese que el residuo r de un número m entre n es un número en $\mathbb{Z}_n$, por lo que $\mathbb{Z}_n$ está cerrada bajo ambos operaciones además, por el *algoritmo de la división*, el residuo es único así que las operaciones están bien definidas.

Ejemplo 1.2.2. *En el cuadro 1.5 y en el cuadro 1.6 se encuentran las tablas de la suma y el producto en* $\mathbb{Z}_5$ *y* $\mathbb{Z}_6$ *respectivamente. En estos dos cuadros podemos observar lo siguiente:*

Cuadro 1.5: Las tablas de suma y multiplicación de $\mathbb{Z}_5$.

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\otimes$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Cuadro 1.6: Las tablas de suma y multiplicación de $\mathbb{Z}_6$.

$\oplus$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\otimes$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

1. *Tanto $\mathbb{Z}_5$ como $\mathbb{Z}_6$ son anillos conmutativos con unidad. Esta observación resulta cierta en general (es decir para todo $\mathbb{Z}_n$), pero hace falta demostrarla.*

2. *En el anillo $\mathbb{Z}_5$ el 0 no tiene divisores propios por lo que $\mathbb{Z}_5$ es un dominio entero, mientras que $\mathbb{Z}_6$ no no es un dominio entero, ya que $3 \otimes 2 = 0$.*

3. *En $\mathbb{Z}_5$ todo elemento tiene inverso multiplicativo, mientras que en $\mathbb{Z}_6$ solamente el 1 y el 5 tiene inverso multiplicativo, por lo que $\mathbb{Z}_5$ sí es un campo y $\mathbb{Z}_6$ no lo es.*

Teorema 1.2.1. *Sea $n \in \mathbb{N}$, con $n \geq 2$. Entonces $(\mathbb{Z}_n; \oplus, \otimes)$ es un anillo conmutativo con unidad.*

Demostración. El conjunto $\mathbb{Z}_n$ está cerrado bajo las operaciones $\oplus$ y $\otimes$ porque el residuo de un a número m entre n es un número en $\mathbb{Z}_n$. Probaremos primero que $\mathbb{Z}_n$ forma un grupo abeliano con la suma.

A1 La operación $\oplus$ es conmutativa en $\mathbb{Z}_n$.

Sean $a, b \in \mathbb{Z}_n$ y sean $a \oplus b = r$ y $b \oplus a = r'$. Entonces $a + b = np + r$ y $b + a = np' + r'$ con $0 \leq r, r' < n$. Como $a + b = b + a$ y el residuo es único, por el algoritmo de la división, se sigue que $r = r'$ y $a \oplus b = b \oplus a$.

A2 La operación $\oplus$ es asociativa en $\mathbb{Z}_n$.

Sean $a, bc \in \mathbb{Z}_n$, y sean $b \oplus c = r_1$ y $a \oplus b = r_2$.

$a\oplus(b\oplus c) = a\oplus(r_1) = a\oplus(b+c-nq_1) = r_1' = (a+(b+c-nq_1))-nq_1' = (a+b+c-n(q_1+q_1'))$.

$(a\oplus b)\oplus c = (r_2)\oplus c = (a+b-nq_2)\oplus c = r_2' = (a+b)+c-nq_2))-nq_2' = (a+b+c-n(q_2+q_2'))$.

Por lo tanto $a+b+c = n(q_1+q_1')+r_1'$ y $a+b+c = n(q_2+q_2')+r_1'$ y por el algoritmo de la división, se sigue que $r_1' = r_2'$ y $a\oplus(b\oplus c) = a\oplus(b\oplus c)$.

A3 Existe un neutro aditivo z en $\mathbb{Z}_n$ tal que $a+z = z+a = a$ para todo $a\in\mathbb{Z}_n$.

Vamos a probar que 0 es neutro aditivo $\mathbb{Z}_n$. Sea $a\in\mathbb{Z}_n$, entonces $0\le a<n$.

$a\oplus 0 = r$ donde $a = a+0 = nq+r$ y $0\le r<n$. Como $0\le a<n$ y el residuo es único, entonces $r=a$ y $a\oplus 0 = a$.

Por lo tanto $z=0$ es neutro aditivo en $\mathbb{Z}_n$.

A4 Todo elemento $a\in\mathbb{Z}_n\setminus 0$ tiene inverso aditivo, denotado $(-a)$. Sea $a\in\mathbb{Z}_n\setminus 0$, entonces $0<a<n$.

Vamos a probar que $n-a$ es inverso aditivo de a.

Como $0<a<n$, entonces $-n<-a<0$, $n-n<n-a<n+0$ y $0<n-a<n$, por lo que $n-a\in\mathbb{Z}_n$.

$a\oplus(n-a) = r$ donde $a+(n-a) = nq+r$, por lo que $q=1$ y $r=0$.

Por lo tanto el inverso aditivo de a en $\mathbb{Z}_n$ es $n-a$.

La prueba de las otras propiedades ($M1, M2, M3, D$) se dejan como ejercicio (ejercicio 1.17). □

Queremos clasificar los anillos $\mathbb{Z}_n$ que resultan ser campos. Para lograr esta tarea resulta conveniente construir la table de suma y multiplicación en $\mathbb{Z}_{12}$ y determinar qué elementos sí tienen inverso multiplicativo (ejercicio 1.18).

Proposición 1.2.2. *Sea $n\in\mathbb{N}$, con $n\ge 2$ y sea $a\in\mathbb{Z}_n\setminus\{0\}$. El elemento a tiene inverso multiplicativo en $\mathbb{Z}_n$ si y sólo si $mcd(a,n)=1$.*

Demostración. Sea $a\in\mathbb{Z}_n$ con $a>0$ tal que a tiene un inverso multiplicativo $a^{-1}\in\mathbb{Z}_n$, entonces $a\otimes(a^{-1}) = 1$, entonces $a(a^{-1}) = 1+nq$ para alguna $q\in\mathbb{Z}$, y $a(a^{-1})-nq = 1$ implica que 1 es combinación lineal de a y n. Como 1 es el menor entero positivo, 1 es la combinación lineal mínima positivo de a y n y se sigue que $mcd(n,a)=1$.

Si $mcd(n,a)=1$, entonces 1 es combinación lineal de a y n y existen $r,s\in\mathbb{Z}$ tales que $ar+ns=1$ lo cual implica que $ar = n(-s)+1$ y por la definición del producto en $\mathbb{Z}_n$ se tiene que $a\otimes r = 1$ y r es inverso multiplicativo de a. □

Teorema 1.2.3. *Sea $n\in\mathbb{N}$, con $n\ge 2$. Entonces $\mathbb{Z}_n$ es un campo si y solo si n es un número primo.*

Demostración. Consecuencia de la proposición 1.2.2. □

1.2.3 Congruencias

En este capítulo estudiamos la relación **congruencia** (o función módulo).

Definición 1.2.4. *Sea $n \in \mathbb{N}$, con $n \geq 2$. Sean $a, b \in \mathbb{Z}$. Decimos que "a* **es congruente** *con b* módulo *n", y lo denotamos $a \equiv b$ (**mod** n), si $n \mid a - b$.*[1]

Observación 1.2.5. *Sean $a, b, n \in \mathbb{Z}$, con $n \geq 2$ tales que $a \equiv b$ (**mod** n), entonces*

1. *$a = b + nk$, para alguna $k \in \mathbb{Z}$, ya que $n \mid a - b$*
2. *El residuo de a entre n es igual al residuo de b entre n.*

Proposición 1.2.6. *Dado $n \in \mathbb{N}$, con $n \geq 2$. La "a congruente con b módulo n" es una relación de equivalencia.*[2]

Demostración. Ejercicio 1.23. Como la congruencia es una relación de equivalencia, esta tiene sus clases de equivalencia. Ver ejercicio 1.25. □

Proposición 1.2.7. *Sea $a, b, c, d, n \in \mathbb{Z}$, con $n \geq 2$.*

1. *Si $a \equiv b$ (**mod** n) y $c \equiv d$ (**mod** n), entonces $a + c \equiv b + d$ (**mod** n).*
2. *Si $a \equiv b$ (**mod** n), entonces $ac \equiv bc$ (**mod** n).*

Demostración. Sean $a, b, c, d, n \in \mathbb{Z}$, con $n \geq 2$ tales que

1. $a \equiv b$ (**mod** n) y $c \equiv d$ (**mod** n). Por definición tenemos que $n \mid a - b$ y $n \mid c - d$, entonces $n \mid ((a-b)+(c-d))$, por lo que $n \mid ((a+c)-(b+d))$, aplicamos la definición de congruencia y se sigue el resultado $(a + c) \equiv (b + d)$ (**mod** n).
2. Ejercicio 1.26.

□

Ejemplo 1.2.3. *Encuentra todas las soluciones de*

$$23x \equiv 11 \quad (\textbf{mod}\ 19). \tag{1.1}$$

Por definición tenemos que $23x - 11 = 19k$, con $k \in \mathbb{Z}$, entonces $23x - 19k = 11$. El número 11 es combinación lineal de 23 y 19 si y sólo si mcd$(19, 23) \mid 11$.

Encontramos el máximo común divisor de 19 y 23 usando el algoritmo de Euclides[2] *para luego escribir el máximo común divisor como combinación lineal de 19 y 23.*

$$\begin{aligned} 23 &= 19(1) + 4 \\ 19 &= 4(4) + 3 \\ 4 &= 3(1) + 1 \\ 3 &= 1(3) + 0. \end{aligned}$$

[1] $n|a$ — b si existe $k \epsilon Z$ tal que a-b=kn

[2] visto en la UEA *Matemáticas Discretas I*

Por lo que $mcd(19, 23) = 1$ *y como* $1 \mid 11$*, podemos escribir* 11 *como combinación lineal de* 23 *y* 19.

$$\begin{aligned} 1 &= 4 - 3 = 4 - (19 - 4(4)) = 4 - 19 + 4(4) = -19 + 5(4) \\ &= -19 + 5(23 - 19) = -19 + 5(23) - 5(19) = 5(23) - 6(19) \\ 1 &= 5(23) - 6(19). \end{aligned}$$

Multiplicamos por 11 *ambos lados y tenemos que*

$$11 = (55)(23) - (66)(19).$$

De esta manera tenemos que $x = 55$ *es una solución de la congruencia. Por el ejercicio 1.30 las soluciones de la congruencia (1.1) son aquellas que satisfacen*

$$s \equiv 55 \pmod{19}.$$

La solución en $\mathbb{Z}_{19}$ *es* 17 *y el conjunto* S *de todas las soluciones de la congruencia (1.1) es*

$$S = \{17 + 19k : k \in \mathbb{Z}\}.$$

Proposición 1.2.8. *Sean* $a, b, n \in \mathbb{Z}$*, con* $n \geq 2$*. La congruencia* $ax \equiv b \pmod{n}$ *tiene solución si y sólo si* $d \mid b$*, donde* $d = mcd(a, n)$*.*

Demostración. Ejercicio 1.34. □

1.2.4 Ejercicios

Ejercicio 1.14. *Considera el reloj de* 6 *y resuelva las siguientes ecuaciones:*

i) $x + 5 = 2$. *ii*) $4x = 2$. *iii*) $3x = 2$. *vi*) $5x = 1$. *v*) $1 = 4x$.

Ejercicio 1.15. *Resuelva las siguientes ecuaciones primero para el reloj de 12 horas y luego para el reloj de 15 horas:*

i) $x + 7 = 5$. *ii*) $3 = 7x$. *iii*) $4 = 3x$. *vi*) $x = 2 - 9$. *v*) $1 = 2x$.

Ejercicio 1.16. *Construye las tablas de sumar y multiplicar para el anillo* $\mathbb{Z}_8$*. En base a esto, encuentra los inversos aditivos e inversos multiplicativos (para los que tengan).*

Ejercicio 1.17. *Completa la prueba del teorema 1.2.1.*

Ejercicio 1.18. *Construye las tablas de sumar y multiplicar para el anillo* $\mathbb{Z}_{12}$*. En base a esto, encuentra los inversos aditivos e inversos multiplicativos (para los que tengan). ¿Qué propiedad tienen en común los elementos de* $\mathbb{Z}_{12}$ *que no tienen inverso multiplicativo? y ¿qué propiedad tienen los que sí tienen inverso multiplicativo?*

Ejercicio 1.19. *Calcula el inverso multiplicativo de cada uno de los siguientes números (para los que tengan y en caso de no tener, explica el por qué no tiene) en* $\mathbb{Z}_{2016}$*:*

i) *35* . *ii*) *121* . *iii*) *445.*

Ejercicio 1.20. *De un ejemplo de un anillo en donde no se cumpla el axioma 1.1.5.*

Ejercicio 1.21. *Prueba que* $\mathbf{Z}_n$ *con la suma y el producto usual forma un dominio entero.*

Ejercicio 1.22. *Sean* $a, b, n \in \mathbb{Z}$*, con* $n > 0$ *y* $a \equiv b$ (***mod*** n)*. Entonces* $a + n \equiv b$ (***mod*** n)*.*

Ejercicio 1.23. *Prueba la proposición 1.2.6.*

Ejercicio 1.24. *Prueba que la relación de congruencia es una relación de equivalenca. Encuentra las clases de equivalencia de la relación* $a \equiv b$ (***mod*** 7)*. ¿Cuántas son?. ¿Cuántas clases de equivalencia tiene la relación* $a \equiv b$ (***mod*** n)*?*

Ejercicio 1.25. *En cada inciso enumera cuatro elemento de la clase de equivalencia de la relación de congruencia con el módulo correspondiente.*

i) [2] *módulo* 5. *ii*) [3] *módulo* 9. *iii*) [8] *módulo* 18.

Ejercicio 1.26. *Prueba el inciso 2. de la proposición 1.2.7.*

Ejercicio 1.27. *¿Bajo que condiciones se tiene que* $ab \equiv ac$ (***mod*** n)*, implica que* $b \equiv c$ (***mod*** n)*?*

Ejercicio 1.28. *Sean* $a, b, m, n \in \mathbb{Z}$*, con* $n, m \geq 2$ *tales que* $a \equiv b$ (***mod*** n)*, entonces* $a^m \equiv b^m$ (***mod*** n)*.*
(Hint: Inducción Matemático)

Ejercicio 1.29. *Verifica que para todo* $k \in \mathbb{Z}$ *se tiene que* $x = 55 \pm (19)k$ *es solución de la congruencia en el ejemplo 1.2.3.¿ Es* 17 *la única solución de la congruencia en* $\mathbb{Z}_{19}$*?*

Ejercicio 1.30. *Sean* $a, b, n \in \mathbb{Z}$*, con* $n \geq 2$ *y* $mcd(a, n) = 1$*. Si* s_1, s_2 *son soluciones de la congruencia* $ax \equiv b$ (***mod*** n)*, entonces* $s_1 \equiv s_2$ (***mod*** n)*.*

Ejercicio 1.31. *Prueba que para todo* $n \in \mathbb{Z}$*, exactamente uno de los enteros* $n,\ 2n-1,\ 2n+1$ *es divisible entre* 3*.*

Ejercicio 1.32. *Dado una congruencia* $ax \equiv b$ (***mod*** n) *que tiene solución,¿ Bajo qué condiciones hay una única solución en* $\mathbb{Z}_n$*?*

Ejercicio 1.33. *Resuelve las siguientes congruencias.*

i) $35x \equiv 42$ (***mod*** 2009). *ii*) $121x \equiv 72$ (***mod*** 2009).

Ejercicio 1.34. *Prueba la proposición 1.2.8.*

Ejercicio 1.35. *Uno de los primeros sistemas de criptografía es basado en la posición de la letra en una tabla o en el alfabeto. Fue usado por los griegos y romanos. Por ejemplo, si cada letra en un texto se sustituye por la letra siete lugares hacia la derecha en el alfabeto, la palabra* astuto *se convierte en la palabra* hzabav *ya que* $a \to h$*,* $s \to z$*,* $t \to a$*,* $u \to b$ *y* $o \to v$*. ¿Cuál fue el movimiento que se aplicó a la siguiente frase* Oe zivheh wmipvi wi leooe iq oe wmpqogmheh*?*

1.3 Álgebra Booleana

En esta sección estudiamos la estructura algebraíca llamada *álgebra booleana* desarrollada por el filósofo y matemático inglés George Boole.[3] El *álgebra booleana* consiste en un método para resolver problemas de lógica que recurre solamente a los valores binarios 1 y 0 y a tres operadores fundamentales: suma $(+, \wedge, \cup, o)$, producto $(\cdot, \vee, \cap, y)$ e inverso (inverso, negación, complemento, no) y tiene muchas aplicaciones prácticas en la física, la biología, las matemáticas, ingeniería, electrónica, y especialmente en la informática; el álgebra de booleana es considera como la base de la aritmética computacional moderna.

Sea $B = \{0, 1\}$. Definimos las operaciones suma $+$, producto $\cdot$ e inverso entre elementos booleanos. Como sólo tenemos dos posibles valores, definimos exhaustivamente las operaciones:

$$\begin{array}{lll} \text{Suma} & 0+0=0, & 0+1=1+0=1+1=1, \\ \text{Producto} & 1\cdot 1=1, & 0\cdot 1=1\cdot 0=0\cdot 0=0, \\ \text{Inverso} & \overline{0}=1, & \overline{1}=0. \end{array}$$

Sea $x \in B$, con $B = \{0, 1\}$. De la definición podemos establecer las siguientes propiedades.

$$\begin{array}{lll} x+x=x, & & \\ x^2=x\cdot x=x, & & \\ x+y=0 & \Leftrightarrow & x=y=0, \\ x\cdot y=1 & \Leftrightarrow & x=y=1. \end{array}$$

Ejemplo 1.3.1. *Lógica matmática. El valor de verdad de una proposición es un elemento del conjunto $\{\mathcal{F}, \mathcal{V}\}$. Este conjunto forma con las operaciones conjunción $\wedge$, disyunción $\vee$ y negación $\neg$ un algebra booleana con los valores falso $\mathcal{F}$ y verdadero $\mathcal{V}$ representados por 0 y 1 respectivamente. La* **tabla de verdad** *de las operaciones definidas entre dos proposiciones $P, Q \in \{\mathcal{F}, \mathcal{V}\}$ es:*

Cuadro 1.7: La tabla de verdad de $P \wedge Q$, $P \vee Q$ y $\neg P$.

P	Q	$P \wedge Q$	$P \vee Q$	$\neg P$
0	0	0	0	1
0	1	1	0	1
1	0	1	0	0
1	1	1	1	0

Para P y Q y se tiene que

$$\begin{array}{lll} x\wedge x=x & & x\vee x=x \\ x\wedge y=0 & \Leftrightarrow & x=y=0 \\ x\vee y=1 & \Leftrightarrow & x=y=1 \end{array}$$

[3] George Boole (1815-1864) filósofo y matemático inglés se considera junto con De Morgan y Newton como los que desarrollaron la lógica simbólica (la representación del razonamiento mediante símbolos matemáticos). Boole desarrolló el *álgebra booleana* la aplico a la lógica en su obra *Investigación sobre las leyes del pensamiento* (1854) y argumentó que la lógica debería ser una rama de las matemáticas y no de la filosofía.

Cuadro 1.8: La tabla de verdad para conjuntos.

A	B	$A \cup B$	$A \cap B$	$\overline{A}$
0	0	0	0	1
0	1	1	0	1
1	0	1	0	0
1	1	1	1	0

Ejemplo 1.3.2. *Sea $\mathcal{U}$ el conjunto universal (no vacío). Entonces $\{\mathcal{U}, \emptyset\}$ con las operaciones unión, $\cup$, intersección, $\cap$, y complemento, —, forma un algebra booleana con los elementos $\emptyset, \mathcal{U}$, representados por 0 y 1 respectivamente.*

y para $A, B \in \{\mathcal{U}, \emptyset\}$ se tiene que

$$\begin{array}{lcl} A \cup A = A & & A \cap A = A \\ A \cup B = 0 & \Leftrightarrow & A = B = 0 \\ A \cap B = 1 & \Leftrightarrow & A = B = 1 \end{array}$$

1.3.1 Funciones booleanas

En el álgebra booleana es fundamental la existencia de una forma algebraica que proporcione explícitamente el valor de una función para todas las combinaciones de los valores de las variables. Por ejemplo, si tienes una proposición compuesta que consta de conjunciones y disyunciones entre varias proposiciones.

Ejemplo 1.3.3. *Sea $P = P_1 \wedge (P_2 \vee P_3) \wedge \neg(P_4 \vee P_5)$ una proposición compuesta por las proposiciones $P_1, P_2, \ldots, P_5$. El valor de la proposición P está en función del valor de las 5 proposiciones y podemos escribir que*

$$P = f(P_1, P_2, P_3, P_4, P_5) = P_1 \wedge (P_2 \vee P_3) \wedge \neg(P_4 \vee P_5).$$

Como el valor de P es un elemento de B tenemos que $P : B^5 \to B$. La función tiene $|B|^5 = 2^5 = 32$ casos distintos en donde tendríamos que evaluar la función.

Ejemplo 1.3.4. *Evalua las siguientes dos funciones booleanas en* $(1, 1, 0, 0)$.

$$i) \quad f(w,x,y,z) = wx + x\overline{y} + yz. \qquad ii) \quad f(w,x,y,z) = xy + wx\overline{y}\,\overline{z} + \overline{y}\,z.$$

$i)$ $f(w,x,y,z) = wx + x\overline{y} + yz$ $\quad f(1,1,0,0) = 1 \cdot 1 + 1\overline{0} + 0 \cdot 0 = 1 + 1 + 0 = 1.$

$ii)$ $f(w,x,y,z) = xy + wx\overline{y}\,\overline{z} + \overline{y}\,z$ $\quad f(1,1,0,0) = 1 \cdot 0 + 1 \cdot 1 \cdot \overline{0} \cdot \overline{0} + \overline{0} \cdot 0 = 0 + 1 + 0 = 1.$

Definición 1.3.1. *Una* **función booleana** *es una función $f : B^n \to B$, con $n \geq 2$, cuyas variables son binarias y se rigen bajo los operadores del álgebra booleana.*

Proposición 1.3.2. *Sea $n \in \mathbb{Z}$, con $n \geq 2$, y sean dos funciones booleanas $f, g : B^n \to B$. Sea $b = (b_1, b_2, \ldots, b_n)$ con $b_1, b_2, \ldots, b_n \in B$. Entonces*

(i) $\overline{f}(b_1, b_2, \ldots, b_n) = \overline{f(b_1, b_2, \ldots, b_n)}$,

(*ii*) $(f+g)(b) = f(b) + g(b)$,

(*iii*) $fg(b) = f(b)g(b)$.

Las funciones booleanas se pueden representar algebraicamente, por medio de una tabla de verdad, numérica y con una gráfica. La representación que se use dependerá de uso que se busca.

Ejemplo 1.3.5. *Sea* $f : B^3 \to B$, *dada por* $f(x, y, z) = x \cdot y + z$ *o bien* $f(x, y, z) = (x \vee y) \wedge z$.

Cuadro 1.9: La tabla de la función booleana $f(x, y, z) = x \cdot y + z$.

x	y	z	xy	$xy + z$
0	0	0	0	0
0	0	1	0	1
0	1	0	0	0
0	1	1	0	1
1	0	0	0	0
1	0	1	0	1
1	1	0	1	1
1	1	1	1	1

Ejemplo 1.3.6. *Simplifica la expresión booleana* $x + xy$.
$x + xy = x1 + xy = x(1 + y) = x1 = x$.

Ejemplo 1.3.7. *Simplifica la expresión booleana* $(wx + \overline{\overline{x}z})(w + x + y + \overline{z})$.

$$\begin{aligned}(wx + \overline{\overline{x}z})(w + x + y + \overline{z}) &= (wx + x + \overline{z})(w + x + y + \overline{z}) \\ &= (x(w + 1) + \overline{z})(w + x + y + \overline{z}) \\ &= (x + \overline{z})((x + \overline{z}) + (w + y)) = x + \overline{z}.\end{aligned}$$

Definición 1.3.3. *Una* **literal** x_i *es un número fijo, en el caso de álgebras booleanas* $x_i \in \{0, 1\}$. *Las literales no son variables.*

En el álgebra booleana la simplificación de una expresión algebraica no es única como lo es en el caso de los números reales. Por eso surge la necesidad de tener expresiones algebraicas que son únicas para poder comparar y determinar si dos expresiones son iguales o no. Vamos a estudiar dos expresiones de una función booleana con la propiedad de ser única: la función normal disyuntiva y la función normal conjuntiva.

Función normal disyuntiva

Si un sumando de la expresión es una conjunción de todas las variables, decimos que es una conjunción fundamental. En el ejemplo 1.3.6 xy es una conjunción fundamental, mientras que en el ejemplo 1.3.4 xy no es una conjunción fundamental pero $wx\overline{y}\,\overline{z}$ si lo es.

Definición 1.3.4. *Sea* $f : B^n \to B$, *una función booleana. Decimos que y es una* **conjunción fundamental**, *si* $y = y_1 y_2 \dots y_n$ *con* $y_i \in \{x_i, \overline{x_i}\}$, *para* $1 \leq i \leq n$.

Definición 1.3.5. *Sea $f : B^n \to B$, una función booleana. La* **función normal disyuntiva** (*f.n.d.*) *de la función f es una representación de f en suma (disyunción) de conjunciones (productos) fundamentales.*

Para encontrar la *f.n.d.* de una función booleana $f : B^n \to B$, se evalúa la función en todas los casos posibles usando una tabla de verdad. Recordamos que $x_1x_2 \ldots x_n = 1$ si y solo si $x_1 = x_2 = \ldots = x_n = 1$, es decir, si el valor de la función es 1, entonces al menos uno de sus conjunciones fundamentales tiene valor 1. Los conjunciones fundamentales cuyo valor es 1 reciben el nombre de **mintérminos**, es decir, una conjunción fundamental $y = y_1y_2 \ldots y_n$ es un mintérmino si $y_i = x_i$ si $x_i = 1$ y $y_i = \overline{x_i}$ si $x_i = 0$. La expresión *f.n.d.* es la disyunción de todos los mintérminos.

Ejemplo 1.3.8. *Considera la función booleana $f : B^3 \to B$, dada por $f(x, y, z) = x \cdot y + z$ (del ejemplo 1.3.5). Construimos la tabla para encontrar los mintérminos de la función (ver cuadro 1.10).*

Cuadro 1.10: La tabla con mintérminos de la función booleana $f(x, y, z) = x \cdot y + z$.

x	y	z	xy	$xy + z$	mintérminos
0	0	0	0	0	
0	0	1	0	**1**	$\overline{x}\,\overline{y}z$
0	1	0	0	0	
0	1	1	0	**1**	$\overline{x}yz$
1	0	0	0	0	
1	0	1	0	**1**	$x\overline{y}z$
1	1	0	1	**1**	$xy\overline{z}$
1	1	1	1	**1**	xyz

La f.n.d. es $f(x, y, z) = \overline{x}\,\overline{y}z + \overline{x}yz + x\overline{y}z + xy\overline{z} + xyz.$

Si n es un número grande, la expresión de la *f.n.d.* de una función dado, puede resultar poco práctico y poco manejable. Vamos a definir una expresión simplificada de la *f.n.d.* que resulta mas práctica. A cada mintérmino $y = y_1y_2 \ldots y_n$ le vamos a asociar el número binario de n bits $x_1x_2 \ldots x_n$. Es decir, si $y_i = x_i$, entonces $x_i = 1$ y si $y_i = \overline{x_i}$, entonces $x_i = 0$. En el ejemplo 1.3.8 el mintérmino $\overline{x}\,\overline{y}z$ corresponde al caso $x = 0$, $y = 0$, $z = 1$ que representa el número binario 001_2, cuyo valor decimal es 1, como el valor decimal del mintérmino $\overline{x}\,\overline{y}z$ es 1 lo denotamos por m_1. El mintérmino $\overline{x}\ y\ z$ corresponde al caso $x = 0$, $y = 1$, $z = 1$ que representa el número binario 011_2, cuyo valor decimal es 3, como el valor decimal del mintérmino $\overline{x}\ y\ z$ es 3 lo denotamos por m_3. Si $m_{i_1}, m_{i_2}, \ldots, m_{i_k}$ son todos los mintérminos de la *f.n.d.*, podemos expresar la como una suma de los valores decimales asociados a cada mintérmino:

$$f(x_1, x_2, \ldots, x_n) = \sum{}_m(m_{i_1}, m_{i_2}, \ldots, m_{i_k}).$$

Ejemplo 1.3.9. *Encuentra la expresión en suma de mintérminos de f.n.d. de la función booleana $f : B^3 \to B$, dada por $f(x, y, z) = x \cdot y + z$. Completamos la tabla en el cuadro 1.10 encontrada en el ejemplo 1.3.8.*

La notación con mintérminos es $f(x, y, z) = \sum{}_m(1, 3, 5, 6, 7).$

Cuadro 1.11: La tabla con coeficientes binarios de la función booleana $f(x, y, z) = x \cdot y + z$.

x	y	z	xy	$xy + z$	mintérminos	
0	0	0	0	0		
0	0	1	0	**1**	$\overline{x}\,\overline{y}z$	$001_2 = 1$
0	1	0	0	0		
0	1	1	0	**1**	$\overline{x}yz$	$011_2 = 3$
1	0	0	0	0		
1	0	1	0	**1**	$x\overline{y}z$	$101_2 = 5$
1	1	0	1	**1**	$xy\overline{z}$	$110_2 = 6$
1	1	1	1	**1**	xyz	$111_2 = 7$

La f.n.d. se puede encontrar analíticamente completando cada sumando que no sea una conjunción fundamental, es decir, multiplicando el sumando por la suma del literal que falta y su complemento.

Ejemplo 1.3.10. *Considera la función booleana* $f(x, y, z) = xy + \overline{x}z$.

$$f(x, y, z) = xy + \overline{x}z = xy(z + \overline{z}) + \overline{x}(y + \overline{y})z = xyz + xy\overline{z} + \overline{x}yz + \overline{x}\,\overline{y}z.$$

Función normal conjuntiva

Si un factor de la expresión es una desyunción de todas las variables, decimos que es una desyunción fundamental. En el ejemplo 1.3.7 el factor $w + x + y + \overline{z}$ es una desyunción fundamental.

Definición 1.3.6. *Sea* $f : B^n \to B$*, una función booleana. Decimos que* y *es una* **disyunción fundamental***, si* $y = y_1 + y_2 + \ldots + y_n$ *con* $y_i \in \{x_i, \overline{x_i}\}$*, para* $1 \leq i \leq n$.

Definición 1.3.7. *Sea* $f : B^n \to B$*, una función booleana. La* **función normal conjuntiva** (*f.n.c.*) *de la función* f *es una representación de* f *en producto (conjunción) de disyunciones (sumas) fundamentales.*

Para encontrar la *f.n.c.* de una función booleana $f : B^n \to B$, se evalúa la función en todas los cosos posibles, usando una tabla de verdad. Recordamos que $x_1 + x_2 + \ldots + x_n = 0$ si y solo si $x_1 = x_2 = \ldots = x_n = 0$, es decir, si el valor de la función f es 0, entonces al menos uno de sus disyunciones fundamentales es cero. Los disyunciones fundamentales cuyo valor es cero reciben es nombre de **maxtérminos**, es decir, una disyunción fundamental $y = y_1 + y_2 + \ldots + y_n$ es un maxtérmino si $y_i = x_i$ cuando $x_i = 0$ y $y_i = \overline{x_i}$ si $x_i = 1$ (nótese que es justo al reves que para los mintérminos). La expresión de *f.n.c.* es la conjunción de todos los maxtérminos.

Ejemplo 1.3.11. *Encuentra la f.n.c. de la función booleana* $f : B^3 \to B$*, dada por* $f(x, y, z) = x \cdot y + z$ *(del ejemplo 1.3.5). Construimos la tabla para encontrar los mintérminos de la función (ver cuadro 1.12).*

La f.n.c. es $f(x, y, z) = (x + y + z)(x + \overline{y} + z)(\overline{x} + y + z)$.

Cuadro 1.12: La tabla con maxtérminos de la función booleana $f(x, y, z) = x \cdot y + z$.

x	y	z	xy	$xy + z$	maxtérminos
0	0	0	0	**0**	$(x + y + z)$
0	0	1	0	1	
0	1	0	0	**0**	$(x + \overline{y} + z)$
0	1	1	0	1	
1	0	0	0	**0**	$(\overline{x} + y + z)$
1	0	1	0	1	
1	1	0	1	1	
1	1	1	1	1	

Igual que para la *f.n.d.*, vamos a definir una expresión simplificada de la *f.n.c.*. A cada maxtérmino $y = y_1 + y_2 + \ldots + y_n$, le asocia el número binario de n bits $x_1 x_2 \ldots x_n$. Es decir, si $y_i = x_i$, entonces $x_i = 0$ y si $y_i = \overline{x_i}$, entonces $x_i = 1$. Es importante resaltar que la asigación de ceros y unos para el caso de maxtérminos es justo al reves que para los mintérminos. En el ejemplo 1.3.11 el maxtérmino $(x + y + z)$ corresponde al caso $x = 0$, $y = 0$, $z = 0$ que representa el número binario 000_2, cuyo valor decimal es 0, como el valor decimal del maxtérmino $(x+y+z)$ es 0 lo denotamos por M_0. El maxtérmino $(\overline{x}+y+z)$ corresponde al caso $x = 1$, $y = 0$, $z = 0$ que representa el número binario 100_2, cuyo valor decimal es 4, como el valor decimal del maxtérmino $(\overline{x} + y + z)$ es 4 lo denotamos por M_4. Si $M_{i_1}, M_{i_2}, \ldots, M_{i_k}$ son todos los maxtérminos de la *f.n.c.*, podemos expresar la como un producto de los valores decimales asociados a cada maxtérmino:

$$f(x_1, x_2, \ldots, x_n) = \prod\nolimits_M (M_{i_1}, M_{i_2}, \ldots, M_{i_k}).$$

Ejemplo 1.3.12. *Encuentra la expresión en producto de maxtérminos de f.n.c. de la función booleana $f : B^3 \to B$, dada por $f(x, y, z) = x \cdot y + z$. Completamos la tabla en el cuadro 1.12 encontrada en el ejemplo 1.3.11.*

La notación con maxtérminos $\quad f(x, y, z) = \prod\nolimits_M (0, 2, 4)$.

Ejemplo 1.3.13. *Sea $g(w, x, y, z) = (w + x + y)(x + \overline{y} + z)(w + \overline{y})$.*
Construimos la tabla de verdad de la función $g(w, x, y, z)$ en el cuadro 1.15.
La f.n.d. de la función $g(w, x, y, z)$ es

$$g(w, x, y, z) = \overline{w}x\overline{y}\,\overline{z} + \overline{w}x\overline{y}z + w\overline{x}\,\overline{y}\,\overline{z} + w\overline{x}\,\overline{y}z + w\overline{x}yz + wx\overline{y}\,\overline{z} + wx\overline{y}z + wxy\overline{z} + wxyz.$$

La f.n.c. de la función $g(w, x, y, z)$ es

$$\begin{aligned} g(w, x, y, z) &= (w + x + y + z)(w + x + y + \overline{z})(w + x + \overline{y} + z)(w + x + \overline{y} + \overline{z}) \\ &= (w + \overline{x} + \overline{y} + z)(w + \overline{x} + \overline{y} + \overline{z})(\overline{w} + x + \overline{y} + z). \end{aligned}$$

Encontremos las expresiones en mintérminos y maxtérminos en el cuadro 1.15.

$$\begin{aligned} g(w, x, y, z) &= \sum\nolimits_m (4, 5, 8, 9, 11, 12, 13, 14, 15). \\ g(w, x, y, z) &= \prod\nolimits_M (0, 1, 2, 3, 6, 7, 10). \end{aligned}$$

Cuadro 1.13: La tabla de la función booleana $f(x, y, z) = x \cdot y + z$.

x	y	z	xy	$xy + z$	maxtérminos	
0	0	0	0	**0**	$(x + y + z)$	$000_2 = 0$
0	0	1	0	1		
0	1	0	0	**0**	$(x + \overline{y} + z)$	$010_2 = 2$
0	1	1	0	1		
1	0	0	0	**0**	$(\overline{x} + y + z)$	$100_2 = 4$
1	0	1	0	1		
1	1	0	1	1		
1	1	1	1	1		

1.3.2 Propiedades del Álgebra Booleana

Cuando definimos las operaciones booleanas revisamos un par de las propiedades de las operaciones. En el cuadro 1.16 están enlistadas todas las propiedades del álgebra booleana y su versión correspondiente en lógica de proposiciones y teoría de conjuntos. Algunas de las propiedades coinciden con propiedades de las operaciones entre números reales, como la propiedad conmutativa, mientras que otras propiedades no tienen sentido en los reales, como la propiedad de idempotencia. Revisa qué propiedades coinciden con las propiedades en el conjunto de los números reales y qué propiedades no tienen sentido en el conjunto de los números reales. En particular, en el ejercicio 1.44 preguntamos ¿qué diferencia notas en la propiedad de inverso?

1.3.3 Circuitos combinatorios

El álgebra booleana se puede aplicar a la teoría de circuitos eléctricos. Sean P y Q dos proposiciones. Si cada una de las proposiciones P y Q se asocia con un interruptor que está cerrado si la afirmación es verdadera y abierto si es falsa, entonces la proposición $P \wedge Q$ se representa en el circuito conectando los interruptores en serie. La corriente circulará por este circuito si y sólo si ambos interruptores están cerrados, esto es, si ambas P y Q son verdaderas. De la misma manera, otro circuito se puede usar para representar $P \vee Q$. En este caso los interruptores tienen que estar conectados en paralelo, con lo que la corriente circula si o P o Q o ambas son verdaderas (interruptores cerrados). Con otras palabras:

El foco L está prendido solamente si ambos interruptores A y B están cerrados: Si $A = 1$ y $B = 1$, entonces $L = 1$.

$$L = A \vee B \text{ o } L = A \cdot B$$

En la figura 1.3.3 se puede ver el circuito combinatorio asociado a $A \cdot B$.

Cuadro 1.14: La tabla de la función booleana $g(w,x,y,z) = (w+x+y)(x+\overline{y}+z)(w+\overline{y})$.

w	x	y	z	$(w+x+y)$	$(x+\overline{y}+z)$	$(w+\overline{y})$	g	mintérminos	maxtérminos
0	0	0	0	0	1	1	**0**		$(w+x+y+z)$
0	0	0	1	0	1	1	**0**		$(w+x+y+\overline{z})$
0	0	1	0	1	0	0	**0**		$(w+x+\overline{y}+z)$
0	0	1	1	1	1	0	**0**		$(w+x+\overline{y}+\overline{z})$
0	1	0	0	1	1	1	1	$\overline{w}x\overline{y}\,\overline{z}$	
0	1	0	1	1	1	1	1	$\overline{w}x\overline{y}z$	
0	1	1	0	1	1	0	**0**		$(w+\overline{x}+\overline{y}+z)$
0	1	1	1	1	1	0	**0**		$(w+\overline{x}+\overline{y}+\overline{z})$
1	0	0	0	1	1	1	1	$w\overline{x}\,\overline{y}\,\overline{z}$	
1	0	0	1	1	1	1	1	$w\overline{x}\,\overline{y}z$	
1	0	1	0	1	0	1	**0**		$(\overline{w}+x+\overline{y}+z)$
1	0	1	1	1	1	1	1	$w\overline{x}yz$	
1	1	0	0	1	1	1	1	$wx\overline{y}\,\overline{z}$	
1	1	0	1	1	1	1	1	$wx\overline{y}z$	
1	1	1	0	1	1	1	1	$wxy\overline{z}$	
1	1	1	1	1	1	1	1	$wxyz$	

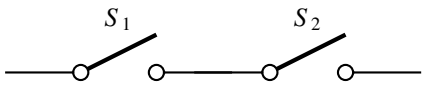


Figura 1.6: El circuito combinatorio $A \cdot B$.

El foco L está prendido si al menos una de los interruptores A, B están cerrados: Si $A = 1$ o $B = 1$, entonces $L = 1$.

$$L = A \wedge B \text{ o } L = A + B$$

En la figura 1.3.3 se puede ver el circuito combinatorio asociado a $A + B$.

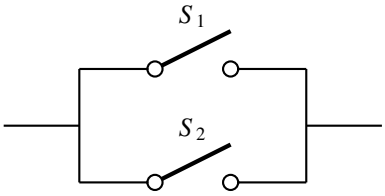


Figura 1.7: El circuito combinatorio $A + B$.

Ejemplo 1.3.14. *Considera el ejemplo $f : B^3 \to B$, dada por $f(x,y,z) = x \cdot y + z$ (del ejemplo 1.3.5).*

Cuadro 1.15: La tabla de coeficientes binarios de la función booleana $g(w, x, y, z)$.

mintérminos		maxtérminos	
		$(w + x + y + z)$	$0000_2 = 0$
		$(w + x + y + \overline{z})$	$0001_2 = 1$
		$(w + x + \overline{y} + z)$	$0010_2 = 2$
		$(w + x + \overline{y} + \overline{z})$	$0011_2 = 3$
$\overline{w}x\overline{y}\,\overline{z}$	$0100_2 = 4$		
$\overline{w}x\overline{y}z$	$0101_2 = 5$		
		$(w + \overline{x} + \overline{y} + z)$	$0110_2 = 6$
		$(w + \overline{x} + \overline{y} + \overline{z})$	$0111_2 = 7$
$w\overline{x}\,\overline{y}\,\overline{z}$	$1000_2 = 8$		
$w\overline{x}\,\overline{y}z$	$1001_2 = 9$		
		$(\overline{w} + x + \overline{y} + z)$	$1010_2 = 10$
$w\overline{x}yz$	$1011_2 = 11$		
$wx\overline{y}\,\overline{z}$	$1100_2 = 12$		
$wx\overline{y}z$	$1101_2 = 13$		
$wxy\overline{z}$	$1110_2 = 14$		
$wxyz$	$1111_2 = 15$		

Prendido: Si $x \cdot y + z = 1$*, entonces* $xy = 1$ *o* $z = 1$*, entonces*

$$(x = y = 1) \wedge (z = 1) =$$
$$((x, y, \overline{z} = 1) \wedge (x, y, z = 1)) \wedge ((x, \overline{y}, z = 1) \wedge (\overline{x}, y, z = 1) \wedge (\overline{x}, \overline{y}, z = 1)) =$$
$$(x, y, \overline{z} = 1) \wedge (x, y, z = 1) \wedge (x, \overline{y}, z = 1) \wedge (\overline{x}, y, z = 1) \wedge (\overline{x}, \overline{y}, z = 1)$$

Apagado: Si $x \cdot y + z = 0$*, entonces* $xy = 0$ *y* $z = 0$*, entonces*

$$(x = 0 \wedge y = 0) \vee (z = 0) =$$
$$((x = y = 0) \wedge (x = 0 \wedge y = 0)) \vee (z = 0) =$$
$$((x = y = 0) \wedge (x = \overline{y} = 0) \wedge (\overline{x} = y = 0)) \vee (z = 0) =$$
$$(x, y, z = 0) \wedge (x, \overline{y}, z = 0) \wedge (\overline{x}, y, z = 0)$$

Ejemplo 1.3.15. *Diseña un alarma que suene cuando: Alguna ventana o alguna puerta se abre y el sistema esté habilitado.*

En forma lógica se expresaría:

La alarma suena $A = 1$
Las dos venta V_1 *o* V_2
Las dos puertas P_1 *o* P_2
Se habra una ventana / puerta $V_i = 1$, $P_i = 1$
El sistema está habilitado $S = 1$

Cuadro 1.16: Tabla de propiedades del Álgebra Booleano

Propiedad	Variables booleanas	Lógica matemática	Conjuntos
	$\overline{\overline{x}} = x$	$\neg(\neg P) = P$	$\overline{\overline{A}} = A$
Leyes de Morgan	$\overline{x+y} = \overline{x} \cdot \overline{y}$	$\neg(P \wedge Q) = (\neg P) \vee (\neg Q)$	$\overline{A \cup B} = \overline{A} \cap \overline{B}$
	$\overline{x \cdot y} = \overline{x} + \overline{y}$	$\neg(P \vee Q) = (\neg P) \wedge (\neg Q)$	$\overline{A \cap B} = \overline{A} \cup \overline{B}$
Conmutativa	$x + y = y + x$	$P \wedge Q = Q \wedge P$	$A \cup B = B \cup A$
	$x \cdot y = y \cdot x$	$P \vee Q = Q \vee P$	$A \cap B = B \cap A$
Asociativa	$x + (y + z) = (x + y) + z$	$P \wedge (Q \wedge R) = (P \wedge Q) \wedge R$	$A \cup (B \cup C) = (A \cup B) \cup C$
	$x \cdot (y \cdot z) = (x \cdot y) \cdot z$	$P \vee (Q \vee R) = (P \vee Q) \vee R$	$A \cap (B \cap C) = (A \cap B) \cap C$
Distribuitiva	$x \cdot (y + z) =$ $(x \cdot y) + (x \cdot z)$	$P \vee (Q \wedge R) =$ $(P \vee Q) \wedge (P \vee R)$	$A \cap (B \cup C) =$ $(A \cap B) \cup (A \cap C)$
Idempotencia	$x + x = x$	$P \wedge P = P$	$A \cup A = A$
	$x \cdot x = x$	$P \vee P = P$	$A \cap A = A$
Identidad	$x + 0 = x$	$P \wedge \mathcal{F} = P$	$A \cup \emptyset = A$
	$x \cdot \mathbf{1} = x$	$P \vee \mathcal{V} = P$	$A \cap \mathcal{U} = A$
Inverso	$x + \overline{x} = \mathbf{1}$	$P \wedge (\neg P) = \mathcal{V}$	$A \cup \overline{A} = \mathcal{U}$
	$x \cdot \overline{x} = \mathbf{0}$	$P \vee (\neg P) = \mathcal{F}$	$A \cap \overline{A} = \emptyset$
Dominación	$x + \mathbf{1} = \mathbf{1}$	$P \wedge \mathcal{V} = \mathcal{V}$	$A \cup \mathcal{U} = \mathcal{U}$
	$x \cdot \mathbf{0} = \mathbf{0}$	$P \vee \mathcal{F} = \mathcal{F}$	$A \cap \emptyset = \emptyset$
Absorción	$x + x \cdot y = x$	$P \wedge (P \vee Q) = P$	$A \cup (A \cap B) = A$
	$x \cdot (x + y) = x$	$P \vee (P \wedge Q) = A$	$A \cap (A \cup B) = A$

Solución:

$$\begin{aligned} A &= ((V_1 \wedge V_2) \wedge (P_1 \wedge P_2)) \vee S \qquad \textit{(notación lógica)} \\ A &= ((V_1 + V_2) + (P_1 + P_2)) \cdot S \qquad \textit{(notación funciones).} \end{aligned}$$

1.3.4 Aplicaciones de algebra booleana a la teoría de las gráficas

En la teoría de las gráficas el álgebra booleana se puede aplicar cuando nos interesa si hay o no hay caminos de cierta longitud (o circuitos de cierta longitud). Por ejemplo, si queremos determinar si hay un camino o no de longitud k (y no nos interesa el número de caminos de longitud k) podemos trabajar la matiz de adyacencias con entradas booleanas, así la entrada a_{ij} de la tercera potencia de la matriz de adyacencias, indica si hay algún camino de longitud 3 entre el vértice i y el vértice j.

1.3.5 Ejercicios

Ejercicio 1.36. *Evaluar las siguientes funciones booleanas en $x = 1, y = 0, z = 0, w = 1$.*
i) $(x, y, z, w) = x\overline{y} + \overline{xy}$. *ii)* $f(x, y, z, w) = xw + \overline{y} + yz$.

Ejercicio 1.37. *¿Es posible determinar el valor de la siguiente función booleana para $x = 1$ y $y, w \in B$. En caso negativa ¿Cuántos casos hay?*
i) $x + xy + w$, *ii)* $xy + w$, *iii)* $\overline{x}y + xw$.

Ejercicio 1.38. *Simplifica las siguientes expresiones booleanas*
i) $xy + (x + y)\overline{z} + y$. *ii)* $x + y + (\overline{\overline{x} + y + z})$.

Ejercicio 1.39. *Sea* $f : B^4 \to B$. *¿Cuántos renglones tiene la tabla de la función booleana* f*?*

Ejercicio 1.40. *Determinar la función normal conjuntiva y la función normal disyuntiva de las siguientes funciones booleanas.*

i. *Sea* $f : B^3 \to B$, *definida por* $f(x, y, z) = \overline{\overline{(x + y)} + (\overline{x}z)}$.

ii. *Sea* $f : B^4 \to B$, *definida por* $f(w, x, y, z) = (wz + \overline{x}yz)(x + \overline{x}\,\overline{y}z)$.

Ejercicio 1.41. *Usando tabla de verdad para verificar que la f.n.c. de* $f(x, y, z) = xyz + xy\overline{z}) + \overline{x}yz + \overline{x}\,\overline{y}z$.

Ejercicio 1.42. *Sea* $f : B^n \to B$. *Sea* $f(b_1, b_2, \ldots, b_n) = \sum_m(i_1, i_2, \ldots, i_k)$ *y sea* $J = \mathbb{Z}_n \setminus \{i_1, i_2, \ldots, i_k\}$. *Entonces* $f(b_1, b_2, \ldots, b_n) = \prod_M(J)$.

Ejercicio 1.43. *Usando el ejercicio anterior determina la f.n.d. de* $f(x, y, z) = (x + y + z)(x + \overline{y} + z)(\overline{x} + \overline{y} + z)$.

Ejercicio 1.44. *Para cada uno de las propiedades de la tabla 1.16, determina si coincide con una propiedad en el conjunto de los números reales. Si la propiedad no tienen sentido en el conjunto de los números reales, proporciona un contraejemplo. En particular, ¿qué diferencia notas en la propiedad del inverso?*

Ejercicio 1.45. *Compruebe que los dos circuitos combinatorios en la figura 1.45 son equivaler*

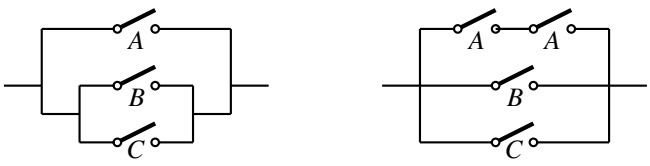


Figura 1.8: Los circuitos combinatorios del ejercicio 1.45.

Ejercicio 1.46. *Encuentra la función booleana de los circuitos de cada una de las figuras 1.46, simplifícala y encuentra el circuito combinatorio de la función simplificada.*

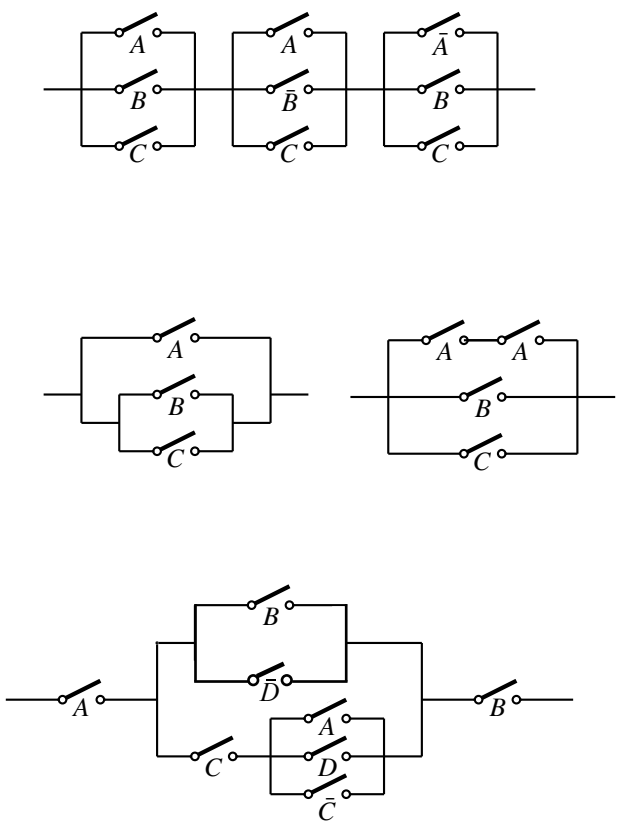


Figura 1.9: Los circuitos combinatorios del ejercicio 1.46.

1.4 Proyectos

El sistema criptográfico de llave público RSA.

Uno de los sistemas de criptografía que han tenido mas importancia es el sistema criptográf de llave público RSA. Realiza una breve revisión histórica de la criptografía y explica el funcionamiento del sistema criptográfico de llave público RSA. Para mayo información ver sección 5.4 en [11].

Criptografía. Códigos de barra.

Los códigos de barras aparecen en mucho áreas de la vida cotidiana. Explicar como funciona el sistema de códigos de barra.

Condiciones de indiferencia - Dominación en gráficas.

Investiga y explicar la relación entre el concepto de dominación en Teoría de las Gráficas y el Álgebra Booleano. Explica al menos dos ejemplos que ilustra esta relación. Para mayor información ver sección 15.3 en [9].

Circuitos electrónicos

Investiga y explicar la relación entre el Álgebra Booleano y los circuitos electrónicos. Explica al menos dos ejemplos y su aplicación a otras áreas de conocimientos. Para mayor información ver sección en [11].

2 Anillos de Polinomios

En este capítulo vamos a revisar las propiedades del conjunto de polinomios con coeficientes en un anillo $(\mathbf{A}, +, \cdot)$. Cuando el anillo es un campo, definimos la divisiíon de polinomios y trazamos analogías entre tal anillo de polinomios y el anilllo de los números enteros $\mathbb{Z}$. Al final nos enfocamos en el anillo de polinomios con coeficientes en el conjunto $\mathbb{R}$ y en $\mathbb{Z}$.

Vamos a considerar únicamente polinomios con una variable. Un polinomio es una expresión algebraica que consta de suma finita donde cada sumando consta de un coeficiente (una constante) multiplicado por la variable elevado a una potencia no negativa. Los coeficientes pueden ser números enteros, naturales, racionales o reales según lo que representa el polinomio

Ejemplo 2.0.1. *Ejemplos polinomios*

1. $P(x) = 2x^2 + 3x - 1$ *es un polinomio con variable x;* 2 *es el coeficiente de* x^2*;* 3 *es el coeficiente de x y el coeficiente de* x^0 *es* -1.
2. $P(x) = \frac{1}{2}x^3 - \frac{7}{8}x + 4$ *es un polinomio con variable x;* $1/2$ *es coeficiente de* x^3*;* 0 *es coeficiente de* x^2*;* $7/8$ *es coeficiente de x y el coeficiente de* x^0 *es* 4.
3. $P(x) = \frac{1}{4}x^5 + \pi x^3 - 0.8x - 1$ *es un polinomio con variable x;* $1/4$ *es coeficiente de* x^5*;* 0 *es coeficiente de* x^4*,* x^2*;* π *es coeficiente de* x^3*,* 0.8 *es coeficiente de x y el coeficiente de* x^0 *es* -1.

Vamos a estudiar los polinomios cuyos coeficientes pertenecen a un mismo anillo, $(\mathbf{A}, +, \cdot)$. Para simplificar la notación, diremos simplemente que $\mathbf{A}$ es un anillo. En el ejemplo 2.0.1 en el inciso 1. los coeficientes del pertenecen al anillo $\mathbb{Z}$; en el inciso 2. los coeficientes del pertenecen al anillo $\mathbb{Z}$ y en el inciso 3. los coeficientes del pertenecen al anillo $\mathbb{R}$.

Definición 2.0.1. *Un* **polinomio** *con coeficientes en el anillo* $\mathbf{A}$ *es una expresión algebraica*

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0, \text{ con } a_i \in \mathbf{A}, \text{ para } 0 \leq i \leq n.$$

Sea $\mathbf{z}$ el neutro aditivo del anillo $\mathbf{A}$; si n es el máximo entero tal que $a_n \neq \mathbf{z}$, decimos que el polinomio tiene **grado** n. El **polinomio nulo** es el polinomio cuyos coeficientes $a_i = \mathbf{z}$ para todo entero $i \geq 0$, por lo que es polinomio nulo no tiene grado. En el anillo de los números reales el polinomio nulo es $p(x) = 0$. El coeficiente a_0 es el **término constante**. En el ejemplo 2.0.1 en el inciso 1. el grado del polinomio es 2 y el término constante es -1; en el inciso 2. el grado del polinomio es 3 y el término constante es 4 y en el inciso 3. el grado del polinomio es 5 y el término constante es -1.

Los polinomio son una herramienta importante en la solución de problemas en muchas áreas del conocimiento. El siguiente ejemplo sencillo ilustra un ejemplo su uso.

Ejemplo 2.0.2. *Queremos encontrar la base del sistema numérico en donde el número decimal* 3027 *tiene representación* 5723.

Para resolver el problema tenemos que encontrar una solución positiva para la ecuación $5x^3 + 7x^2 + 2x + 3 = 3027$. *Al simplificar, obtenemos* $5x^3 + 7x^2 + 2x - 3024$, *es decir, tenemos que encontrar una solución donde el siguiente polinomio tenga el valor de* 0.

$$P(x) = 5x^3 + 7x^2 + 2x - 3024.$$

2.1 Anillo de polinomios

Sea $\mathbf{A}[x]$ el conjunto de todos los polinomios con coeficientes en $\mathbf{A}$. Vamos a probar que $\mathbf{A}[x]$ forma un anillo llamado el anillo de polinomio con coeficientes en $\mathbf{A}$ y determinar qué propiedades del anillo $\mathbf{A}$ se heredan al anillo $\mathbf{A}[x]$.

Ejemplo 2.1.1. $\mathbb{R}[x]$ *es el conjunto de todos los polinomios con coeficientes reales.*
$\mathbb{Q}[x]$ *es el conjunto de todos los polinomios con coeficientes racionales.*
$\mathbb{Z}[x]$ *es el conjunto de todos los polinomios con coeficientes enteras.*
$\mathbb{Z}_n[x]$ *es el conjunto de todos los polinomios con coeficientes en* $\mathbb{Z}_n$.
$n\mathbb{Z}[x]$ *es el conjunto de los polinomios cuyos coeficientes son multiplos de n.*

Definición 2.1.1. *Sea* $(\mathbf{A}, +, \cdot)$ *un anillo y* $P(x), Q(x) \in \mathbf{A}[x]$, *con*

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0, \qquad Q(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0.$$

Decimos que $P(x) = Q(x)$ *si* $m = n$ *y* $a_i = b_i$ *para todo* $0 \leq i \leq n$.

Ejemplo 2.1.2. *Sean* $P(x), Q(x) \in \mathbb{R}[x]$ *con* $P(x) = \frac{1}{2}x^2 - 0.8x + 2$ *y* $Q(x) = 0.5x^2 - \frac{4}{5}x + 2$. *Claramente* $P(x) = Q(x)$.

Ejemplo 2.1.3. *Sea* $\mathbf{A} = \mathbb{Z}_6$ *con las operaciones usuales de* $\mathbb{Z}_6$. *Sea* $P(x) \in \mathbb{Z}_6[x]$ *definida por* $P(x) = 3x^2 - x + 2$. *Como* $[-1] = [5]$ *en* $\mathbb{Z}_6$, *entonces* $P(x) = 3x^2 + 5x + 2$.

Primero definimos las operaciones de suma y producto entre polinomios en el conjunto $\mathbf{A}[x]$, donde $(\mathbf{A}, +, \cdot)$ es un anillo. Sean $P(x),\ Q(x) \in \mathbf{A}[x]$, con $n \geq m \geq l$, y

$$\begin{aligned} P(x) &= a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0, \\ Q(x) &= b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0. \end{aligned}$$

Suma de polinomios

$$P(x) + Q(x) = (a_n + b_n)x^n + (a_{n-1}b_{n-1})x^{n-1} + \ldots + (a_1 + b_1)x + (a_0 + b_0),$$

donde $b_j = 0$, para $m < j \leq n$ y la suma $a_i + b_i$ es la suma definida en el anillo $(\mathbf{A}, +, \cdot)$. Como $a_i, b_i \in \mathbf{A}$ y $\mathbf{A}$ es un anillo, entonces $a_i + b_i \in \mathbf{A}$ y el conjunto $\mathbf{A}[x]$ es cerrado bajo la suma de polinomios.

Ejemplo 2.1.4. *Considera los polinomios* $p(x) = 2x^2 - 4x + 7$ *y* $q(x) = x^3 + 4x - 5$*, con* $p(x), q(x) \in \mathbb{Z}[x]$*,*

$$p(x) + q(x) = x^3 + 2x^2 + 2.$$

Producto de polinomios

$$P(x) \cdot Q(x) = \sum_{i+j=0}^{n+m} a_i b_j x^{i+j}.$$

El coeficiente de x^k es $\sum_{i+j=k} a_i b_j x^k$. Como $a_i, b_j \in \mathbf{A}$ y $\mathbf{A}$ es un anillo, entonces $a_i b_i \in \mathbf{A}$ y el conjunto $\mathbf{A}[x]$ es cerrado bajo el producto de polinomios.

Ejemplo 2.1.5. *Considera los polinomios* $p(x) = 2x^2-4x+7$ *y* $q(x) = 4x-5$*, con* $p(x), q(x) \in \mathbb{Z}[x]$*,*

$$\begin{aligned} p(x) \cdot q(x) &= (-5 \cdot 7) + (7 \cdot 4 - 4 \cdot (-5))x^1 + (-5 \cdot 2 - 4 \cdot 4)x^2 + (2 \cdot 4)x^3 \\ &= -35 + 48x - 26x^2 + 8x^3 = 8x^3 - 26x^2 + 48x - 35. \end{aligned}$$

*Cuando alguno de los dos polinomio tiene pocos sumandos, el producto se puede hacer "*a pié*".*

$$\begin{aligned} q(x) \cdot p(x) &= (4x - 5)(2x^2 - 4x + 7) \\ &= 4x(2x^2 - 4x + 7) - 5(2x^2 - 4x + 7) \\ &= 8x^3 - 16x^2 + 28x - (10x^2 - 20x + 35) \\ &= 8x^3 - 26x^2 + 48x - 35. \end{aligned}$$

En las operaciones de suma y producto entre dos polinomios, las operaciones entre coeficientes son las del anillo correspondiente. Es decir, si los polinomios pertenecen a $n\mathbb{Z}[x]$, entonces las operaciones entre los coeficientes son las operaciones en $n\mathbb{Z}$ mientras que si los polinomios pertenecen a $\mathbb{Z}$, las operaciones entre los coeficientes son las operaciones en $\mathbb{Z}$ que son las mismas que en $\mathbb{R}$.

Ejemplo 2.1.6. *Considera los polinomios* $p(x) = 5x^2 + 3x + 2$ *y* $q(x) = x^2 + x + 5$*, con* $p(x), q(x) \in \mathbb{Z}_6$*. Las operaciones entre los coeficientes de los polinomios son las operaciones en* $\mathbb{Z}_6$*.*

$$p(x) + q(x) = (5 + 1)x^2 + (3 + 1)x^1 + (2 + 5) = 4x + 1.$$

Ejemplo 2.1.7. *Considera los polinomios* $p(x) = 3x+5$ *y* $q(x) = 2x^2+3$*, con* $p(x), q(x) \in \mathbb{Z}_6$*. Las operaciones entre los coeficientes de los polinomios son las operaciones en* $\mathbb{Z}_6$*.*

$$p(x) \cdot q(x) = (5 \cdot 3) + (5 \cdot 2 + 3 \cdot 3)x^1 + (3 \cdot 2)x^2 = 3 + (4 + 3)x^2 + 0x^2 = 3 + x^2.$$

Vamos a probar el siguiente teorema.

Teorema 2.1.2. *Sea* $(\mathbf{A}, +, \cdot)$ *un anillo. Entonces* $\mathbf{A}[x]$ *es un anillo con las operaciones definidas entre polinomios (llamado el anillo de polinomios con coeficientes en* $\mathbf{A}$*). Las operaciones entre los coeficientes son las operaciones del anillo* $\mathbf{A}[x]$*.*

Para probar que $(\mathbf{A}[x]; +, \cdot)$ es un anillo, tenemos que probar que satisface todas los axiomas de anillo.

Sean $P(x),\ Q(x),\ R(x) \in \mathbf{A}[x]$

A.1 La suma de dos polinomios conmuta

$$P(x) + Q(x) = (a_n + b_n)x^n + (a_{n-1}b_{n-1})x^{n-1} + \ldots + (a_1 + b_1)x + (a_0 + b_0),$$

como $a_i, b_i \in \mathbf{A}$ y $\mathbf{A}$ es un anillo, entonces $a_i + b_i = b_i + a_i$ y

$$\begin{aligned} P(x) + Q(x) &= (b_n + a_n)x^n + (b_{n-1}a_{n-1})x^{n-1} + \ldots + (b_1 + a_1)x + (b_0 + a_0) \\ &= Q(x) + P(x). \end{aligned}$$

A.2 La suma de dos polinomios es asociativa

$$\begin{aligned} (P(x) + Q(x)) + R(x) &= ((a_n + b_n)x^n + (a_{n-1}b_{n-1})x^{n-1} + \ldots + (a_1 + b_1)x + (a_0 + b_0)) + R(x) \\ &= ((a_n + b_n) + c_n)x^n + ((a_{n-1} + b_{n-1}) + c_{n-1})x^{n-1} + \ldots + ((a_1 + b_1) + c_1) \\ &\quad ((a_0 + b_0) + c_0), \end{aligned}$$

como $a_i, b_i \in \mathbf{A}$ y $\mathbf{A}$ es un anillo, entonces $(a_i + b_i) + c_i = a_i + (b_i + c_i)$ y

$$\begin{aligned} (P(x) + Q(x)) + R(x) &= (a_n + (b_n + c_n))x^n + (a_{n-1} + (b_{n-1} + c_{n-1}))x^{n-1} + \ldots + (a_1 + (b_1 + c_1))x + \\ &\quad (a_0 + (b_0 + c_0)) \\ &= P(x) + (Q(x) + R(x)). \end{aligned}$$

A.3 Existe un polinomio que es neutro aditivo. Sea $\mathbf{0}$ el neutro aditivo del anillo $(\mathbf{A}, +, \cdot)$. Entonces $\mathbf{Z}(x) = \mathbf{0}$ es el neutro aditivo de los polinomio en el conjunto $\mathbf{A}\,[x]$.

$$\begin{aligned} P(x) + \mathbf{Z}(x) &= (a_n + \mathbf{0})x^n + (a_{n-1} + \mathbf{0})x^{n-1} + \ldots + (a_1 + \mathbf{0})x + (a_0 + \mathbf{0}) \\ &= a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \\ &= P(x). \end{aligned}$$

A.4 Dado un polinomio $P(x)$ existe un polinomio que es inverso aditivo.

Sea $(-\mathbf{a}_i)$ el inverso aditivo de a_i en el anillo $(\mathbf{A}, +, \cdot)$. Por propiedades del anillo $(\mathbf{A}, +, \cdot)$, $a_i + (-\mathbf{a}_i) = \mathbf{0}$ para cada $0 \leq i \leq n$, y

$$(-\boldsymbol{P}(x)) = (-\boldsymbol{a}_n)x^n + (-\boldsymbol{a}_{n-1})x^{n-1} + \ldots + (-\boldsymbol{a}_1)x + (-\boldsymbol{a}_0)$$

es el inverso aditivo de $P(x)$ en el conjunto $\mathbf{A}\,[x]$.

$$\begin{aligned} P(x) + (-\boldsymbol{P}(x)) &= (a_n + (-\mathbf{a}_n))x^n + (a_{n-1} + (-\mathbf{a}_{n-1}))x^{n-1} + \ldots + (a_1 + (-\mathbf{a}_1))x + (a_0 + (-\mathbf{a}_0)) \\ &= \mathbf{0}x^n + \mathbf{0}x^{n-1} + \cdots + \mathbf{0}x + \mathbf{0} \\ &= \mathbf{Z}(x). \end{aligned}$$

M.2 El producto de dos polinomios es asociativa

$$\begin{aligned} P(x) \cdot Q(x) \cdot R(x) &= (\sum_{i+j=0}^{n+m} a_i b_j x^{i+j}) \cdot R(x) = \sum_{(i+j)+k=0}^{(n+m)+l} ((a_i b_j)c_k)x^{(i+j)+k} \\ &= \sum_{i+(j+k)=0}^{n+(m+l)} (a_i(b_j c_k))x^{i+(j+k)} = P(x) \cdot (\sum_{j+k=0}^{m+l} b_j c_k x^{j+k}) \\ &= P(x) \cdot (Q(x) \cdot P(x)). \end{aligned}$$

D El producto se distribuye sobre la suma

$$\begin{aligned} P(x)\cdot(Q(x)+R(x)) &= P(x)\cdot((b_n+c_n)x^n+(b_{n-1}+c_{n-1})x^{n-1}+\ldots+(b_1+c_1)x+(b_0+c_0)) \\ &= \sum_{i+j=0}^{n+m} a_i(b_j+c_j)x^{i+j} = \sum_{i+j=0}^{n+m}(a_ib_j+a_ic_j)x^{i+j} = \sum_{i+j=0}^{n+m}(a_ib_jx^{i+j}+a_ic_jx^{i+j}) \\ &= \sum_{i+j=0}^{n+m} a_ib_jx^{i+j} + \sum_{i+j=0}^{n+m} a_ic_jx^{i+j} \\ &= P(x)\cdot Q(x)+P(x)\cdot R(x). \end{aligned}$$

Hemos probado el siguiente resultado:

Corolario 2.1.3. *Sea* $(\mathbf{A},+,\cdot)$ *un anillo conmutativo (con unidad respectivamente). Entonces* $\mathbf{A}[x]$ *es un anillo conmutativo (con unidad respectivamente).*

Demostración. Sea $(\mathbf{A},+,\cdot)$ un anillo conmutativo. Entonces el producto de dos polinomios conmuta:

$$P(x)\cdot Q(x) = \sum_{i+j=0}^{n+m} a_ib_jx^{i+j} = \sum_{j+i=0}^{m+n} b_ja_ix^{j+i} = Q(x)\cdot P(x).$$

Sea $(\mathbf{A},+,\cdot)$ un anillo con unidad. Entonces existe un polinomio que es neutro multiplicativo. Sea $\mathbf{u}$ el neutro multiplicativo del anillo $(\mathbf{A},+,\cdot)$. Entonces $\mathbf{U}(x)=\mathbf{u}$ es el neutro multiplicativo de los polinomio en el conjunto $\mathbf{A}\,[x]$:

$$P(x)\cdot \boldsymbol{U}(x) = \sum_{j=0,i+j=0}^{n+0} a_i\mathbf{u}(x^{i+j}) = \sum_{i=0}^{n} a_ix^i = P(x).$$

□

Ejemplo 2.1.8. *Sean* $f,g\in\mathbb{Z}_8$, *con* $f(x)=4x^2+1$, *y* $g(x)=2x+3$. *Entonces* $fg(x)=(4x^2+1)(2x+3)=8x^3+12x^2+2x+3$. *Como* $[8]=[0]$ *y* $[12]=[4]$ *en* $\mathbb{Z}_8$, *entonces* $fg(x)=4x^2+2x+3$.

En el ejemplo anterior el grado del producto de dos polinomios resultó menor que la suma de los grados de los dos polinomios, lo cual no puede suceder si el anillo de los coeficientes es el anillo $\mathbb{R}$. En el siguiente teorema caracterizamos los anillos que satisfacen que su anillo de polinomios se cumple que $gr(fg)=gr(f)+gr(g)$. Es importante recordar que $\mathbb{Z}_8$ no es un dominio entero.

Teorema 2.1.4. *Sea* $(\mathbf{A},+,\cdot)$ *un anillo conmutativo con unidad. Entonces* $\mathbf{A}$ *es un dominio entero si y solo si para todo* $f,g\in\mathbf{A}[x]$ *no nulos se tiene que*

$$gr(fg)=gr(f)+gr(g).$$

Demostración. Sea $\mathbf{A}$ un dominio entero y sean $f,g\in\mathbf{A}[x]$ dos polinomios de grado n y m respectivamente. Sean

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0,$$

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0.$$

Como $gr(f) = n$ y $gr(g) = m$, entonces $a_n, b_m \neq 0$, y como $\mathbf{A}$ un dominio entero, entonces $a_n \cdot b_m \neq 0$. Ahora $fg = \sum_{i+j=0}^{n+m} a_i b_j x^{i+j}$, como $a_n \cdot b_m \neq 0$, entonces

$$gr(fg) = n + m = gr(f) + gr(g).$$

Supongamos que para todo $f, g \in \mathbf{A}[x]$ no nulos, se tiene que $gr(fg) = gr(f) + gr(g)$. Para llegar a una contradicción, supongamos que $\mathbf{A}$ no es un dominio entero. En este caso existen $a, b \in \mathbf{A}$ tales que $a, b \neq 0$ y $ab = 0$. Sean $f, g \in \mathbf{A}[x]$, con $f(x) = ax + a_0$, $g(x) = bx + b_0$, entonces $fg = abx^2 + (ab_0 + ba_0)x + a_0b_0 = (ab_0 + ba_0)x + a_0b_0$. Por lo que $gr(fg) < gr(f) + gr(g)$, lo cual contradice la hipótesis que $gr(fg) = gr(f) + gr(g)$ para todo $f, g \in \mathbf{A}[x]$ no nulos. Por lo tanto $\mathbf{A}[x]$ sí es un dominio entero. □

Definición 2.1.5. *Sea $(\mathbf{A}, +, \cdot)$ un anillo con unidad u y $f \in \mathbf{A}[x]$ con $gr(f) \geq 1$. Si $r \in \mathbf{A}$ y $f(r) = 0$, decimos que r es una* **raíz del polinomio** *$f(x)$.*

Ejemplo 2.1.9. *Encuentra las raíces del polinomio $f(x) = x^2 - 2$ para $f(x) \in \mathbb{R}[x]$.*

$$f(x) = 0 \Leftrightarrow x^2 - 2 = 0 \Leftrightarrow x^2 = 2 \Leftrightarrow |x| = \sqrt{2} \Leftrightarrow x = \mp\sqrt{2}.$$

Se sigue que $f(x) = (x - \sqrt{2})(x + \sqrt{2})$ ya que $f(x) \in \mathbb{R}[x]$. Nótese que si $f(x) = x^2 - 2$ y $f(x) \in \mathbb{Z}[x]$ o $f(x) \in \mathbb{Q}[x]$, entonces $f(x)$ no tendría raíces.

Ejemplo 2.1.10. *Encuentra las raíces del polinomio $f(x) = x^2 + 3x + 2$ para $f(x) \in \mathbb{Z}_6[x]$. Como $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, sólo tenemos seis posibles valores para x y podemos evaluamos el polinomio $f(x)$ en cada uno de los seis posibles valores*

$$\begin{array}{lll} f(0) = 2, & f(1) = 1 + 3 + 2 = 0, & f(2) = 4 + 0 + 2 = 0, \\ f(3) = 3 + 3 + 2 = 2\,, & f(4) = 4 + 0 + 2 = 0, & f(5) = 1 + 3 + 2 = 0. \end{array}$$

Las raíces del polinomio $f(x)$ son $1, 2, 4, 5$.

Nótese que en el ejemplo 2.1.10, el polinomio $f(x)$ tiene 4 raíces y es de grado 2. En la educación media-superior nos ense¿an que un polinomio de grado n cuyos coeficientes son números reales, tiene a lo mas n raíces. En las siguientes secciones vamos a caracterizar los anillos $\mathbf{A}$ que satisfacen que cualquier polinomio $f(x) \in \mathbf{A}[x]$ tenga a los más tantos raíces como su grado.

2.1.1 Algoritmo de la División para Polinomio

Dado un campo $\mathbf{K}$, la división en $\mathbf{K}[x]$ es análogo a la división en $\mathbb{Z}$. Los polinomios irreducibles en $\mathbf{K}[x]$ juegan el papel $\mathbf{K}[x]$ que los de primos en $\mathbb{Z}$. En particular, si r es una raíz del polinomio $p(x) \in \mathbf{K}[x]$, entonces $x - r$ juega el mismo papel en de un número primo en $\mathbb{Z}$.

Definición 2.1.6. *Sea $\mathbf{K}$ un campo, sean $f(x), g(x) \in \mathbf{K}[x]$ donde $g(x)$ no es el polinomio nulo. Decimos que $g(x)$ es* **divisor** *de $f(x)$ si existe un polinomio $h(x) \in \mathbf{K}[x]$ tal que $g(x) = f(x)h(x)$.*

Teorema 2.1.7 (Algoritmo de la división)**.** *Sea* $\mathbf{K}$ *un campo y* $f(x), g(x) \in \mathbf{K}[x]$*, con* $gr(g(x)) = n \geq 1$*. Entonces existen dos polinomios* $q(x), r(x) \in \mathbf{K}[x]$ *tales que*

$$f(x) = g(x)q(x) + r(x),$$

con $r(x) = 0$ *o* $0 \leq gr(r(x)) < gr(g(x))$*. Además los polinomios* $q(x), r(x)$ *son únicos.*

Ejemplo 2.1.11. *Sean* $f(x), g(x) \in \mathbb{Z}[x]$*, con* $g(x) = x - 3$ *y* $f(x) = 7x^3 - 2x^2 + 5x - 2$*. Encuentren el cociente y el residuo al dividir el polinomio* $f(x)$ *entre el polinomio* $g(x)$*.*

$$\begin{array}{rr|rrrr} & & 7x^2 & +19x & +62 & \\ x & -3 & 7x^3 & -2x^2 & +5x & -2 \\ \cline{3-6} & & -7x^3 & +21x^2 & & \\ \cline{3-6} & & & 19x^2 & +5x & \\ & & & -19x^2 & +57x & \\ \cline{3-6} & & & & 62x & -2 \\ & & & & -62x & 186 \\ \cline{3-6} & & & & & 184 \end{array}$$

Por lo que $f(x) = (7x^2 + 19x + 62)(x - 3) + 184$*, el cociente es* $q(x) = 7x^2 + 19x + 62$ *y el residuo es* $r = 184$*.*

Ejemplo 2.1.12. *Sean* $f(x), g(x) \in \mathbb{Z}_7[x]$*, con* $g(x) = 3x^2 + 4x + 2$ *y* $f(x) = 6x^4 + 4x^3 + 5x^2 + 3x + 1$*. Encuentren el cociente y el residuo al dividir el polinomio* $f(x)$ *entre el polinomio* $g(x)$*.*

$$\begin{array}{rrr|rrrrr} & & & 2x^2 & +x & +6 & & \\ 3x^2 & +4x & +2 & 6x^4 & +4x^3 & +5x^2 & +3x & +1 \\ \cline{4-8} & & & -6x^4 & -x^3 & -4x^2 & & \\ \cline{4-8} & & & & 3x^3 & +x^2 & +3x & \\ & & & & -3x^3 & -4x^2 & -2x & \\ \cline{4-8} & & & & & 4x^2 & +x & +1 \\ & & & & & -4x^2 & -3x & -5 \\ \cline{4-8} & & & & & & 5x & +3 \end{array}$$

Por lo que $f(x) = (3x^2 + 4x + 2)(2x^2 + x + 6) + 5x + 3$*, el cociente es* $q(x) = 2x^2 + x + 6$ *y el residuo es* $r(x) = 5x + 3$*.*

División sintética

En el caso de dividir un polinomio entre otro polinomio de grado 1 podemos acudir a la división sintética. Revisamos la división del ejemplo 2.1.11. Si sólo escribimos los coeficientes nos queda:

$$\begin{array}{rccccc} & 7 & 19 & 62 & & \\ 3 & 7 & -2 & 5 & -2 & \\ & & 21 & & & \\ \hline & & 19 & 5 & & \\ & & & 57 & & \\ \hline & & & 62 & -2 & \\ & & & & 186 & \\ \hline & & & & 184 & \end{array}$$

En base al ejemplo podemos observar que los coeficientes del cociente igual que el residuo de la división aparecen de manera natural en las cuentas. Si resumimos las cuentas en dos renglones obtenemos lo siguiente.

$$\begin{array}{cccc|c} 7 & -2 & +5 & -2 & 3 \\ & 21 & 57 & 186 & \\ \hline 7 & 19 & 62 & 184 & \end{array}$$

Ahora observamos que cada número de la segunda renglón es el resultado de multiplicar 3 por el número que aparece en el tercer englón de la columna anterior.

$$\begin{array}{cccc|c} 7 & -2 & +5 & -2 & 3 \\ & 7(3) & 19(3) & 62(3) & \\ \hline 7 & 19 & 62 & 184 & \end{array}$$

Ejemplo 2.1.13. *Sean* $f(x) = x^5 + x^4 + 2x^3 + 3x^2 - 4x + 5, g(x) = x + 2$ *con* $f(x), g(x) \in \mathbb{Q}[x]$.

$$\begin{array}{cccccc|c} 1 & 1 & 2 & 3 & -4 & 5 & -2 \\ & -2(1) & -2(-1) & -2(4) & -2(-5) & -2(6) & \\ \hline 1 & -1 & 4 & -5 & 6 & -7 & \end{array}$$

Entonces $f(x) = g(x)q(x) + r$, *donde* $q(x) = x^4 - x^3 + 4x^2 - 5x + 6$, *y* $r = -7$.

Ejemplo 2.1.14. *Considera los polinomios del ejemplo 2.6 inciso 1:*
Sean $g(x) = x - 3$ *y* $f(x) = x^8 + 7x^5 - 4x^4 + 3x^3 + 5x^2 - 4$ *con* $f(x), g(x) \in \mathbb{Q}[x]$.

$$\begin{array}{ccccccccc|c} 1 & 0 & 0 & 7 & -4 & 3 & 5 & 0 & 5 & 3 \\ & 3 & 9 & 27 & 102 & 294 & 891 & 2668 & 8064 & \\ \hline 1 & 3 & 9 & 34 & 98 & 297 & 896 & 2688 & 8060 & \end{array}$$

Entonces $f(x) = g(x)q(x) + r$, *donde* $q(x) = x^7 + 3x^6 + 9x^5 + 34x^4 + 98x^3 + 297x^2 + 896x + 2688$, *y* $r = 8060$.

Ejemplo 2.1.15. *Considera los polinomios del ejemplo 2.6 inciso 2:*
Sean $g(x) = x + 9$ *y* $f(x) = 3x^5 + 8x^4 + x^3 - 2x^2 + 4x - 7$ *con* $f(x), g(x) \in \mathbb{Z}_{11}[x]$.

$$\begin{array}{cccccc|c} 3 & 8 & 1 & 9 & 4 & 4 & 2 \\ & 2(3) & 2(3) & 2(7) & 2(1) & 2(6) & \\ \hline 3 & 3 & 7 & 1 & 6 & 5 & \end{array}$$

Entonces $f(x) = g(x)q(x) + r$, *donde* $q(x) = 3x^4 + 3x^3 + 7x^2 + x + 6$, *y* $r = 5$.

En general, dado un campo $\mathbf{K}$, $b \in \mathbf{K}$ que no sea el neutro aditivo y dos polinomios $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0,\ g(x) = x - b \in \mathbf{K}[x]$, tenemos que.

a_n	a_{n-1}	a_{n-2}	$\ldots$	a_1	a_0	b
	ba_n	$b(a_{n-1} + ba_n)$	$\ldots$		$b\Delta$	
a_n	$a_{n-1} + ba_n$	$a_{n-2} + b(a_{n-1} + ba_n)$	$\ldots$	Δ	$a_0 + b\Delta$	

Entonces $r = a_0 + b\Delta$.

2.1.2 Máximo Común Divisor para polinomios

Vamos a definir el Algoritmo de Euclides para polinomios, para encontrar el máximo común divisor de dos polinomios con coeficientes en un mismo campo. Sean $P(x), Q(x) \in K[x]$. Si el polinomio $P(x) \mid Q(x)$ entonces para cualquier escalar $k \in K$, se tiene también que $k \cdot P(x) \mid Q(x)$. Para definir de manera única el polinomio que es el máximo común divisor de otros dos, pedimos que el coeficiente no nulo de mayor índice sea la unidad.

Definición 2.1.8. *Sea* $\mathbf{A}[x]$ *un anillo de polinomios. Si el anillo* $\mathbf{A}$ *tiene unidad* $\mathbf{u}$*, decimos que un polinomio de grado n es* **mónico** *si* $a_n = \mathbf{u}$*. Si un anillo de polinomios tiene coeficientes en alguno de los campos* $\mathbb{R}$*,* $\mathbb{Q}$*,* $\mathbb{Z}$ *o* $\mathbb{Z}_p$*, entonces un polinomio de grado n es mónico si* $a_n = 1$*.*

Definición 2.1.9. *Sean* $f, g \in \mathbf{K}[x]$*. Decimos que el polinomio* $h(x)$ *es un divisor común de* f *y* g *si* $h(x) \mid f(x)$ *y* $h(x) \mid g(x)$*. Además* $h(x)$ *es el máximo común divisor de* f *y* g *si* $h(x)$ *es un polinomio mónico y toda divisor común* $k(x) \in \mathbf{K}[x]$ *de* $f(x)$ *y* $g(x)$*, divide al polinomio* $h(x)$*.*

Proposición 2.1.10 (Algoritmo de Euclides)**.** *Sean* $f(x), g(x) \in \mathbf{K}[x]$*, tales que* $gr(g(x)) \leq gr(f(x))$ *y* $g(x)$ *no es el polinomio nulo. Primero dividimos* $f(x)$ *entre* $g(x)$ *obteniendo el residuo. Luego, en cada paso, aplicamos el algoritmo de división para el divisor anterior entre el residuo anterior hasta obtener como residuo al polinomio nulo.*

$$\begin{array}{rcll}
f(x) & = & q(x)g(x) + r(x) & gr(r(x)) < gr(g(x)) \\
g(x) & = & q_1(x)r(x) + r_1(x) & gr(r_1(x)) < gr(r(x)) \\
r(x) & = & q_2(x)r_1(x) + r_2(x) & gr(r_2(x)) < gr(r_1(x)) \\
 & & \vdots & \vdots \\
r_{k-2}(x) & = & q_k(x)r_{k-1}(x) + r_k(x) & gr(r_k(x)) < gr(r_{k-1}(x)) \\
r_{k-1}(x) & = & q_{k+1}(x)r_k(x) + r_{k+1}(x) & r_{k+1}(x) = 0
\end{array}$$

El último residuo no nulo $r_{k-1}(x)$ *es un máximo común divisor de los polinomios* $f(x), g(x)$*, y es un multiplo del máximo común divisor* **mónico** *de los polinomios* $f(x)$ *y* $g(x)$*.*

Demostración. Dados dos polinomios $f(x), g(x) \in \mathbf{K}[x]$, con $gr(g(x)) \leq gr(f(x))$ y $g(x)$ no

nulo. Aplicamos el algoritmo de división hasta tener como residuo al polinomio nulo,

$$\begin{array}{rcll} f(x) & = & q(x)g(x) + r(x) & gr(r(x)) < gr(g(x)) \\ g(x) & = & q_1(x)r(x) + r_1(x) & gr(r_1(x)) < gr(r(x)) \\ r(x) & = & q_2(x)r_1(x) + r_2(x) & gr(r_2(x)) < gr(r_1(x)) \\ & & \vdots & \vdots \\ r_{k-2}(x) & = & q_k(x)r_{k-1}(x) + r_k(x) & gr(r_k(x)) < gr(r_{k-1}(x)) \\ r_{k-1}(x) & = & q_{k+1}(x)r_k(x) + r_{k+1}(x) & r_{k+1}(x) = 0 \end{array}$$

En cada paso se aplica el ejercicio 2.8 que dice que si $h(x)$ divide a los polinomios $f(x), g(x)$ con $f(x) = q(x)g(x) + r(x)$, entonces $h(x)$ divide al polinomio residuo $r(x)$. □

Ejemplo 2.1.16. *Encontrar usando el Algoritmo de Euclides el máximo común divisor de* $f(x), g(x)$*, con* $f(x) = 6x^4 + 9x^3 + 5x^2 + 3x + 1$, $g(x) = 3x^3 - 3x^2 + x - 1$

$$\begin{array}{cccc|ccccc} & & & & 2x & +5 & & & \\ \hline 3x^3 & -3x^2 & +x & -1 & 6x^4 & +9x^3 & +5x^2 & +3x & -1 \\ & & & & -6x^4 & +6x^3 & -2x^2 & +2x & \\ \hline & & & & & 15x^3 & +3x^2 & +5x & -1 \\ & & & & & -15x^3 & +15x^2 & -5x & -5 \\ \hline & & & & & & 18x^2 & & -6 \end{array}$$

Por lo que $f(x) = g(x)(2x + 5) + (18x^2 - 6)$.

Ahora dividimos $g(x) = 3x^3 - 3x^2 + x - 1$ *entre el residuo de la división anterior* $(18x^2 - 6)$*, por el inciso 2. del corolario 2.1.11, podemos simplificar la división como sigue*

$$\begin{array}{cc|cccc} & & x & -1 & & \\ \hline 3x^2 & -1 & 3x^3 & -3x^2 & +x & -1 \\ & & -3x^3 & & -x & \\ \hline & & & -3x^2 & & -1 \\ & & & +3x^2 & & +1 \\ \hline & & & & & 0 \end{array}$$

Por lo que $g(x) = 6(3x^2 - 1)(x - 1) = 18(x^2 - 1/3)(x - 1)$*. Según el Algoritmo de Euclides (proposición 2.1.10)*

$$mcd(f(x), g(x)) = x^2 - 1/3.$$

Decimos que dos polinomios f, g son primos relativos si $mcd(f(x), g(x)) = 1$.

2.1.3 Raíces de polinomios

Como consecuencia del Algoritmo de la División para Polinomios se tiene el siguiente resultado:

Corolario 2.1.11. *Sea* $\mathbf{K}$ *un campo,* $a \in \mathbf{K}$ *y* $f(x), g(x) \in \mathbf{K}[x]$*, con* $gr(f(x)) = n \geq 1$*. Entonces*

1. *$f(a)$ es el residuo de $f(x)$ entre $(x-a)$.*
2. *a es raíz de f si y solo si $(x-a) \mid f(x)$ (es decir, $(x-a)$ es factor de $f(x)$).*
3. *$(x-a) \mid f(x) - f(a)$.*
4. *Si $(x-a) \mid f(x)g(x)$, entonces $(x-a) \mid f(x)$ o $(x-a) \mid g(x)$.*

Demostración. Sea $f \in \mathbf{K}[x]$, con $n \geq 1$, y sea $a \in \mathbf{K}$.

1. Por el teorema 2.1.7 existen dos polinomios $q(x)$,$r(x) \in \mathbf{K}[x]$ tales que $f(x) = (x-a)q(x) + r(x)$ tal que $r(x) = 0$ o $0 \leq gr(r(x)) < gr(x-a) = 1$. Si el residuo $r(x) = 0$, entonces $f(x) = (x-a)q(x)$ y si evaluamos el polinomio $f(x)$ en a obtenemos que $f(a) = (a-a)q(a) = 0$, por lo que el $f(a) = 0 = r(x)$. Si $r(x) \neq 0$, entonces $0 \leq gr(r(x)) < 1$, es decir, el grado del residuo $r(x)$ es cero y $r(x)$ es una constante. Sea $r(x) = r$ con $r \in \mathbf{K}$. Podemos reescribir la función $f(x)$ como

   $$f(x) = (x-a)q(x) + r.$$

   Evaluamos el polinomio $f(x)$ en a:

   $$f(a) = (a-a)q(a) + r = 0 + r = r.$$

   Por lo que $f(a)$ es el residuo de $f(x)$ entre $(x-a)$.

2. Si a es una raíz de $f(x)$, tenemos por definición que $f(a) = 0$. Por el incico 1, el residuo de $f(x)$ entre $(x-a)$ es cero, y $f(x) = (x-a)q(x)$. Por lo que $(x-a) \mid f(x)$.

   Si $(x-a) \mid f(x)$, entonces $f(x) = q(x)(x-a)$ y por la unicidad del residuo en el Teorema 2.1.7, el residuo es cero. Entonces $f(a) = 0$ y a es raíz de f.

3. Por el Teorema 2.1.7, se tiene que $f(x) = (x-a)q(x) + r$ con $r \in \mathbf{K}$. Como $f(a) = r$, entonces $f(x) = (x-a)q(x) + f(a)$, y $f(x) - f(a) = (x-a)q(x)$ por lo que

   $$(x-a) \mid f(x) - f(a).$$

4. Si $(x-a) \mid f(x)g(x)$, entonces por el inciso 2. tenemos que $f(a)g(a) = 0$. Como $f(a), g(a) \in \mathbf{K}$ y $\mathbf{K}$ es un campo, entonces por el ejercicio 1.9, $f(a) = 0$ o $g(a) = 0$, de allí a es raíz de $f(x)$ o a es raíz de $g(x)$. Por lo tanto $(x-a) \mid f(x)$ o $(x-a) \mid g(x)$.

□

Proposición 2.1.12. *Sea $(\mathbf{K}, +, \cdot)$ un campo, sea $f(x) \in \mathbf{K}[x]$ un polinomio de grado n, entonces f tiene a lo más n raíces en $\mathbf{K}$.*

Demostración. Por inducción sobre el grado n del polinomio.
Base: Sea $f \in \mathbf{K}[x]$ un polinomio de grado 1, con $f(x) = a_1x - a_0$, y $a_1 \neq 0$. Como $\mathbf{K}$ es un campo, entonces a_1 tiene un inverso multiplicativo (a_1^{-1}), por lo que

$$f(x) = 0 \Leftrightarrow a_1x - a_0 = 0 \Leftrightarrow a_1x = a_0 \Leftrightarrow x = (a^{-1})a_0.$$

Por lo tanto $x = (a^{-1})a_0$ es raíz de $f(x)$.

Supón que α_1 y α_2 son raíces de $f(x)$. Entonces $f(\alpha_1) = 0 = f(\alpha_2) \Leftrightarrow a_1\alpha_1 - a_0 = a_1\alpha_2 - a_0 \Leftrightarrow a_1\alpha_1 = a_1\alpha_2 \Leftrightarrow \alpha_1 = \alpha_2$, pues a_1 tiene inverso multiplicativo. Por lo tanto $f(x) = a_1x - a_0$ tiene una sola raíz, a saber $x = (a^{-1})a_0$.

Hipótesis de Inducción: Supón que un polinomio $f(x) \in \mathbf{K}[x]$ de grado k tiene a lo más k raíces en $\mathbf{K}$.

Paso inductivo: Sea $g(x) \in \mathbf{K}[x]$ de grado $k+1$. Si $g(x)$ no tiene raíces, entonces tiene a lo mas $k+1$, pues $0 < k+1$. Si α es raíz de $g(x)$, entonces existe $q(x) \in \mathbf{K}[x]$ tal que $g(x) = (x-\alpha)q(x)$ donde $q(x)$ tiene grado k, luego por la hipótesis de inducción q tiene a lo más k raíces y $g(x)$ tiene a lo mas las raíces de q y la raíz α, por lo que a lo más tiene $k+1$ raíz. □

2.1.4 Ejercicios

Ejercicio 2.1. *Determina el número de polinomios de grado* 2 *en* $\mathbb{Z}_2$.

Ejercicio 2.2. *Determina el número de polinomios de grado* 2 *en* $\mathbb{Z}_7$.

Ejercicio 2.3. *¿Qué base debe tener el sistema numérico en donde* 754 *tenga la representación* 3254*?*

Ejercicio 2.4. *Sea* $(\mathbf{A}, +, \cdot)$ *un dominio entero (definición 1.1.5). Entonces* $\mathbf{A}[x]$ *es un dominio entero.*

Ejercicio 2.5. *¿Cuántas soluciónes tiene* $x + y + z = 0$ *en* $\mathbb{Z}_2$*? y en* $\mathbb{Z}_3$*?*

Ejercicio 2.6. *En cada inciso encuentra el cociente y el residuo al dividir el polinomio* $f(x)$ *entre el polinomio* $g(x)$*.*

i) Sean $g(x) = x - 3$ *y* $f(x) = x^8 + 7x^5 - 4x^4 + 3x^3 + 5x^2 - 4$ *con* $f(x), g(x) \in \mathbb{Q}[x]$.

ii) Sean $g(x) = x + 9$ *y* $f(x) = 3x^5 + 8x^4 + x^3 - 2x^2 + 4x - 7$ *con* $f(x), g(x) \in \mathbb{Z}_{11}[x]$.

Ejercicio 2.7. *Dada las siguientes dos tablas de división sintética, expresa en cada caso como polinomios el divisor, el dividiendo, el cociente y el residuo.*

i)

6	−11	−21	−4	−2
	−12	46	−50	
6	−23	25	−54	

ii)

1	−10	24	−1	0	36	6
	6	−24	0	−6	−36	
1	−4	0	−1	−6	0	

Ejercicio 2.8. *Si* $h(x)$ *divide a los polinomios* $f(x), g(x)$ *con* $f(x) = q(x)g(x) + r(x)$*, entonces* $h(x)$ *divide al residuo* $r(x)$*. Hint: La prueba es análoga a la prueba para el resultado análogo en* $\mathbb{Z}$*.*

Ejercicio 2.9. *Encuentren el máximo común divisor de las siguientes parejas de polinomios en el anillo que se indica.*

1. $f(x) = x^5 - x^4 + x^3 + x^2 - x - 1$ *y* $g(x) = x^2 + x - 2$ *en el anillo* $\mathbb{Q}[x]$.
2. $f(x) = x^4 + x^3 + 1$ *y* $g(x) = x^2 + x + 2$ *en el anillo* $\mathbb{Z}_2[x]$.

Ejercicio 2.10. *Si* $f(x) \mid g(x)$*, entonces toda raíz de* $f(x)$ *es raíz de* $g(x)$.

Ejercicio 2.11. *Sea* $f \in \mathbb{R}[x]$. *Entonces* $(x - a) \mid f(x)$ *si y solamente si* $(x - \overline{a}) \mid f(x)$.

Ejercicio 2.12. *Si* $(x - a) \mid f(x)$ *y* $(x - a) \nmid g(x)$*, entonces* $(x - a) \nmid f(x) + g(x)$.

2.2 Propiedades de los anillos de polinomios

El anillo de polinomios con coeficientes en el anillo A tiene las misma propiedades que el anillo A, salvo orden. Primero vamos a clasificar los polinomios irreducibles de grado a lo mas tres. Los polinomios irreducibles juegan el mismo papel que lo números primos en $\mathbb{Z}$.

2.2.1 Polinomio irreducibles

Sea $\mathbf{K}$ un campo y $f(x) \in \mathbf{K}[x]$, con grado al menos 2. Decimos que $f(x)$ es **reducible** si existen $g(x), h(x) \in \mathbf{K}[x]$, tales que $f(x) = g(x)h(x)$ y $gr(g(x)), gr(h(x)) \geq 1$. Si $f(x)$ no es reducible, decimos que es **irreducible**.

Teorema 2.2.1. *Sea* $\mathbf{K}$ *un campo y* $f(x) \in \mathbf{K}[x]$.

1. *Si* $f(x)$ *tiene grado a lo más* 1*, entonces* $f(x)$ *es irreducible.*
2. *Si* $2 \leq gr(f(x)) \leq 3$*, entonces el polinomio* $f(x)$ *tiene una raíz si y solo si* $f(x)$ *es reducible.*

Demostración. Ejercicio 2.18. □

Sea $\mathbf{K}$ un campo y sea $f(x) \in \mathbf{K}[x]$ un polinomio de grado al menos 4. Puede darse el caso en que $f(x)$ es reducible sin tener raíces. Por ejemplo: Sea $f(x) \in \mathbb{R}[x]$, con

$$\begin{aligned} f(x) &= x^4 - 2x^3 + 5x^2 - 2x + 4 \\ &= (x^2 + 1)(x^2 - 2x + 4). \end{aligned}$$

No es difícil comprobar que los factores son irreducibles en $\mathbb{R}[x]$ (basta probar que no tienen raíces reales).

Ejemplo 2.2.1. *Considera los campos* $\mathbb{R}[x], \mathbb{Q}[x]$ *y* $\mathbb{C}[x]$. *Determina en qué campos los siguientes polinomios tienen raíces, encuentra las (según el campo) así como la factorización del polinomio. Determina en qué campos son irreducibles.*

1. $p(x) = x^2 + 1$

   En $\mathbb{C}[x]$ *el polinomio* $p(x)$ *tiene dos raíces* $x = -i$ *y* $x = i$, *por lo que* $p(x) = (x+i)(x-i)$, *pero es irreducible en* $\mathbb{R}[x]$ *y en* $\mathbb{Q}[x]$.

2. $p(x) = x^4 + 2x^2 + 1$

   El polinomio $p(x)$ *es reducible en* $\mathbb{R}[x], \mathbb{Q}[x]$ *ya que* $p(x) = x^4 + 2x^2 + 1 = (x^2 + 1)^2$, *aunque no tiene raíces reales. En* $\mathbb{C}[x]$ *el polinomio tiene dos raíces dobles:* $x = -i$ *y* $x = i$, *por lo que* $p(x) = (x+i)(x-i)$ *y la factorización en* $\mathbb{C}[x]$ *es* $p(x) = (x+i)^2(x-i)^2$.

Ejemplo 2.2.2. *Encontrar las raíces de los siguientes polinomios en el anillo de polinomios especificado.*

1. $p(x) = x^3 + x^2 + x + 1$, *en* $\mathbb{Z}_2[x]$.

2. $p(x) = x^3 + x + 1$, *en* $\mathbb{Z}_2[x]$.

3. $p(x) = x^2 + x + 1$, *en* $\mathbb{Z}_3[x]$.

1. $p(0) = 1$, $p(1) = 0$, *entonces* 1 *es raíz del polinomio* $p(x)$. *Usamos división sintética para encontrar el cociente.*

$$\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 1 \\ & 1(1) & 1(0) & 1(1) & \\ \hline 1 & 0 & 1 & 0 & \end{array}$$

   Entonces $p(x) = x^3 + x^2 + x + 1 = (x^2 + 1)(x + 1)$. *Sea* $g(x) = x^2 + 1$, $g(0) = 1$ *y* $g(1) = 0$, *por lo que* 1 *es raíz de* $g(x)$. *Usamos división sintética para encontrar el cociente.*

$$\begin{array}{ccc|c} 1 & 0 & 1 & 1 \\ & 1(1) & 1(1) & \\ \hline 1 & 1 & 0 & \end{array}$$

   Entonces $p(x) = x^3 + x^2 + x + 1 = (x^2 + 1)(x + 1) = (x + 1)^3$. *Por lo que* 1 *es una raíz "triple" de* $p(x)$.

2. $p(0) = 1$, $p(1) = 1$, *entonces el polinomio* $p(x)$ *no tiene raíces.*

3. $p(0) = 1$, $p(1) = 0$, $p(2) = 1$, *entonces* 1 *es raíz del polinomio* $p(x)$. *Usamos división sintética para encontrar el cociente.*

$$\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ & 1(1) & 1(2) & \\ \hline 1 & 2 & 0 & \end{array}$$

   Entonces $p(x) = x^2 + x + 1 = (x - 1)(x + 2) = (x + 2)^2$.

2.2.2 El anillo de polinomios $\mathbb{R}[x]$.

Teorema 2.2.2 (Teorema Fundamental del Álgebra)**.** *Todo polinomio $f(x) \in \mathbb{R}[x]$, de grado $n \in \mathbb{N}$ tiene al menos una raíz compleja.*

La prueba del Teorema Fundamental del Álgebra sale del objetivo de las notas.

Teorema 2.2.3 (Teorema de la Factorización Única)**.** *Sea $f(x) \in \mathbb{C}[x]$, de grado $n \in \mathbb{N}$, Entonces existen n números complejas $\alpha_1, \alpha_2, \ldots, \alpha_n$ no necesariamente distintos entre sí, y un número $c \in \mathbb{C}$ tales que*

$$f(x) = c(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n).$$

Además, esta factorización es única salvo el orden de los factores.

Demostración. **Existencia**: Demostración por inducción sobre el grado n del polinomio.
Base: Sea $f(x) \in \mathbb{C}[x]$, de grado $n = 1$. Asumimos que $f(x) = ax - b$, con $a \neq 0$. Sea a^{-1} el inverso multiplicativo de a, entonces $f(x) = a(x - ba^{-1})$ y $c = a$ y $\alpha = ba^{-1}$ y el teorema es cierto para $n = 1$.
Hipótesis de Inducción: Supón que todo polinomio $f(x)$ de grado k tiene una factorización

$$f(x) = c(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_k),$$

con $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{C}$ no necesariamente distintos entre sí, y $c \in \mathbb{C}$.
Paso inductivo: Sea $g(x) \in \mathbb{C}[x]$, de grado $k+1$. Por el teorema Fundamental del álgebra $g(x)$ tiene una raíz compleja α. Entonces $x - \alpha \mid g(x)$ y existe un $q(x) \in \mathbb{C}[x]$ tal que $g(x) = q(x)(x-\alpha)$. Entonces $q(x)$ es de grado k y por la hipóteses de inducción sabemos que existen k números complejas $\alpha_1, \alpha_2, \ldots, \alpha_k$ no necesariamente distintos entre sí, y un número $c \in \mathbb{C}$ tales que

$$q(x) = c(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_k).$$

Por lo que

$$\begin{aligned} g(x) &= q(x)(x-\alpha) \\ &= c(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_k)(x-\alpha). \end{aligned}$$

Sea $\alpha_n = \alpha$, entonces $g(x) = c(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_k)(x-\alpha_{k+1})$.

Por el Principio de Inducción hemos probado la existencia de la factorización. Falta probar la unicidad.

Unicidad: Ejercicio 2.19. □

Observa que dada $f(x) = c(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$, con $c \neq 0$, y $n \in \mathbb{N}$, entonces α es raíz de $f(x)$ si y solo si $\alpha = \alpha_i$ para alguna $1 \leq i \leq n$.

Definición 2.2.4. *Sea $f(x) = c(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$, con $c \neq 0$, y $n \in \mathbb{N}$, un polinomio de grado n. Decimos que una raíz α de $f(x)$ es de multiplicidad m si*

$$(x-\alpha)^m \mid f(x), \text{ pero } (x-\alpha)^{m+1} \nmid f(x).$$

o bien si hay m indices i tales que $\alpha_i = \alpha$.

Ejemplo 2.2.3. *Determinar la multiplicidad de $x = 1$ en el polinomio*

$$f(x) = x^4 - 2x^3 + 2x^2 - 2x + 1.$$

Usaremos división sintética para determinar la multiplicidad.

					|
1	−2	2	−2	1	| 1
	1(1)	1(−1)	1(1)	1(−1)	
1	−1	1	−1	0	
	1(1)	1(0)	1(1)		
1	0	1	0		
	1(1)	1(1)			
1	1	2			

Por lo que $(x-1)^2 \mid f(x)$, pero $(x-1)^3 \nmid f(x)$. Por lo tanto $x = 1$ es una raíz de multiplicidad 2.

Raíces complejas de polinomios con coeficientes reales.

Proposición 2.2.5. *Sea $f \in \mathbb{R}[x]$, y sea $\alpha \in \mathbb{C}$ una raíz de f. Entonces $\overline{\alpha}$ tambien es una raíz del polinomio $f(x)$.*

Demostración. Sea $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots a_1 x + a_0$, y sea α una raíz de $f(x)$. Si $\alpha \in \mathbb{R}$, entonces $\overline{\alpha} = \alpha$ por lo que la proposición es cierta. Si $\alpha \notin \mathbb{R}$, entonces

$$\begin{aligned} f(\overline{\alpha}) &= a_n\overline{\alpha}^n + a_{n-1}\overline{\alpha}^{n-1} + \ldots + a_1\overline{\alpha} + a_0 \\ &= a_n\overline{\alpha^n} + a_{n-1}\overline{\alpha^{n-1}} + \ldots + a_1\overline{\alpha} + a_0, \end{aligned}$$

ya que $\overline{\alpha}^n = \overline{\alpha^n}$. Como cada coeficiente $a_i \in \mathbb{R}$, entonces $a = \overline{a}$ y

$$\begin{aligned} f(\overline{\alpha}) &= \overline{a_n\alpha^n} + \overline{a_{n-1}\alpha^{n-1}} + \ldots \overline{a_1\alpha} + \overline{a_0} \\ &= \overline{a_n\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1 x + a_0} \\ &= \overline{f(\alpha)} = \overline{0} = 0. \end{aligned}$$

Por lo que $\overline{\alpha}$ es raíz de $f(x)$. □

Observa que las raíces no complejas (no reales) siempre vienen en parejas $\{\alpha, \overline{\alpha}\}$.

Como consecuencia de la proposición 2.2.5 y el Teorema de la Factorización Única (teorema 2.2.3) tenemos el siguiente resultado.

Corolario 2.2.6. *Sea $f \in \mathbb{R}[x]$ un polinomio de grado $n \in \mathbb{N}$. Entonces $f(x)$ es irreducible si y solo si*

1. *$f(x)$ es de grado 1, o*
2. *$f(x)$ es de grado 2 y $f(x)$ no tiene raíces reales.*

Raíces racionales de polinomios con coeficientes enteros

Vamos a caracterizar las raíces racionales de un polinomio con coeficientes enteras.

Proposición 2.2.7. *Sea* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots a_1 x + a_0$, $a_i \in \mathbb{Z}$ *para* $0 \leq i \leq n$, *Sean* $p, q \in \mathbb{Z}$ *primos relativos. Si* $\frac{p}{q} \in \mathbb{Q}$ *es una raíz de* $f(x)$, *entonces* $p \mid a_0$ *y* $q \mid a_n$.

Demostración. Sean $p, q \in \mathbb{Z}$ primos relativos tales que $\frac{p}{q} \in \mathbb{Q}$ es una raíz de $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots a_1 x + a_0$, entonces $f\left(\frac{p}{q}\right) = 0$.

Primero probaremos que $p \mid a_0$. Evaluamos la función $f(x)$ en la raíz racional $\frac{p}{q}$:

$$\begin{aligned} 0 &= f\left(\frac{p}{q}\right) = a_n\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \ldots + a_1\left(\frac{p}{q}\right) + a_0 \\ 0 &= a_n p^n + a_{n-1}p^{n-1}q + a_{n-2}p^{n-2}q^2 + \ldots + a_1 pq^{n-1} + q^n a_0, \end{aligned}$$

ya que $q \neq 0$. Despejamos el sumando $a_0(-q^n)$:

$$\begin{aligned} a_0(-q^n) &= a_n p^n + a_{n-1}p^{n-1}q + a_{n-2}p^{n-2}q^2 + \ldots + a_1 pq^{n-1} \\ &= p(a_n p^{n-1} + a_{n-1}p^{n-2}q + \ldots + a_2 pq^{n-2} + a_1 q^{n-1}). \end{aligned}$$

Por lo que $p \mid a_0 q^n$. Como $mcd(p, q) = 1$, entonces $p \mid a_0$.

Vamos a probar que $q \mid a_n$. Evaluamos la función $f(x)$ en la raíz racional $\frac{p}{q}$:

$$\begin{aligned} 0 &= a_n\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \ldots + a_1\left(\frac{p}{q}\right) + a_0 \\ 0 &= a_n p^n + a_{n-1}p^{n-1}q + a_{n-2}p^{n-2}q^2 + \ldots + a_1 pq^{n-1} + q^n a_0, \end{aligned}$$

ya que $q \neq 0$. Despejamos el sumando $a_n(-p^n)$:

$$\begin{aligned} a_n(-p^n) &= a_{n-1}p^{n-1}q + a_{n-2}p^{n-2}q^2 + \ldots + a_1 pq^{n-1} + q^n a_0 \\ &= q(a_{n-1}p^{n-1} + a_{n-2}p^{n-2}q + a_{n-3}p^{n-3}q^2 + \ldots + a_1 pq^{n-2} + q^{n-1}a_0). \end{aligned}$$

Por lo que $q \mid a_n p^n$. Como $mcd(p, q) = 1$, entonces $q \mid a_n$. □

Por lo tanto las raíces racionales de un polinomio con coeficientes enteras es un subconjunto del conjunto $\{\pm\frac{p}{q} : p \mid a_0, q \mid a_n\}$. Observa además que las raíces racionales de un polinomio mónico son raíces enteras, pues $a_n = 1$.

Ejemplo 2.2.4. *Para el polinomio* $f(x) = 4x^4 - 4x^3 + 5x^2 - 8x - 6$ *enumera las posibles ráices racionales, determina cuales de en efecto son raíces y finalmente usa esta información para encontrar una*
factorización del polinomio en que cada factor es irreducible en $\mathbb{Q}[x]$, *luego factoriza el polinomio en factor es irreducible* $\mathbb{R}[x]$ *y finalemente factoriza el polinomio factores lineales en* $\mathbb{C}[x]$.

Los divisores positivos de 4 *son* $\{1, 2, 4\}$, *y de* 6 *son* $\{1, 2, 3, 6\}$. *Las posibles raíces son* $\{\pm\frac{p}{q} : p \mid 6, q \mid 4\} = \{\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm 2, \pm 3, \pm\frac{3}{2}, \pm\frac{3}{4}, \pm 6\}$. *Hay* 16 *posibles raíces racionales.*

Usaremos división sintética para buscar las raíces. En caso de tener una raíz racional factorizamos el polinomio para simplificaremos la busqueda.

4	−4	5	−8	−6	1
	4	0	5	−3	
4	0	5	−3	−9	

4	−4	5	−8	−6	−1
	−4	8	−13	21	
4	−8	13	−21	15	

Por lo que $x = \pm 1$ *no son raíces de* $f(x)$.

4	−4	5	−8	−6	$\frac{1}{2}$
	2	1	3	$-2\frac{1}{2}$	
4	2	6	−5	$-8\frac{1}{2}$	

4	−4	5	−8	−6	$-\frac{1}{2}$
	−2	3	−4	6	
4	−6	8	−12	0	

Por lo que $x = \frac{1}{2}$ *no es raíz de* $f(x)$*, pero* $x = -\frac{1}{2}$ *sí es raíz de* $f(x)$*, y* $f(x) = (x + \frac{1}{2})(4x^3 - 6x^2 + 8x - 12)$.

Buscamos ahora las raíces de $g(x) = 4x^3 - 6x^2 + 8x - 12$*. Sabemos que* $x \in \{-1, 1, -\frac{1}{2}\}$ *no son raíces del polinomio* $g(x)$*. Las posibles raíces del polinomio* $g(x)$ *son*

$$\{-\frac{1}{2}, \pm\frac{1}{4}, \pm 2, \pm 3, \pm\frac{3}{2}, \pm\frac{3}{4}, \pm 6\}.$$

4	−6	+8	−12	$\frac{1}{2}$
	2	−2	3	
4	−4	6	−9	

Por lo que $x = -\frac{1}{2}$ *no es raíz de* $g(x)$*, y no es raíz de multiplicidad* 2 *de* $f(x)$.

4	−6	+8	−12	$\frac{1}{4}$
	1	$\frac{-5}{4}$	$\frac{27}{16}$	
4	−5	$\frac{27}{4}$	$\frac{-165}{16}$	

4	−6	+8	−12	$-\frac{1}{4}$
	−1	$-\frac{7}{4}$	$-\frac{25}{16}$	
4	−7	$\frac{25}{4}$	$\frac{-217}{16}$	

por lo que $x = \pm\frac{1}{4}$ *no son raíces de* $g(x)$*, y tampoco son raíces de* $f(x)$.

4	−6	+8	−12	2
	8	4	24	
4	2	12	−12	

4	−6	+8	−12	−2
	−8	28	−72	
4	−14	36	−84	

Por lo que $x = \pm 2$ *no son raíces de* $g(x)$*, y tampoco son raíces de* $f(x)$.

4	−6	+8	−12	3
	12	18	78	
4	6	26	66	

4	−6	+8	−12	−3
	−12	54	−186	
4	−18	62	−198	

Por lo que $x = \pm 3$ *no son raíces de* $g(x)$*, y tampoco son raíces de* $f(x)$.

4	−6	+8	−12	$\frac{3}{2}$
	6	0	12	
4	0	8	0	

Por lo que $x = \frac{3}{2}$ es una raíz de $g(x)$, $g(x) = (x - \frac{3}{2})(4x^2 + 8)$ y

$$\begin{aligned} f(x) &= \left(x + \frac{1}{2}\right)(4x^3 - 6x^2 + 8x - 12) = \left(x + \frac{1}{2}\right)\left(x - \frac{3}{2}\right)(4x^2 + 8) \\ &= 4\left(x + \frac{1}{2}\right)\left(x - \frac{3}{2}\right)(x^2 + 2). \end{aligned}$$

La factorización en factores irreducibles en $\mathbb{Q}[x]$ es

$$f(x) = 4\left(x + \frac{1}{2}\right)\left(x - \frac{3}{2}\right)(x^2 + 2).$$

Como $h(x) = x^2+2$ no tiene raíces reales, también es la factorización en factores irreducibles en $\mathbb{R}[x]$.

Buscamos las raíces complejas del polinomio $h(x) = x^2 + 2$. Sea $h(x) = 0$, entonces $x^2 + 2 = 0 \Rightarrow x^2 = -2 \Rightarrow x = \pm\sqrt{-2} = \pm\sqrt{2}i$. Por lo que $h(x) = (x - \sqrt{2}i)(x + \sqrt{2}i)$, y la factorización en factores irreducibles en $\mathbb{C}[x]$ es

$$f(x) = 4\left(x + \frac{1}{2}\right)\left(x - \frac{3}{2}\right)(x - \sqrt{2}i)(x + \sqrt{2}i).$$

2.2.3 Ejercicios

Ejercicio 2.13. *Encuentren la factoriazación de los siguientes polinomios*

1. *$p(x) = x^2 + 1$, en $\mathbb{Z}_2$.*
2. *$p(x) = x^4 + x^3 + 1$, en $\mathbb{Z}_2$.*
3. *$p(x) = x^2 + x + 1$ en $\mathbb{Z}_3$, $\mathbb{Z}_5$ y $\mathbb{Z}_7$.*
4. *De un ejemplo de un polinomio con coeficientes reales que no tenga raíces.*

Ejercicio 2.14. *Sea $f(x) = x^2+3x+2$ en $\mathbb{Z}_6$. ¿Es la factorización del polinomio $f(x)$ único? ¡Justifica tu respuesta! (vean el ejemplo 2.1.10).*

Ejercicio 2.15. *Encontrar las raíces en $\mathbb{R}[x], \mathbb{Q}[x], \mathbb{C}[x]$ de los siguientes polinomios.*
a) $p(x) = x^4 - 16$, b) $p(x) = x^4 - 25$.

Ejercicio 2.16. *Sea $P(x) \in \mathbb{Z}$ un polinomio mónico. Si r es una raíz de $P(x)$, entonces $r \mid a_0$, donde a_0 es el término constante del polinomio $P(x)$.*

Ejercicio 2.17. *Sea $P(x) \in \mathbb{C}$ un polinomio mónico de grado n. Sean $r_1, r_2, \ldots, r_n$ las n raíces de $P(x)$. Entonces $r_1 \cdot r_2 \cdot \cdots \cdot r_n = a_0$, donde a_0 es el término constante del polinomio $P(x)$.*

Ejercicio 2.18. *Prueba el teorema 2.2.1*

Ejercicio 2.19. *Prueba la unicidad del Teorema de la Factorización Única (teorema 2.2.3).*

Ejercicio 2.20. *Determinar la multiplicidad de $x = 1$ en los siguientes polinomios*

1. $f(x) = x^4 - x^3$.
2. $f(x) = x^5 - 3x^4 + 5x^3 - 4x^2 + 3x - 1$.
3. $f(x) = x^4 - 2x^3 + 2x^2 - 2x + 1$.

Ejercicio 2.21. *Para cada polinomio enumera las posibles raíces racionales, determina cuales de en efecto son raíces y finalmente usa esta información para encontrar una factorización del polinomio en que cada factor es irreducible en $\mathbb{Q}[x]$.*

1. $x^4 - 4x^3 - 9x^2 + 16x + 20$.
2. $x^4 - 4x^3 - x^2 - 16x - 20$.
3. $12x^4 - 3x^3 - 31x^2 + 4x + 20$.
4. $12x^5 - 9x^4 + 4x^3 - 3x^2 - 8x + 6$.
5. $2x^6 - 5x^5 + x^4 + 5x^3 - 7x^2 + 10x - 6$.
6. $2x^7 - 3x^5 + 2x^4 - x^3 + 7x - 2$.

2.3 Proyectos

Números pitagóricos

Una terna de números naturales a, b, c forma una **terna pitagórica** si hay un triángulo rectángulo cuyos lados son a, b y c. Es fácil checar si una terna dada es una terna pitagórica, por ejemplo $3, 4, 5$ forman una terna pitagórica ya que

$$3^2 + 4^2 = 5^2.$$

¿Cuántas ternas pitagóricas hay? ¿Encuentra una manera anaítica para caracterizar las ternas pitagóricas. Para mayor información ver capítulo 8 en [13].

Una aplicación de la división sintética

Dado un polinomio $P(x)$ encuentra un algoritmo para escribir el polinomio $P(x)$ como un polinomio en términos de $x - a$, es decir,

$$P(x) = a'_n(x-a)^n + a'_{n-1}(x-a)^{n-1} + a'_{n-2}(x-a)^{n-2} + \cdots + a'_2(x-a)^2 + a'_1(x-a)^1 + a'_0.$$

En [4] hay un algoritmo basado en la división sintética. Busca al menos una aplicación de este cambio.

Funciones Generatrices

Los polinomios juegan un papel importante en la construcción de funciones generatrices. Estudia explica dos ejemplos de la sección 9.1 [9], así como un ejemplo teórico y otro práctico de otra fuente. Explica con tus propias palabras la importancia de las funciones generatrices en solución de problemas teóricas como prácticas.

3 Introducción a la Teoría de las Gráficas

Se dice que la Teoría de las Gráficas nació con el problema de los puentes de Königsberg (Sección 3.0.1) que el matemático Leonard Euler[4] consideró en su versión general en *Solutio Problematis ad geometriam situs pertinentis, Commentarii Academiae Scientiarum Imperialis Petropolitanae 8 (1736), pp. 128-140*. Pasaron 100 años antes de que saliera el primer libro de Teoría de las Gráficas: *Theorie der endlichen und unendlichen Graphen* (Teubner, Leipzig, 1936) escrito por König. Hoy en día la Teoría de las Gráficas se ha convertido en una rama amplia y popular dentro de las matemáticas discretas tanto en aspectos teóricos como por la extensa gamma de aplicaciones que tiene en las matemáticas, computación así como en las ciencias sociales.

Una gráfica puede modelar una situación real o hipotética y se puede estudiar sus estructuras y propiedades para dar solución a un problema real o teórico. El objetivo del capítulo es introducir los fundamentos de la Teoría de las Gráficas y revisar algunos problemas o situaciones que se pueden modelar mediante una gráfica o una gráfica dirigida. Los conceptos básicos se motivan a través de cuatro problemas que fueron importantes para el desarrollo de la Teoría de las Gráficas. Después se presentan las definiciones formales así como una revisión de la teoría básica que se requiere para darle respuesta a los problemas que se modelan. Durante el capítulo se trabaja, cuando sea oportuno, con aplicaciones de la Teoría de las Gráficas en diferentes áreas de las ciencias sociales y ciencias exactas como redes de distribución, computación, eletrónica, ciencias sociales, pero también tiene aplicaciones teóricas como cadenas discretas de Markov, representación de grupos y relaciones finitas.

Vamos a motivar intuitivamente algunos conceptos antes de introducir la terminología de la Teoría de las Gráficas y antes de iniciar con la revisión teórica. En esta sección introductoria consideramos una gráfica como un conjunto de vértices (puntos) y un conjunto de aristas (líneas) donde cada arista une exactamente dos puntos.

3.0.1 Los puentes de Königsberg.

La ciudad alemana (ahora rusa) Königsberg (ver figura 3.1) fue testigo del inicio de la rama de las matemáticas llamada Teoría de las Gráficas (o Teoría de los Grafos). La ciudad de Königsberg es atravezada por un rio con islas. En el siglo XVIII, era costumbre hacer paseos los domingos y los habitantes de la ciudad de Königsberg procuraban recorrer cada puente exactamente una vez, sin embargo no lo lograban. Siempre faltaba algún puente o tenían que recorrer algún puente mas de una vez.

[4] "Hace trescientos años, nació en Basilea el matemático más prolífico de toda la historia. A lo largo de su dilatada vida científica amplió las fronteras de las matemáticas en todas sus ramas, y no sólo las fronteras de las matemáticas, su actividad creadora se extiende por la casi totalidad de las ciencias. Su influencia impregna todas las materias científicas a lo largo del siglo XVIII. Sin su figura las matemáticas serían otras."
Fuente: http://divulgamat.ehu.es/weborriak/historia/MateOspetsuak/Euler.asp

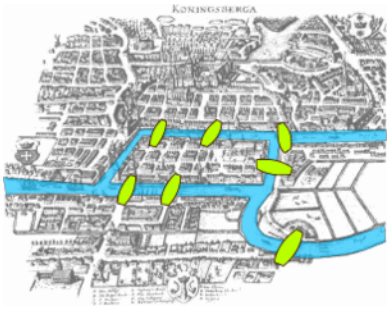


Figura 3.1: Un mapa de la ciudad de Königsberg, año 1750.

se puede. Euler resolvió el problema usando sucesiones de letras y abarcando todas las posibilidades y aunque él nunca uso una gráfica para modelar el problema, la manera en que resolvió el problema se considera como los antecedentes de la Teoría de las Gráficas. La representación del problema mediante una gráfica apareció muchos años después. En la figura 3.2, cada vértice (punto) representa una isla o una parte de tierra firme y las aristas (líneas) representan los puentes que hay entre dos partes de tierra (isla o tierra firme). Con un lenguaje coloquial, decimos que una gráfica/diagrama/dibujo es euleriana cuando podemos dibujarla de tal forma que recorremos cada línea exactamente una vez, sin levantar el lápiz del papel y además regresamos al punto inicial. O bien, una gráfica G tiene un *recorrido euleriano*, si podemos dibujar la gráfica G de tal forma que recorremos cada arista exactamente una vez y regresamos al vértice inicial. Una gráfica es euleriana si tiene un recorrido euleriano. Las gráficas eulerianos están caracterizadas (ver sección 3.4.2).

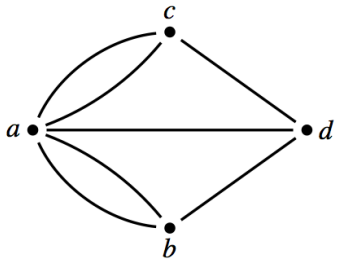


Figura 3.2: Una gráfica que modela los puentes de la ciudad de Königsberg.

3.0.2 El agente viajero.

En el siglo XIX el matemático W. R. Hamiltón inventó un juego de mesa sobre el dodecaedro (ver figura 3.3): Cada vértice del dodecaedro representa una ciudad de Europa y el juego consiste en recorrer cada una de las ciudades (es decir, cada vértice) sin visitar la misma ciudad dos veces. Sin embargo, el juego se vuelve muy aburrido en cuando un jugador encuentra un recorrido bueno, porque este mismo recorrido le sirve para cualquier asignación de ciudades. Los recorridos que pasa exactamente una vez por cada vértice y que regresa al vértice inicial se llaman *ciclos hamiltonianos* en honor a W. R. Hamiltón.

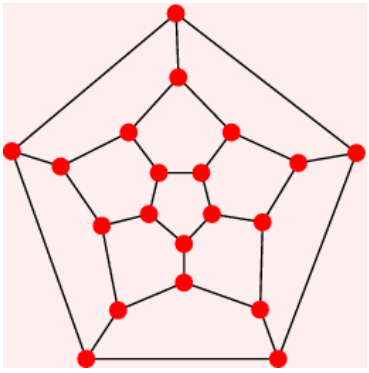


Figura 3.3: El dodecaedro.

El problema de determinar si una gráfica tiene un ciclo hamiltoniano es un problema *NP*-completo.[5] Se han determinado condiciones necesarias y condiciones suficientes, pero no se conoce ninguna caracterización de las gráficas que tienen un ciclo hamiltoniano (ver sección 3.4.2).

El problema del agente viajero generaliza el juego de Hamilton. Un agente de ventas debe visitar n ciudades sin repetir ninguna de ellas y quiere minimizar el costo del recorrido, el costo puede estar en términos del costo, la distancia o el tiempo. Con una gráfica se modela las ciudades y caminos. Los vértices de la gráfica son las ciudades y las aristas son los caminos entre las ciudades. A cada arista se le asigna el costo de recorrer el camino que representa la arista. El problema del agente viajero es estudiado tanto por su interés teórico como por sus aplicaciones. Es un problema que atrae a mucha gente porque tiene una formulación muy sencilla. Sin embargo, para entender la complejidad del problema se requiere una base sólida de Teoría de las Gráficas, Computación, así como Programación Lineal y Entera.

3.0.3 La fábrica de ladrillos

Durante la segunda guerra mundial, el matemático húngaro P. Turán realizó trabajos forzados en una fábrica de ladrillos. Los ladrillos se transportaban en trenes y cuando un tren pasaba por una intersección de dos vías de ferrocarril, se caían algunos ladrillos. Para evitar esta pérdida de material, se buscaba una manera de conectar los tres almacenes con cada una de las tres fábricas mediante v?as de ferrocarril sin que se intersectaran las vías. Turán se hizo la siguiente pregunta:

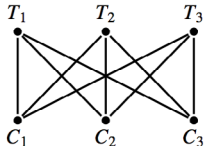
> ¿Cómo se puede conectar con vías de tren p fábricas a q bodegas, de manera que el número de cruces entre las vías sea el menor posible?

El problema fue planteado hace mas de 60 años, y aún sigue abierto, además dio origen al estudio del *número de cruces* de una gráfica, que es un tópico de la Teoría de las Gráficas que ha recibido mucha atensión en los últimos dos décadas por sus aplicaciones en el área

[5] Un problema es *NP*- completo si el probla de determinar si se cumple la propiedad o no, es equivalente a otro problema *NP*-completo para los problemas *NP*- completos no existe un algorítmo que en tiempo polinomial pueda determinarse si se cumple la propiedad o no.

de computación. Probablemente han escuchado el caso particular y popular del problema anterior.

En el pueblo San Juan hay tres tenditas que le llevan mercancía a tres de las casas del pueblo. Resulta que los tres repartidores (uno por cada tienda) están peleados entre sí y si se encuentran empiezan a pelear. ¿Puedes ubicar las tres casas y los tres servicios así como las rutas de los tres repartidores, de modo que las rutas no se intersectan? (Ver figura 3.4)



3.4: Una gráfica que modela el ejemplo de las tres casas y tres tenditas

Este problema está relacionado con tópicos importantes dentro de la Teoría de las Gráficas: las gráficas planas y el número de cruces. Decimos que una gráfica es plana, si está dibujada de manera que sus aristas no se cruzan. Una gráfica es aplanable si se puede dibujar de manera plana. Las gráficas que son planas (o en su caso aplanables) están caracterizadas (ver sección 3.4.1). El problema de las tres casas y tres tenditas es un problema de determinar si la gráfica que modela el problema es plana (aplanable) o no. Las gráficas planas son además las gráficas que nos interesan en el siguiente problema.

3.0.4 El Teorema de los cuatro colores

Los cartógrafos, que realizaban los mapas en el siglo XVIII, coloreaban los países (o regiones) de tal manera que a cada país le tocaba un solo color y a dos países con frontera común les tocaban colores distintos. Sabían que cualquier mapa lo podrían colorear de esta manera con a lo mas 4 colores, pero no podían explicar porqué. A cada mapa le asociamos una gráfica de la siguiente manera: a cada región y/o país del mapa se le asocia un vértice y dos vértices se unen por medio de una arista si las regiones que representan tienen frontera común. Dos países tiene frontera común si su frontera es no trivial. Las gráficas que obtenemos de esta manera las podemos dibujar de manera que sus aristas no se cruzan.

Teorema 3.0.1 (El Teorema de los Cuatro Colores)**.** *Los vértices de una gráfica plana se puede colorear con* 4 *colores de modo que dos vértices adyacentes sean de color distinto.*

El problema de los cuatro colores estuvo abierto por casi dos siglos. Durante los siglos XIX y XX hubo varias pruebas erróneas del Teorema de los Cuatro Colores, entre ellos Kempe (1879), Tait (1880), Heawood (1890), Veblen (1919),

Figura 3.5: Un mapa de México del siglo XVIII.

algunas pruebas hasta fueron aceptados y publicadas y no fue hasta después de varios años que alguién se percató del error en la prueba.

El teorema de los cuatro colores es el primer ejemplo de un teorema importante que se resolvió usando una computadora. En 1977 utilizaron una computadora para analizar los más de 1,000 casos. Después, un grupo de matemáticos (Robertson, Sanders, Seymour, Thomassen) probaron el teorema de los cuatro colores sin el uso de la computadora. Redujeron el número de casos que analizó la computadora al análisis de 633 casos, dando así una prueba matemática al Teorema 3.0.1. El siguiente resultado es una versión más debil de Teorema de los cuatro colores. La prueba es bonita, pero sale del objetivo del capítulo.

Teorema 3.0.2. *Los vértices de una gráfica plana se puede colorear con* 5 *colores de modo que dos vértices adyacentes sean de color distinto.*

3.0.5 Terminología y notación

En esta sección revisamos la terminología para establecer un lenguaje común. Una *gráfica* G es una pareja $(V(G), A(G))$, donde $V(G)$ es un conjunto finito de vértices (puntos, nodos) y $A(G)$ son las parejas o pares de una relación binaria llamada adyacencia. En el caso de que la relación es simétrica, el conjunto $A(G)$ es el conjunto de aristas (rayas, lineas) y decimos que G es una gráfica (sin dirección). Cuando la relación no es simétrica $A(G)$ es el conjunto de flechas de la gráfica y decimos que G es una digráfica. A menudo escribiremos solamente V y A para hacer referencia a al conjunto de vértices y aristas de una gráfica. Una **arista** es un subconjunto de orden 2 del conjunto de vértices. Dos vértices son **adyacentes** (o **vecinos**) si hay una arista entre ellos, es decir, los vértices $u, v \in V(G)$ son adyacentes si $\{u, v\} \in A(G)$ o simplemente $uv \in A(G)$ para simplificar la escritura. Una arista $a \in A(G)$ y un vértice $V \in V(G)$ son **incidente** si $a = \{u, v\}$ para algún vértice $u \in V(G)$. Una gráfica se puede visualizar representando cada vértice con un punto y cada arista con una curva/linea entre los dos vértices que definen la arista. Por ejemplo, sea $G(V, A)$ la gráfica con $V = \{a, b, c, d, e\}$ y $A = \{ab, bc, cd, de, ea, ac\}$. En la figura 3.6 se muestra una

representación de la gráfica G. Sea $U \subseteq V(G)$. Si no hay aristas entre los vértices

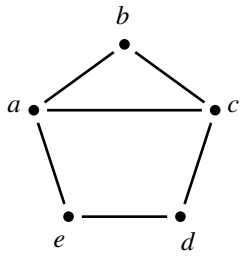


Figura 3.6: Una gráfica simple.

del conjunto U, decimos que U es un conjunto **independiente**. Cuando $\{u, v\} \in A(G)$ decimos que u y v son los vértices extremos de la arista $\{u, v\}$. Una arista cuyo vértice inicial coincide con su vértice final se llama un **lazo**. Una gráfica tiene **aristas multiples** si hay dos aristas distintas entre los mismos dos vértices, por ejemplo, en la gráfica de la figura 3.2 las aristas entre los vértices $\{a, c\}$ son aristas multiples. Una gráfica con aristas multiples es una **multigráfica**. Una gráfica sin lazos y sin aristas multiples se llama **gráfica simple**. En este trabajo se considerarán únicamente gráficas simples salvo cuando que se indica que la gráfica puede ser una muligráfica. La **vecindad** de un vértice $v \in V(G)$ es el conjunto de sus vecinos, es decir, de los vértices que son adyacentes al vértices v. A la vecindad de v la denotamos por $N(v)$, $N(v) = \{u : \{u, v\} \in A(G)\}$. El **grado** (o *valencia*), $d(v)$, de un vértice $v \in V(G)$ es $d(v) = |\{w : \{w, v\} \in A(G)\}| = |N(v)|$. Por ejemplo, en la figura 3.6, la vecindad del vértice a es $N(a) = \{b, c, e\}$, mientras la vecindad del vértices d es $N(d) = \{c, e\}$, y se tiene que $d(a) = 3$ y $d(d) = 2$.

Teorema 3.0.3. *Sea G una gráfica. Entonces*

$$\sum_{v \in V(G)} d(v) = 2|A(G)|.$$

Demostración. Ejercicio 3.7. □

Como consecuencia se tiene que la suma de los grados de los vértices de una gráfica es un número par.

Corolario 3.0.4. *El número de vértices de grado impar es un número par.*

Una gráfica H es una *subgráfica* de la gráfica G, si $V(H) \subseteq V(G)$ y $A(H) \subseteq A(G)$, (ver figura 3.7). Sea H una subgráfica de G, decimos que H es una subgráfica **generadora** de la gráfica G si $V(H) = V(G)$, en la figura 3.7, la gráfica G_2 es una subgráfica generadora de la gráfica G, mientras que la gráfica G_1 no lo es porque $e \in A(G)$, pero $e \notin A(G_1)$. Sea $V' \subseteq V(G)$. La subgráfica **inducida** por el conjunto V', denotada por $G[V']$, es la gráfica cuyo conjunto de vértices es V' y $\{v, w\} \in A(G[V'])$ si y sólo si $v, w \in V(G')$ y $\{v, w\} \in A(G)$, en

la figura 3.7, la gráfica G_3 es la subgráfica inducida por $\{a, b, c, e\}$ de la gráfica G, mientras que la gráfica G_1 no lo es porque $b, c \in V(H)$, $\{b, c\} \in A(G)$, pero $\{b, c\} \notin A(G)$. Si H es subgráfica de G, y $v \in V(H)$, entonces $N(v, H)$ denota la vecindad del vértice v restringida a la subgráfica H.

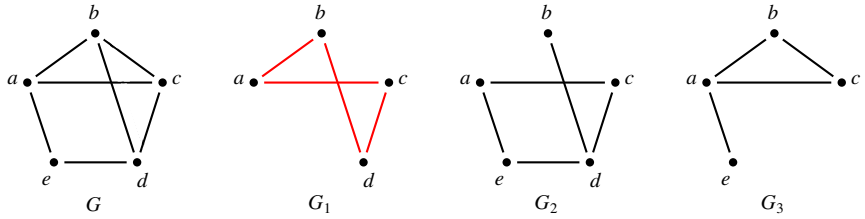


Figura 3.7: Las gráficas G_1, G_2, G_3 son subgráficas de la gráfica G.

Dada una gráfica G definimos el **complemento**, denotado por $\overline{G}$ de la gráfica G como (ver figura 3.6):

$$V(\overline{G}) = V(G)$$

$$A(\overline{G}) = \{\{u, v\} : u, v \in V(G) \text{ y } \{u, v\} \notin A(G)\}.$$

Nótese que si H es la gráfica con los mismos vértices de G y las aristas de H es la unión de las aristas de G y las aristas del complemento de G, entonces H es una gráfica completa.

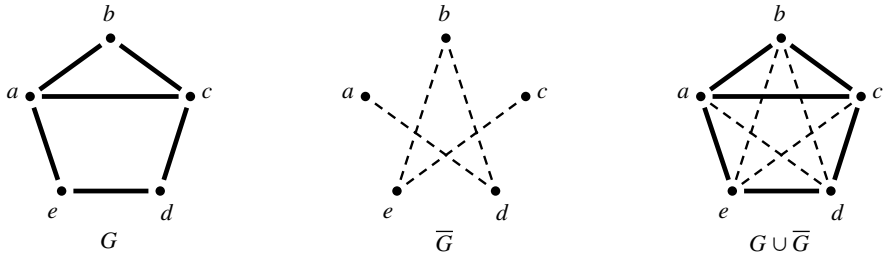


Figura 3.8: Una gráfica simple G, su complemento $\overline{G}$ y la unión de ellas.

Teorema 3.0.5. *En una gráfica siempre hay dos vértices del mismo grado.*

Demostración. Por el Principio del Palomar, notando que en una gráfica simple con n vértices, no puede haber un vértice de grado $n - 1$ y un vértice de grado 0. □

Teorema 3.0.6. *En una gráfica con* 6 *vértices hay un ciclo de longitud* 3 *o hay* 3 *vértices que son independientes.*

Demostración. Ejercicio 3.10. □

3.0.6 Ejercicios

Ejercicio 3.1. *Sea G una gráfica con* 17 *aristas y $d(v) \geq 3$ para todo $v \in V(G)$. ¿Cuál es el máximo número de vértices de la gráfica G?*

Ejercicio 3.2. *Sea G una gráfica conexa con* 6 *aristas y $d(u) = d(v) = d(w) = 3$ para $u, v, w \in V(G)$. ¿Cuál es el mínimo número de vértices de la gráfica G? Justifica tu respuesta.*

Ejercicio 3.3. *Construye todas las gráficas de orden* 4*. Para cada gráfica construye una sucesión (la* **sucesión de grados***) no decreciente con los grados de la gráfica. Trata de encontrar algún criterio para determinar si una gráfica se repite en tu lista. Justifica que tu lista es completa (deben ser* 11*), es decir, contiene todas las gráficas de orden* 4 *y no se repite ninguna.*

Ejercicio 3.4. *¿Puedes construir una gráfica con 5 vértices tal que la sucesión de los grados de la gráfica coincide con la sucesión de los grados del complemento de la gráfica? Contesta la misma pregunta para una gráfica con 6 vértices.*

Ejercicio 3.5. *Prueba que el corolario 3.0.4.*

Ejercicio 3.6. *En una reunión de cinco personas el número total de saludos de mano es un número par.*

Ejercicio 3.7. *Prueba el teorema 3.0.3.*

Ejercicio 3.8. *En una reunión de cinco personas siempre hay dos personas que saludan al mismo número de personas.*

Ejercicio 3.9. *Completa la prueba del teorema 3.0.5.*

Ejercicio 3.10. *En una reunión de seis personas siempre hay tres personas que se conocen entre sí o tres personas que no se conocen.*

3.1 Matrices para gráficas

Una gráfica G se puede representar mediante su dibujo o enlistando los vértices y las aristas, en este caso decimos que $G = (V(G), A(G))$ donde $V(G)$ es el conjunto de vértices de G y $A(G)$ es el conjunto de aristas de G.

Ejemplo 3.1.1. *La gráfica G de la figura 3.6 se puede representar como $G = (V(G), A(G))$ donde el conjunto de vértices es $V(G) = \{a, b, c, d, e\}$ y el conjunto de aristas es $A(G) = \{\{a, b\}, \{b, c\}, \{c, d\}, \{b, d\}, \{d, e\}, \{e, a\}\}$.*

Un dibujo de una gráfica es poco manejable en una computadora y las listas de los vértices y las aristas pueden ocupar mucho espacio si la gráfica tiene muchas aristas. A continuación vamos a exponer otras dos maneras de representar una gráfica mediante una matriz. Éstas dos maneras de representar una gráfica nos permiten estudiar propiedades de la gráfica usando álgebra lineal y en algunos resultan mas adecuadas para la implementación de algoritmos en programas.

3.1.1 Matriz de adyacencia

Sea G una gráfica con n vértices. La **matriz de adyacencia** de la gráfica G es una matriz $A_G = \{a_{i,j}\}$ con n renglones y n columnas donde cada entrada a_{ij} se define como

$$a_{i,j} = \begin{cases} 1 & \text{si } \{v_i, v_j\} \in A(G) \\ 0 & \text{en otro caso} \end{cases}$$

Por la definición de la matriz de adyacencia ésta es cuadrada y simétrica. La matriz de adyacencia de la gráfica de la figura 3.6 es

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

Nota que, la suma de los elementos de un renglón (o de una columna) es el grado del vértice correspondiente.

Es importante notar que la matriz de adyacencia (o incidencia) depende de la enumeración de los vértices (y de las aristas). Esto se refleja en el siguiente ejemplo.

Ejemplo 3.1.2. *Considera las gráficas G y G' en la figura 3.9. Las matrices de*

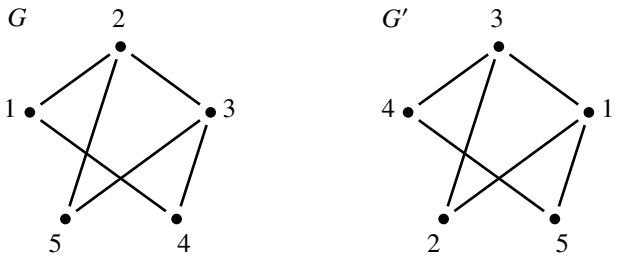


Figura 3.9: Las gráficas G y G' del ejemplo 3.1.2.

adyacencia de éstas gráficas son:

$$A_G = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix}, \qquad A_{G'} = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

En el ejemplo 3.1.3 exploramos la información que se puede extraer de la matriz de adyacencia al elevar la matriz a segunda, tercera y cuarta potencia.

Ejemplo 3.1.3. *La matriz de adyacencia de la gráfica G de la figura 3.9, así como la segunda, tercera y cuarta potencia de la matriz* A_G

$$A_G = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix}, \qquad (A_G)^2 = \begin{pmatrix} 2 & 0 & 2 & 0 & 1 \\ 0 & 3 & 1 & 2 & 1 \\ 2 & 1 & 3 & 0 & 1 \\ 0 & 2 & 0 & 2 & 1 \\ 1 & 1 & 1 & 1 & 2 \end{pmatrix}$$

$$(A_G)^3 = \begin{pmatrix} 0 & 5 & 1 & 4 & 2 \\ 5 & 2 & 6 & 1 & 4 \\ 1 & 6 & 2 & 5 & 4 \\ 4 & 1 & 5 & 0 & 2 \\ 2 & 4 & 4 & 2 & 2 \end{pmatrix}, \qquad (A_G)^4 = \begin{pmatrix} 9 & 3 & 11 & 1 & 6 \\ 3 & 15 & 7 & 11 & 8 \\ 11 & 7 & 15 & 3 & 8 \\ 1 & 11 & 3 & 9 & 6 \\ 6 & 8 & 8 & 6 & 8 \end{pmatrix}$$

¿Qué reflejan las entrada de la diagonal en cada una de las matrices?

Podemos observar que la entrada a_{ij}^k *de la k-ésima potencia de la matriz* A_G *indica el número de caminos de longitud k entre el vértice* v_i *y el vértice* v_j*. En* $(A_G)^2$*, la diagonal indica el grado de cada vértice (cada vecino de un vértice v aporta con exactamente un camino de longitud* 2 *de v a v) y, en* $(A_G)^3$ *la diagonal indica el doble del número de triángulos al que pertence cada vértice: para un vértice dado cada triángulo al que pertence se cuenta dos veces ya que el triángulo se puede recorrer de dos maneras, por ejemplo para el vértice* v_2*:* (v_2, v_3, v_5, v_2) *y* (v_2, v_5, v_3, v_2)*. Entre los vértices* v_2 *y* v_3 *hay seis caminos de longitud* 3 *y hay once caminos de longitud* 4 *entre los vértices* v_1 *y* v_3*.*

El estudio de las propiedades algebráicas de las matrices de gráficas es un área relativamente reciente, pero importante porque ofrece otro enfoque para estudiar propiedades de las gráficas. Para mayor información ver [1].

3.1.2 Matriz de incidencia

Sea G una gráfica con n vértices y m aristas. La **matriz de incidencencia** de la gráfica G es una matriz $I_G = \{b_{ij}\}$ con n renglones y m columnas donde cada entrada b_{ij} se define como

$$b_{i,j} = \begin{cases} 1 & \text{si el vértice } v_i \text{ incide en la arista } a_j \\ 0 & \text{en otro caso} \end{cases}$$

La matriz de adyacencia de la gráfica de la figura 3.6 es

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

Nota que, la suma de los elementos de un renglón es el grado del vértice correspondiente y como cada arista tiene dos vértices que inciden en ella, entonces la suma de los elementos de cualquier columna resulta 2.

La matriz de incidencia también contiene toda la información de la gráfica.

3.1.3 Ejercicios

Ejercicio 3.11. *Dibuja la gráfica H de la siguiente matriz de adyacencia:*

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

Ejercicio 3.12. *Considera la siguiente gráfica de la figura 3.10.*

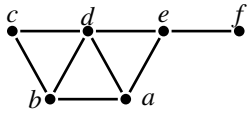


Figura 3.10: Figura del ejercicio 3.12.

1. *Calcula la matriz de adyacencia e incidencia.*
2. *Usa la matriz de adyacencia para calcular el número de triángulos.*
3. *Calcula el número de caminos del vértice a al vértice e de longitud a los mas* 4*. Escribe explícitamente todos estos caminos.*

Ejercicio 3.13.

Considera las siguientes matrices:

$$A = \begin{pmatrix} 0 & 2 & 0 & 1 & 0 \\ 2 & 0 & 1 & 1 & 2 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 3 \\ 0 & 2 & 0 & 3 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 2 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Para cada matriz explica si puede ser una matriz de adyacencia de una gráfica o no. En caso afirmativa construye la gráfica y determina si es una gráfica simple o no.

Ejercicio 3.14. *Considera las siguientes matrices de adyacencia:*

$$A = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 2 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Para cada matriz explica si puede ser una matriz de adyacencia de una gráfica o no. En caso afirmativa construye la gráfica y determina si es una gráfica simple o no.

Ejercicio 3.15. *Considera el ejemplo 3.1.3. Encuentra los seis caminos de longitud* 3 *que hay entre los vértices v_2 y v_3, así como los once caminos de longitud* 4 *entre los vértices v_1 y v_3.*

3.2 Gráficas dirigidas

La relación que define una arista en una gráfica es una relación simétrica. Sin embargo, hay problemas en los que la relación entre los objetos (vértices) no es una relación simétrica, por lo que no se pueden modelar mediante una gráfica. La relación que define una flecha en una gráfica dirigida es una relación asimétrica por lo que las gráficas dirigidas permiten modelar problemas importantes como: Flujo, Teoría de Decisiones, Dominación entre objetos o seres, Juegos NIM, Lógica, Asignación y Localización. Las gráficas dirigidas son una clase importante tanto por modelar una amplia gama de problemas como por su interés teórico. Para motivar la clase de las gráficas dirigidas vamos a revisar tres ejemplos: mapa con calles de un sólo sentído, torneo de tenis y la dominación entre especies de animales. Después formalizamos algunos conceptos y revisamos algunas aplicaciones del concepto de núcleo en gráficas dirigidas.

Mapa con calles de un sólo sentído

Considera el mapa de las calles de la figura 3.11. La gráfica asociada al mapa se construye tomando al conjunto de cruces de calles como conjunto de vértices y el conjunto de aristas es el conjunto de calles. Si algunas de las calles del mapa en la figura 3.11 tuvieran un sólo sentido y quisieramos representar el mapa con una gráfica, la gráfica no podría reflejar la información de la calle de un sólo sentido. Si quisiéramos usar la gráfica para encontrar un camino entre dos destinos, pudiera ser que el camino encontrado usara una calle en sentido contraria. Vamos a considerar el caso en que las calles tiene un sólo sentido, por ejemplo por ser calles estrechas en las que sólo cabe un coche o para hacer el

tránsito mas ágil. Para modelar esta situación representamos cada calle con una flecha, en lugar de una arista, la orientación del sentido de una calle de un sólo sentido (ver figura 3.11). En el caso de tener calles con doble sentido, se pueden representar mediante flechas simétricas o aristas.

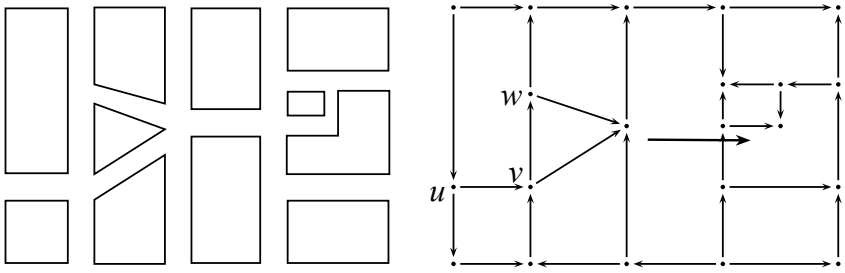


Figura 3.11: El mapa de una cuadra y la gráfica dirigida asociada.

En la figura 3.11 es importante observar que en el caso de los vértices u y v hay un camino de longitud 1 de u a v (pues esta la flecha (u, v)), pero el camino de regreso tiene longitud 3; mientras que para los vértices u y w hay una trayectoria de longitud 2 de u a w, pero no hay ninguna trayectoria de w a u. Así que la noción de "estar conectados" y la noción de distancia en una gráfica dirigida no son relaciones simétricas.

Torneo de tenis

En un deportivo se realiza un torneo de tenis entre 6 jugadores. Para simplificar denotamos a los jugadores por *a, b, c, d, e, f*. El jugador a sólo perdió contra el jugador b, el jugador b sólo perdió contra el jugador f, el jugador c le ganó a los jugadores e y f, el jugador d sólo perdió contra los jugadores a y b, los jugadores e y f sólo ganaron un juego. Para representar los resultados del torneo construimos una gráfica con 6 vértices $\{a, b, c, d, e, f\}$ y pondremos una flecha del vértice u al vértice v si el jugador u le ganó al jugador v.

En el torneo hay un empate entre los jugadores a y b, en ambos salen 4 flechas, del jugador c salen 3 flechas, de los jugadores d y f salen 2 flechas, mientras que del jugador e no sale ninguna ya que perdió todos sus juegos. Se pueden establecer diferentes criterios de desempate en términos de la estructura del torneo.

Dominación entre especies de animales

La cadena alimenticia es un ejemplo clásico de la noción de dominación en un ecosistema. En la biología el especie X domina al especie Y si los del especie X es alimento del especie Y, es decir el cazado (el alimento) domina al cazador

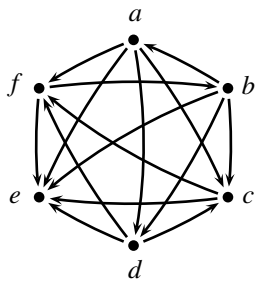


Figura 3.12: Torneo de tenis con 6 jugadores.

(quien necesita el alimento), por ejemplo, los antílopes dominan a los leones y los mosquitos dominan a las ranas. Si cada especie los representamos con un vértice, la flecha $u \to v$ significa que el vértice u es alimento del vértice v.

Se puede estudiar que tan vulnerable o estable es un ecosistema en términos de la digrfica (red) asociada a la cadena alimenticia, así como las causas y posibles efectos de la extinción de un especie.

Formalmente decimos que un conjunto H de vértices es dominante en la gráfica dirigida D, si para para todo vértice $v \in V(D) \setminus H$ existe un vértice $x \in H$ tal que $(x, v) \in A(D)$. Dominación en digráficas tiene aplicaciones en por ejemplo Teoría de las Desiciones, Informática, Modelado, Optimización Multiobjetivo.

Otra relación interesante en una red alimenticia es la relación de competencia. Decimos que dos epecies compiten si comparten el mismo alimento. Las gráficas de competencia así como algunas variaciaciones de ella tiene aplicaciones en ecología, en el estudio de comunicaciones en canales ruidosos, en la asignación de frecuencias para radio, y en modelado de sistemas complejos.

3.2.1 Definiciones básicas

A continuación vamos a revisar algunas propiedades que las gráficas y gráficas dirigidas tienen en común y algunas propiedades donde difieren. Una gráfica dirigida D es una pareja ordenada (V, F) donde V es el conjunto de vértices y F es el conjunto de flechas. Una flecha es una pareja ordenada de dos vértices distintos. Decimos que una flecha $(u, v) \in F(D)$ es **asimétrica** si $(v, u) \notin F(D)$, y es **simétrica** si $(v, u) \in F(D)$. Decimos que v es **exvecino** de u si $(u, v) \in F(D)$, en este caso u es **invecino** de v. La **exvecindad** de un vértice v es el conjunto de exvecinos y la **invecindad** es el conjunto de invecinos. El **exgrado** $d^+(v)$ el la cardinalidad de la exvecindad de v y el **ingrado** $d^-(v)$ el la cardinalidad de la invecindad de v. Los caminos, paseos, trayectorias, circuitos y ciclos son todos dirigidos, es decir $W = (u_0, u_1, \ldots, u_k)$ es un camino dirigido en D si $(u_i, u_{i+1}) \in F(D)$ para todo $0 \leq i \leq k - 1$.

Una gráfica dirigida es **fuertemente conexa** si entre cualquier par de vértices $u, v \in V(D)$ hay una uv-trayectoria y una vu-trayectoria. Una gráfica dirigida D es **débilmente conexa**, si entre cualquier par de vértices $u, v \in V(D)$ hay una uv-trayectoria o una vu-trayectoria (o ambos). La gráfica dirigida en la figura 3.12 no es fuertemente conexa porque no hay una trayectoria dirigida entre el vértice b y el vértice a.

Sea D una gráfica dirigida con n vértices. La **matriz de adyacencia** de la gráfica dirigida D es una matriz $A_D = \{a_{i,j}\}$ con n renglones y n columnas donde cada entrada a_{ij} se define como

$$a_{i,j} = \begin{cases} 1 & \text{si } v_i v_j \in F(D); \\ 0 & \text{en otro caso.} \end{cases}$$

Por la definición de la matriz de adyacencia de una digráfica dirigida es cuadrada, pero no necesariamente simétrica.

Ejemplo 3.2.1. *Considera la digráfica en la figura 3.13. La matriz de adyacencia*

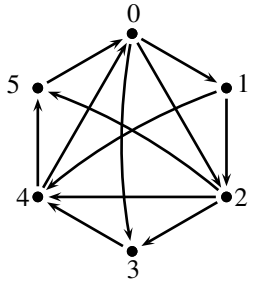


Figura 3.13: La digráfica D del ejemplo 3.2.1

de la digráfica es

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

Nota que, la suma de los elementos de un renglón es el número de flechas que salen del vértice mientras que la suma de los elementos de una columna es el número de flechas que entran al vértices, el ex-grado y el in-grado respectivamente del vértice correspondiente.

3.2.2 Núcleos en gráfica dirigida

El concepto de núcleo surge por primera vez en la rama de Teoría de Juegos con el nombre de *solución* y fue introducido por J. von Neumann and O. Morgenstern [14] en 1944, con el siguiente ejemplo.

Ejemplo 3.2.2 (Definición de solución)**.** *Dado n personas que deben discutir y elegir un elemento de un conjunto X (el conjunto X puede ser un conjunto de situaciones, de productos etc.). Es decir, las n personas tienen que elegir un elemento del conjunto no vacío X, para poder realizar esta elección, necesitan primero establecer una relación de preferencia entre algunos de los elementos de X (puede haber pares de elementos donde no hay preferencia entre ellos). Las preferencias individuales pueden no ser compatibles (es poco probable que todos estén de acuerdo), por lo que vamos a establecer una relación de preferencia "grupal".* En realidad, la importancia de la unanimidad es la capacidad de imponer o de obligar la preferencia de *a* sobre *b. Definimos la relación de* "preferencia grupal" *como la capacidad de un grupo de las n personas de convencer o imponer la preferencia de a sobre b.*

Considerar la digráfica cuyos vértices es el conjunto de situaciones X y las flechas son inducidas por la relación de preferencia grupal, es decir, si b es preferido grupalmente sobre a, entonces la flecha ab pertenece a la digráfica. Si la digráfica tiene un núcleo S (una solución), entonces la elección del elemento de X se restringe a la elección de un elemento dentro de S, ya que para cualquier elemento x fuera de S hay un elemento $s \in S$ tal que s es preferido sobre x.

Formalmente decimos que dada una digráfica D un subconjunto N de los vértices de D es un **núcleo** si es absorbente e independiente. Sea D una digráfica y U un conjunto de vértices de D. Decimos que U es **absorbente** si para todo $v \in V(D) \setminus U$ existe un vértices $u \in U$ tal que $vu \in F(D)$, y U es **independiente** si no hay flechas entre los vértices de U. El concepto de núcleo fue formalizado dentro de la teoría de las gráficas por Claude Berge como sigue: Un subconjunto N de los vértices de una digráfica D es un **núcleo** si satisface los siguientes dos

1. Para todo $u, v \in N$ se tiene que $(u, v), (v, u) \notin F(D)$.
2. Para todo $v \in V(D) \setminus N$ existe un vértice $x \in N$ tal que $(v, x) \in F(D)$.

No todas las gráficas dirigidas tiene núcleo, por ejemplo los ciclos impares no tiene núcleo y los ciclos pares sí tienen núcleo (ver figura 3.14).

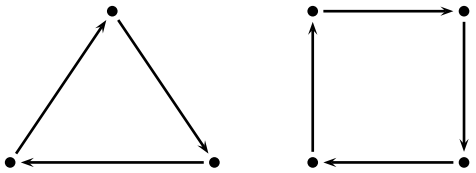


Figura 3.14: Una gráfica dirigida sin núcleo y una gráfica dirigida con núcleo.

Los núcleos tienen aplicaciones en diversas ramas tales como teoría de juegos, teoría de decisiones, lógica, autómatas. Revisamos una aplicación a la Teoría de Juegos.

Ejemplo 3.2.3 (Un juego NIM)**.** *Considera el siguiente juego de dos jugadores A y B sobre una gráfica dirigida D con algún vértice x inicial:*

El jugador A inicia eligiendo un vértice x_0 entre los exvecinos de x_1; luego el jugador B elige un vértice x_2 entre los exvecinos de x_1, y así sucesivamente. El jugador que elige un vértice que es un "pozo" (un vértice cuyo exgrado es cero) gana el juego porque el otro jugador ya no puede seguir jugando.

Si la gráfica dirigida no tiene pozos, el juego no termina nunca o si tiene ciclos/circuitos, entonces se puede extender por mucho tiempo. Se pueden a¿adir condiciones para que el juego siempre termine, por ejemplo determinar de antemano un entero positivo k, tal que si algún vértice haya sido elegido mas de k veces, entonces el juego se empata.

Sin embargo si la gráfica dirigida tiene un núcleo, hay una estratégia no perdedora.

Algoritmo Dijkstra

Vamos a considerar gráficas conexas con pesos en las aristas, decimos que $f : A(G) \to R$ es la función de peso de la gráfica G si $f(a)$ es el peso de la arista a para todo $a \in A(D)$. Si la gráfica no tiene pesos en las aristas, podemos considerar la función de peso $f(a) = 1$ para todo $a \in A(G)$. El algoritmo Dijkstra determina la distancia de un vértice fijo u a cualquier otro vértices de la gráfica.

Algoritmo 3.2.1 (Dijkstra)**.** *Dado una gráfica conexa G con pesos, con n vértices y un vértice $u \in V(G)$. Sea $U = (u = u_1, u_2, \ldots, u_n)$ una ordenación de los vértices de la gráfica G. El algoritmo Dijkstra construye un vector D con n entradas donde cada entrada d_i corresponde a la distancia entre u y el vértice u_i correspondiente. Antes de iniciar, se fija la entrada d_1 como 0 porque la distancia de u a u es 0 y cada una de las restantes entradas del vector D se fija con un número muy grande (por ejemplo $n \times e + 1$ donde e es el peso mayor de las aristas).*

1. *Sea $x = u$.*
2. *Revisamos todos los vecinos de x, excepto los vecinos marcados, y denotamos a los vértices no marcados por v_i.*
3. *Para el vértices actual x, calculamos la* distancia tentativa *a cada uno de sus vecinos v_i con la siguiente fórmula: $dt(v_i) = Dx + d(x, v_i)$, donde Dx denota la entrada correspondiente al vértice x en el vector D. Es decir, la distancia tentativa del vértice v_i es la distancia que tiene el vértice x en el vector D mas la distancia desde x al vértices v_i. Si la distancia tentativa es menor que la distancia almacenada en el vector D, actualizamos el vector con esta distancia tentativa. Es decir: Si $dt(v_i) < Dv_i$, entonces $Dv_i := dt(v_i)$.*
4. *Marcamos como completo el vértice x.*
5. *Tomamos como próximo vértice actual el vértice correspondiente a la entrada de menor valor en D (puede hacerse almacenando los valores en una cola de prioridad) y volvemos al paso 2 mientras existan vértices no marcados.*

Una vez terminado al algoritmo, todos los vértices están marcados y cada entrada de D refleja la distancia entre el vértice u y el vértice correspondiente.

El algoritmo de Dijkstra tiene muchas aplicaciones, como por ejemplo en la programación de tareas (ver proyectos en la sección 3.5).

3.2.3 Ejercicios

Ejercicio 3.16. *Dibuja todos los torneos con* 5 *vértices. ¿Cuántos son? ¿Cuántos tienen un ganador único? ¿Cuántos tienen un empate de dos, tres, cuatro o cinco jugadores?*

Ejercicio 3.17. *En un caso de empate en un torneo, propón un criterio de desempate y expresalo en términos del torneo.*

Ejercicio 3.18. *Busca en internet una digráfica asociada a una red alimenticia que contenga al menos 15 vértices. Caracterizar en térmnos de la digráfica los especies que son herbívoros, carnívoros o omnívoros. En términos de la digráfica, ¿cómo puedes determinar el número de presas y el número de depredadores de una especie?*

Ejercicio 3.19. *Para los ejercicios 3.13 y 3.14, considera las matrices que no pueden ser matrices de una gráfica y determina si pueden ser matrices de adyacencia de una digráfica. En caso afirmativa, construye la digráfica.*

Ejercicio 3.20. *Dada una digráfica asociada a una red alimenticia, investiga ¿cómo son los vértices que hacen vulnerables una red alimenticia? y ¿cómo puedes detectar que especies están en peligro de extinsión en términos de la digráfica?*

Ejercicio 3.21. *Justifica por qué un ciclo de longitud impar no tiene núcleo y justifica por qué un ciclo de longitud par sí tiene núcleo.*

Ejercicio 3.22. *Justifica por qué una digráfica sin ciclos siempre tiene núcleo.*

3.3 Isomorfismos e invariantes

Dos gráficas G y H son iguales si $V(G) = V(H)$ y $A(G) = A(H)$. Sin embargo, dos gráficas pueden tener exactamente la misma estrucura combinatoria y no ser iguales. Por ejemplo, las dos gráficas en la figura 3.15 no son iguales ya que $V(G_1) = \{a, b, c, d, e\}$ y $V(G_2) = \{x, y, z, w, u\}$, pero tienen la misma estructura combinatoria. En este caso diremos que no son iguales, pero si son isomorfas. Las propiedades que comparten gráficas isomorfas se llaman invariantes de gráficas.

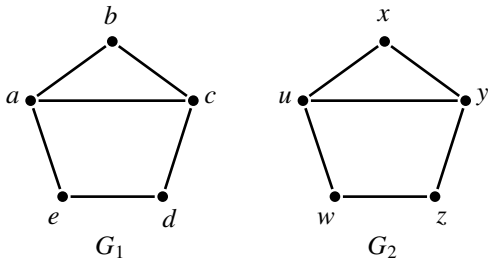


Figura 3.15: Dos gráficas isomorfas.

3.3.1 Isomorfismos

Dado dos gráficas G, H decimos que las dos gráficas son isomorfas si hay una función biyectiva $\varphi : V(G) \to V(H)$ entre los vértices de las gráficas tal que $\{u, v\} \in A(G)$ si y sólo si $\{\varphi(u), \varphi(v)\} \in A(H)$.

Determinar en general si dos gráficas son isomorfas es un problema *NP*-completo, es decir que no hay un algoritmo que en tiempo polinomial determina si dos gráficas son isomorfas o no.

Ejemplo 3.3.1. *Considera las gráficas de la figura 3.16 y, determina cuales de ellas son isomorfas.*

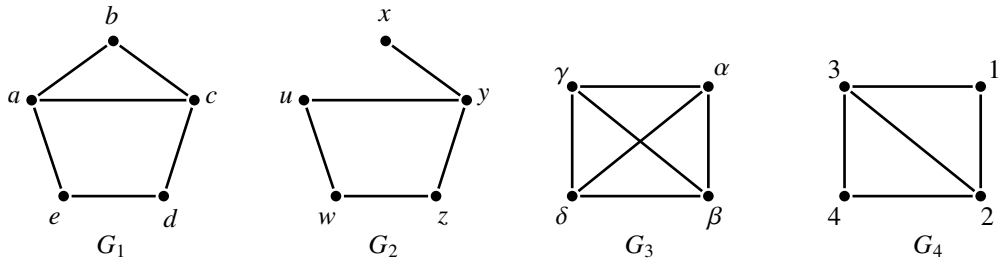


Figura 3.16: Las gráficas G_1, G_2, G_3 y G_4 del ejemplo 3.3.1.

La gráfica G_2 es la única que tiene un vértice de grado 1*, por lo que no es isomorfa a ninguna de la otras gráficas. La gráfica G_1 tiene* 5 *vértices mientras que las otras dos tiene* 4 *vértices, por lo que G_1 tampoco es isomorfa a ninguna de las otras gráficas. G_3 y G_4 ambos tienen* 4 *vértices pero G_3 tiene* 6 *aristas mientras que G_4 solo tiene* 5 *aristas. Por lo tanto ningún par de gráficas en la figura 3.16 son isomorfas.*

Ejemplo 3.3.2. *Considera las gráficas de la figura 3.17 y, determina cuales de ellas son isomorfas.*

Todas las gráficas tienen 6 *vértices y aristas y un vértice de grado* 1*. La gráfica G_2 es la únoca que tiene un vértice de grado* 4*, por lo que no es isomorfa a ninguna de la otras gráficas. Las de otras gráficas tienen dos vértices de grado*

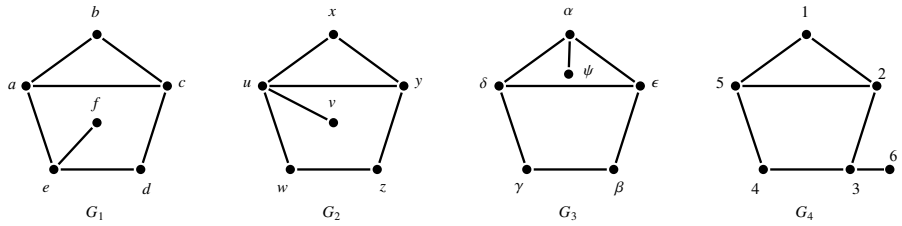


Figura 3.17: Las gráficas G_1, G_2, G_3 y G_4 del ejemplo 3.3.2.

a ninguna de la otras gráficas. Las de otras gráficas tienen dos vértices de grado 2 *y tres vértices de grado* 3*, pero en la gráfica* G_3 *los tres vértices de grado* 3 *son adyacentes entre si, los cual no pasa en las otras gráficas, por lo que* G_3 *tampoco es isomorfa a ninguna de las otras gráficas.*

Ahora consideramos las gráficas G_1 *y* G_4*. Si reflejamos la gráfica* G_4 *con respecto a una recta vertical que pasa por el vértice* 1 *(ver figura 3.18) y luego pasamos el vértice* 6 *adentro del ciclo* $(2, 3, 4, 5, 2)$ *obtenemos una copia de la gráfica* G_1 *pero con otros nombres de los vértices.*

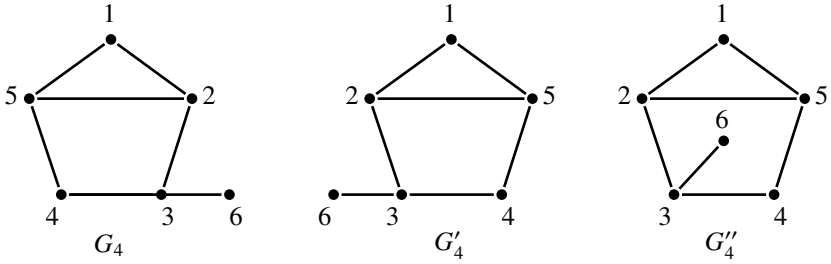


Figura 3.18: Como llevar paso a paso la gráfica G_4 a la gráfica G_1 en el ejemplo 3.3.2.

Usamos el dibujo de la gráfica G''_4 *en la figura 3.18, para encontrar un isomorfismo varphi de* G_4 *en* G_1 *sólo indicando la relación función biyectiva entre los vértices de* G_4 *y* G_1 *correspondiente. Así obtenemos que*

Cuadro 3.1: La regla de correspondencia del isomorfismo obtenido en ej ejemplo 3.3.2.

$v \in V(G_4)$	1	2	3	4	5	6
$\varphi(v) \in V(G_1)$	b	a	e	d	c	f

Por lo que G_1 *y* G_4 *son las únicas gráficas isomorfas en la figura 3.17.*

Ejemplo 3.3.3. *Considera las gráficas de la figura 3.28 y, determina cuales de ellas son isomorfas.*

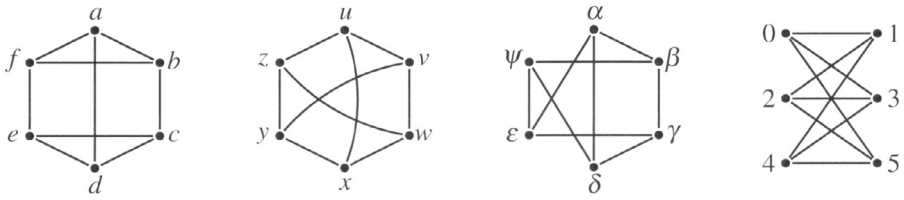


Figura 3.19: Gráficas 3-regulares con 6 vértices.

A menudo se puede encontrar la siguiente afirmación

$$G \cong H \text{ si } Ady(G) = Ady(H).$$

Es importante mencionar que es una condición suficiente pero no necesaria, las gráficas del ejemplo 3.1.2 son isomorfas, pero sus matrices de adyacencia no son iguales.

3.3.2 Invariantes de gráficas

Sean G y H dos gráficas isomorfas y $\varphi : V(G) \to V(H)$ un isomorfismo de G en H. Decimos que una propiedad se conserva bajo isomorfismo si siempre que G la satisface la propiedad $\varphi(G)$ también la satisface. Hay muchas propiedades que se conservan bajo isomorfismo, a estas propiedades se les llaman **invariantes de gráficas**. En los ejemplos 3.3.1, 3.3.2, 3.3.3 aparecen de manera natural algunos invariantes tales como el número de vértices, número de aristas, vértices de cierto grado, ciclos de de cierto longitud.

En la sección revisamos con mayor detalle los invariantes de planaridad, ciclos hamiltonianos y circuitos eulerianos que están enlistados en el siguiente ejemplo.

Ejemplo 3.3.4 (Invariantes de gráficas)**.** *Dadas dos gráficas isomorfas, las siguientes propiedades se conservan bajo isomorfismo*

i) *Número de vértices.*
ii) *Número de aristas.*
iii) *La sucesión de grados.*
iv) *Número de ciclos de longitud k.*
v) *Ser aplanable.*
vi) *Ser euleriana.*
vii) *Ser hamiltoniana.*

Todas ellas son condiciones necesarias, pero no suficientes, para que dos gráficas sean isomorfas. Esto significa que, si el número de vértices de dos

gráficas no coinciden estos no pueden ser isomorfas, o si una gráfica tiene triángulos y la otra gráfica no tiene triángulos, entonces éstas no son isomorfas, pero no es suficiente que dos gráficas tengan el mismo número de vértices para ser isomorfas, no que ambos tengan el mismo número de triángulos. Para probar que dos gráficas son isomorfas hay que encontrar el ismorfismo o bien el reacomodo de los vértices (como en el ejemplo 3.3.2), el reacomodo de los vértices indica cual es el isomorfismo. Un ejemplo de una propiedad que no es una invariante es que las aristas de la gráfica se crucen o no, por que depende del dibujo y no de la estructura combinatoria.

3.3.3 Ejercicios

Ejercicio 3.23. *Menciona alguna propiedad que **no** se conserva bajo isomorfismo (a parte de ser plana).*

Ejercicio 3.24. *Determina si las gráficas de las figuras 3.6 y 3.9 son isomorfas.*

Ejercicio 3.25. *Determina si las dos gráficas en la figura 3.20 son isomorfas.*

Ejercicio 3.26. *Considera las gráficas de la figura 3.21. Determina cuales de las siguientes parejas de gráficas isomorfas. En caso de ser isomorfas comprueba que la función que encontraste es un isomorfismo. En caso de no ser isomorfas justifícalo porque no lo son.*

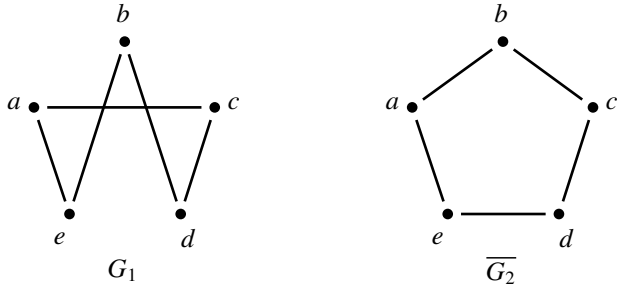


Figura 3.20: Las gráficas G_1 y G_2 del ejercicio 3.25.

3.4 Gráficas no dirigidas

En esta sección revisamos algunas situaciones y problemas que se pueden modelar mediante una gráfica. El objetivo de la sección es que el estudiante pueda resolver un problema usando las gráficas, es decir, construir una gráfica que refleja la situación descrita, expresar el problema en términos de la gráfica así como encontrar una solución en términos de la gráfica.

Ejemplo 3.4.1. *Cristina invita a cuatro personas a cenar a su casa. Ella quisiera que tanto ella como cada uno de sus invitados esté sentado entre dos personas a quienes conoce. La anfitriona Cristina conoce tanto a Isabella como a Alberto. Isabella y Mariana conocen tanto a Juan como a Alberto.*

Construye una gráfica que modele la situación y en términos de la gráfica conteste la siguiente pregunta ¿Se pueden sentar las cinco personas como quisiera Cristina?

En caso afirmativa solamente tenemos que proporciona el resultado en términos de la gráfca, en caso negativo justifica porqué no se puede.

Denotamos cada persona por la letra inicial de su nombre, $V(G) = \{A, C, I, J, M\}$ *y unimos dos vértices por una arista si las personas correspondientes se conocen y el conjunto de aristas es*

$$A(G) = \{\{C, A\}, \{C, I\}, \{C, J\}, \{C, M\}, \{A, I\}, \{A, M\}, \{I, J\}, \{J, M\}\}$$

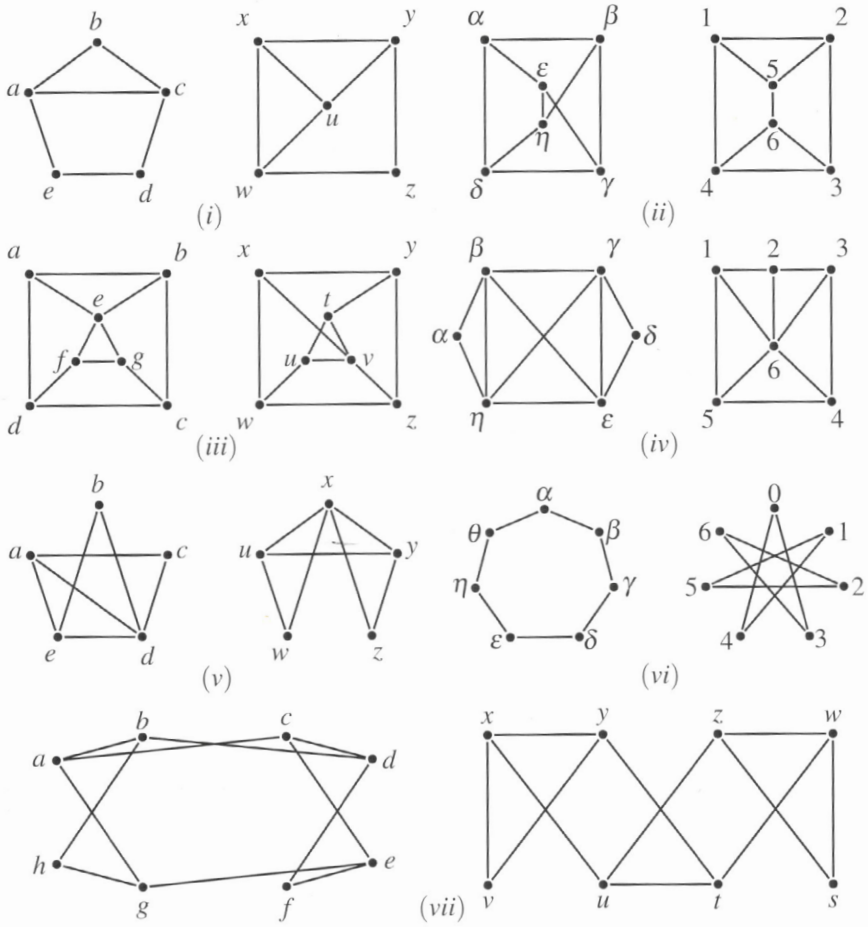


Figura 3.21. Las gráficas del ejercicio 3.26

La gráfica en la figura 3.22 modela esta situación y para acomodar a las personas alrededor de la mesa necesitamos un ***ciclo*** *de long* 5, (C, A, M, J, I, C).

Una manera de acomodar a las cinco personas alrededor de la mesa es: Cristina, Alberto, Mariana, Juan y Isabella.

Ejemplo 3.4.2. *Considera el mapa de las calles de la figura 3.23. La gráfica asociada al mapa se construye tomando al conjunto de cruces de calles como*

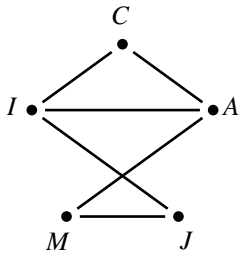


Figura 3.22: Una gráfica que modela el ejemplo 3.4.1.

conjunto de vértices y el conjunto de aristas es el conjunto de calles. Usando la gráfica podemos encontrar caminos entre diferentes destinos, determinar si se pueden recorrer todas la calles de la cuadra sin repetir ninguna (recorrido euleriano) para establecer una ruta para entregar de correspondencia o mercancía de la tienda de la esquina. A veces, el modelado de un problema nos obliga a considerar vértices y/o aristas con cierto peso. Por ejemplo, si queremos encontrar el camino mas corto entre dos destinos en un mapa, y conocemos la longitud de cada calle, podemos asignarle a cada arista la distancia correspondiente, y si queremos encontrar el camino mas rápido entre dos destinos en un mapa y un cruce tiene un semáforo que tarda un determinado tiempo, podemos asignarle tal tiempo al vértice. Hay algoritmos que nos permiten resolver problemas de rutas mas cortas o rutas mas largas, por ejemplo el algoritmo de Dijkstra.

3.4.1 Clases de gráficas

En esta sección revisamos las propiedades de algunas clases particulares de gráficas. Las clases de gráficas que vamos a considerar son: las gráficas completas, la gráfica nula, los ciclos, las gráficas bipartitas y las gráficas planas.

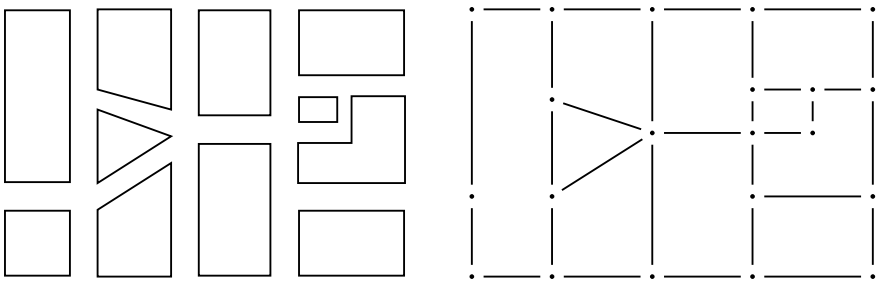


Figura 3.23: El mapa de una cuadra y la gráfica asociada.

Gráfica completa

La gráfica completa K_n es la gráfica con n vértices, donde cualquier par de vértices son adyacentes. Para la gráfica completa se tiene que $d(u) = n - 1$ para cualquier $u \in V(K_n)$.

Por teorema 3.4.7, K_n es una gráfica euleriana si y solo si $n \geq 3$ y $d(u) = n-1$ es un número par. Así que $n - 1 = 2m$ por lo que $n = 2m + 1 \geq 3$. En este caso $d(u) = 2m$ para cualquier $u \in V(K_n)$. Por teorema 3.4.11, toda gráfica completa K_n, con $n \geq 3$ es una gráfica hamiltoniana.

Gráfica nula

La gráfica nula con n vértices, $\overline{K_n}$, es la gráfica sin aristas, es decir, cualquier par de vértices son independientes. Como los vértices forman un conjunto independiente $d(u) = 0$ para cada $u \in V(\overline{K_n})$ y la gráfica no es ni euleriana ni hamiltoniana.

Ciclo

El ciclo C_n es la gráfica conexa con $n \geq 3$ vértices y n aristas, tal que las aristas inducen un ciclo. Para el ciclo C_n se tiene que $d(u) = 2$ para cualquier $u \in V(C_n)$. Por teorema 3.4.7, C_n es una gráfica euleriana y como C_n, con $n \geq 3$ es un ciclo hamiltoniano, entonces el ciclo C_n es una gráfica hamiltoniana.

Gráfica bipartita

Una gráfica G es bipartita si existe una partición de $V(G)$ en dos conjuntos de vértices independientes (cada clase induce una gráfica nula), es decir, si dos vértices están en la misma clase, entonces no hay arista entre ellos. La gráfica bipartita completa $K_{r,s}$ es la gráfica bipartita en que cada vértice de una parte es adyacente a todos los vértices de la otra parte.

Las gráficas bipartitas tienen una caracterización muy bonita.

Teorema 3.4.1. *Una gráfica G es bipartita si y solo si G no tiene ciclos de orden impar.*

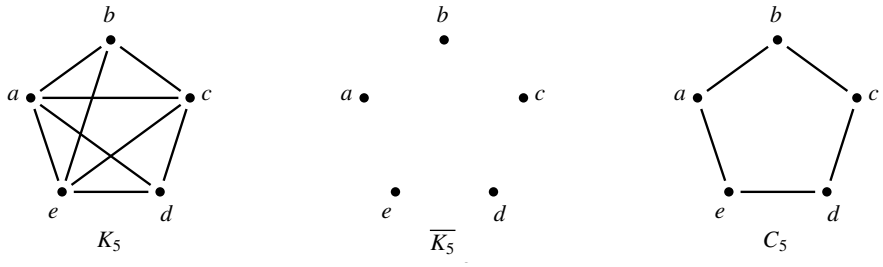


Figura 3.24: La gráfica K_5, la gráfica $\overline{K_5}$ y el ciclo C_5.

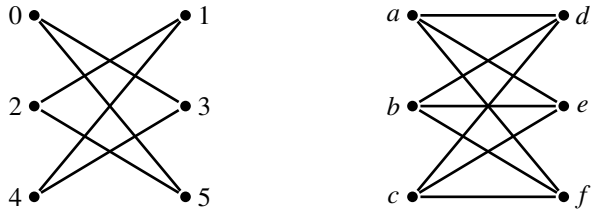


Figura 3.25: Una gráfica bipartita y la gráfica bipartita completa $K_{3,3}$.

Demostración. Ejercicio 3.35. □

Gráfica plana

Definición 3.4.2. *Una* **gráfica plana** *es una gráfica que se puede dibujar en el plano de modo que las aristas de la gráfica no se intersectan.*

En una revisión mas formal del tema de gráficas planas, se requiere contar con dos conceptos: gráficas planas (cuando la gráfica **está** dibujada de modo que las aristas de la gráfica no se intersectan) y gráficas aplanables (cuando la gráfica **se puede** dibujar de modo que las aristas de la gráfica no se intersectan), es decir, la planaridad depende del dibujo particular. Dada una gráfica plana G dibujada en el plano tal que sus aristas no se cruzan. Para un dibujo en particular, podemos considerar las regiones que encierran los ciclos de la gráfica, una región encerrada por un ciclo es una **cara** si el interior es vacío. En una gráfica plana finita hay exactamente una cara infinita, la exterior. Por ejemplo la gráfica de la figura 3.26 tiene 6 caras, (a, b, c, a), (b, c, d, b), (b, d, e, b), (d, e, f, d), (e, f, g, i, h, e) y la cara exterior $(a, c, d, f, g, i, h, e, b, a)$.

Observación 3.4.3. *Una gráfica conexa con una sóla cara no tiene ciclos. Si una gráfica conexa tiene al menos dos caras, entonces tiene al menos un ciclo.*

Para la prueba del siguiente teorema necesitamos un resultado básicos de árboles (gráficas acíclicas y conexas).

Teorema 3.4.4 (Caracterización de Euler)**.** *Dada una gráfica G conexa y plana con n vértices, m aristas y c caras se tiene que*

$$c = m - n + 2.$$

Demostración. Prueba por inducción sobre el número de caras.
Base: Si $c = 1$, entonces G es un árbol y $m = n - 1$ (ver teorema 4.1.3, sección 4.1), por lo que $m - n + 2 = (n - 1) - n + 2 = 1$, y el resultado es válido.
Hipótesis de Inducción: Sea $k \geq 2$. Supongamos que cualquier gráfica plana con $c \leq k - 1$ caras satisface que $c = m - n + 2$.

Paso Inductivo: Considera una gráfica plana G con k caras, n vértices y m aristas. Como G tiene al menos dos caras, entonces G no es árbol por la observación 3.4.3 y G tiene una arista a tal que $G - a$ es conexa. Sea $G' = G - a$; G' tiene n vértices, $m - 1$ aristas y $k - 1$ caras, por la *Hipótesis de Inducción* tenemos para la gráfica G' que $(m - 1) - n + 2 = k - 1$, simplificando queda $m - n + 2 = k$, por lo que la formula es válida para la gráfica G. Por el *Principio de Inducción Matemático* queda probado el teorema. □

Por ejemplo la gráfica de la figura 3.26 tiene 9 vértices, 13 aristas y 6 caras.

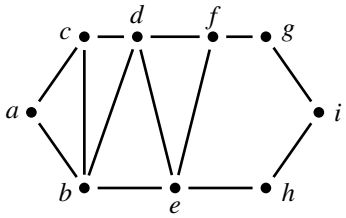


Figura 3.26: La gráfica H para los ejemplos de recorridos.

3.4.2 Recorridos en gráficas

La noción de recorrer una gráfica es muy natural e intuitivo. Un *camino* W en una gráfica G es una sucesión alternante de vértices y aristas de la gráfica G, con

$$W = (v_0, a_0, v_1, a_1, \ldots, v_n),$$

donde $a_i \in A(G)$, con $i = 0, 1, \ldots, n-1$ y $a_i = \{v_i, v_{i+1}\} \in A(G)$. Si G es una gráfica simple, denotaremos los caminos únicamente por su sucesión de vértices $(v_0, v_1, \ldots, v_n)$, un *paseo* en G es un camino en el que no se repiten aristas y una *trayectoria* en G es un camino en el que no se repiten vértices, a la trayectoria con n vértices la denotamos por P_n. El camino W es un *circuito* si $(v_0, v_1, \ldots, v_n)$ es un paseo y $v_0 = v_n$. El camino W es un *ciclo* si $(v_0, v_1, \ldots, v_{n-1})$ es una trayectoria y $v_0 = v_n$, al ciclo con n vértices lo denotamos por C_n. La *longitud* de un camino/paseo/trayectoria/ciclo W, $long(W)$, es el número de aristas de W, así $long(P_n) = n - 1$ y $long(C_n) = n$.

En la figura 3.26, el recorrido $(a, c, d, f, e, d, c, b, e)$ es un camino, pero no es un paseo porque repite la arista $\{c, d\}$, tampoco es una trayectoria porque repite el vértice c. El recorrido (a, c, d, b, e, d, f) es un camino y un paseo, pero no es una trayectoria porque repite el vértice d. El recorrido (a, c, d, b, e, h) es un camino, un paseo y una trayectoria porque no repite ningún vértice. De manera análoga tenemos que $(a, c, d, f, e, d, c, b, a)$ es un camino cerrado pues inicia y termina en el vértice a, pero no es ni circuito ni ciclo, porque repite la arista $\{c, d\}$ y así repite el vértice c. El camino cerrado (a, c, d, f, e, d, b, a) es un circuito, pero no es un ciclo porque repite el vértice d. El camino cerrado (a, c, d, b, a) es un ciclo y así también es un circuito. Una gráfica G es *acíclica* si no contiene ciclos.

Circuito euleriano

La figura 3.27 se conoce como la firma del diablo, porque no se puede hacer este dibujo sin repetir un segmento y sin levantar el lápiz de la hoja. Hoy en día resulta bastante natural preguntarse si un dibujo se puede realizar sin repetir un segmento, sin levantar el lápiz de la hoja y además regresar al punto de partida.

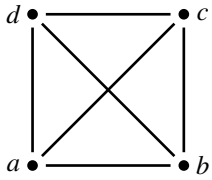


Figura 3.27: La firma del diablo.

El ejemplo de los Puentes de Königsberg, discutido en la sección 3.0.1, fue el primer ejemplo de la historia que se tiene del uso de una gráfica. Leonard Euler (ver p. 3.2) hizo un modelo (una gráfica) de esta situación y pidió en términos de la gráfica que ésta tuviera un recorrido que no repitiera aristas y que pasara por cada arista exactamente una vez. En honor al matemático Leonard Euler (1707 - 1783), padre de la teoría de las gráficas, éste tipo de recorridos recibieron el nombre de circuitos eulerianos.

Definición 3.4.5. *Dada una gráfica G, un* **circuito euleriano** *es un circuito que pasa exactamente una vez por cada una de las aristas de la gráfica. Decimos que una gráfica es euleriana si tiene un circuito euleriano.*

Definición 3.4.6. *Dada una gráfica G, un* **paseo euleriano** *es un paseo que pasa exactamente una vez por cada una de las aristas de la gráfica.*

Una gráfica euleriana tiene un paseo euleriano, pero una gráfica con un paseo euleriana no necesariamente es una gráfica euleriana.

Teorema 3.4.7 (Teorema de Euler)**.** *Una gráfica (posiblemente con aristas múltiples) conexa G tiene un recorrido euleriano si y solo si todos sus vértices tienen grado par.*

Demostración. Sea G una gráfica conexa con un circiuito euleriano W y sea $v \in V(G)$. Cada vez que el circuito W pasa por el vértice v llega al vértice v por una arista, digamos $\{u_1, v\}$, y sale del vértice v usando otra arista, digamos

$\{v, u_2\}$. Si el circuito W pasa k veces por el vértice v, entonces hay k aristas por las que se llega al vértice v, digamos $\{v_1, v_3, \ldots, v_{2k-1}\}$, y k aristas por las que sale del vértice v, digamos $\{v_2, v_4, \ldots, v_{2k}\}$, además, como W es un circuito euleriano, entonces los vértices del conjunto $\{v_1, v_2, \ldots, v_{2k}\}$ son distintos dos a dos y contiene a todos los vecinos de v, por lo tanto v tiene grado $2k$. Como el vértice v es un vértice cualquiera de la gráfica G, entonces todos los vértices tienen grado par.

Sea G una gráfica conexa tal que todos sus vértices tiene grado par. Sea $W = (v_1, v_2, \ldots, v_k, v_1)$ un circuito de longitud máxima en G. Supongamos que W no es euleriano, entonces $A(G) \setminus A(W) \neq \emptyset$. Como G es conexa, hay una arista a tal que $a = \{v_i, w\}$ para algún vértice $v_i \in V(W)$. Sea $G' = G - A(W)$, cada vértice en G' tiene grado par. Sea H la componente conexa que contiene la arista a. Sea C un circuito que contiene a la arista a, con $C = (v_i, w = w_0, w_1, \ldots, w_l = v_i)$, entonces

$$W' = (v_1, v_2, \ldots, v_i, w = w_0, w_1, \ldots, w_l = v_i, v_{i+1}, \ldots, v_k, v_1)$$

es un circuito de longitud mayor que W lo cual contradice la elección del circuito W. Por lo tanto W es un circiuito euleriano y hemos terminado. □

Teorema 3.4.8. *Una gráfica conexa (no necesariamente simple) tiene un paseo euleriano si y solamente si tiene a lo más dos vértices de grado impar.*

Demostración. Sea G una gráfica conexa. Si G no tiene vértices de grado impar, entonces G tiene un circuito euleriano que en particular es un paseo euleriano.

Si G tiene vértices de grado impar, entonces G tiene exactamente dos vértices de grado impar (por hipótesis y el Corolario 3.0.4). Sean $u, v \in V(G)$ tales que el grado de u y v es impar. Si $a = \{u, v\} \notin A(G)$, entonces todos los vértices de $G' = G \cup a$ tienen grado par y por el Teorema 3.4.7, G' tiene un circuito euleriano W. En este caso $W' = W - a$ es un paseo euleriano de G.

Asumimos que $a = \{u, v\} \in A(G)$. Sea $G' = G \cup a'$, donde $a' = \{u, v\} \notin A(G)$. Entonces todos los vértices de G' tienen grado par y por el Teorema 3.4.7, G' tiene un circuito eulerinao W. En este caso $W' = W - a$ es un paseo euleriano de G. □

Ejemplo 3.4.3. *Considera las gráficas de la figura 3.28. En la gráfica G_1 todos los vértices son de grado par por lo que tiene un circuito euleriano. En la gráfica G_2 los vértices u y x son los únicos vértices de grado impar, luego la gráfica G_2 tiene un paseo euleriano.*

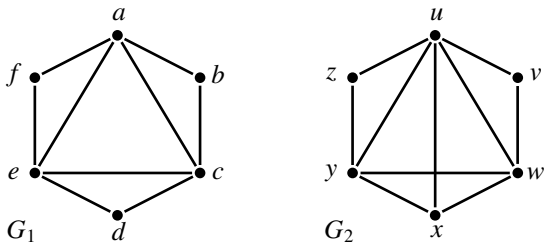


Figura 3.28: Las gráficas del ejemplo 3.4.3.

Aplicaciones

Supón que eres repartidor de correo y tienes que pasar por todas las casas de una ciudad, es decir que habrá que pasar al menos una vez por cada calle. Para minimizar el recorrido habrá que pasar el mínimo número de veces por cada calle. Representamos el sistema de calles con una gráfica como sigue: por cada intersección de calles pondremos un vértice y pondremos una arista entre dos vértices si hay una calle que conecta las intersecciones de calles correspondientes. Para recorrer cada calle habrá que encontrar un recorrido euleriano.

De la misma manera los recorridos eulerianos sirven para determinar rutas para patrullar las calles de una ciudad y rutas para lectura de electricidad/gas, etc.

Ciclo hamiltoniano

En el ejemplo del vendedor viajero discutido en la sección 3.0.2 se busca un recorrido que no repite vértices y que pasa por cada vértice una sóla vez. En honor al matemático William Rowan Hamilton (1805 – 1865) estos recorridos reciben el nombre de recorridos hamiltonianos o ciclos hamiltonianos.

Definición 3.4.9. *Un* **ciclo hamiltoniano** *es un ciclo que pasa una y solamente una vez por cada uno de los vértices de la gráfica. Decimos que una gráfica es hamiltoniana si tiene un ciclo hamiltoniano.*

Definición 3.4.10. *Una* **trayectoria hamiltoniana** *es una trayectoria que pasa una y solamente y vez por cada uno de los vértices de la gráfica.*

Nótese que una gráfica hamiltoniana tiene una trayectoria hamiltoniana, pero una gráfica con una trayectoria hamiltoniana no necesariamente es una gráfica hamiltoniana.

No se conoce ninguna caracterización de las gráficas hamiltonianas. Se conocen una gran cantidad de condiciones necesarias, y algunas condiciones suficientes.

Ejemplo 3.4.4. *Vamos a analizar la gráfica G de la figura 3.29 para determinar si tiene un ciclo hamiltoniano o no. Primero revisamos las propiedades de la*

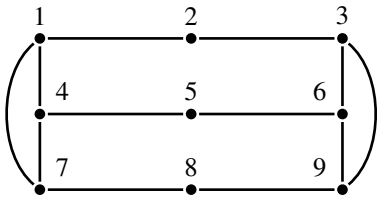


Figura 3.29: La gráfica del ejemplo 3.4.4.

gráfica: $|V(G)| = 9$, $|A(G)| = 12$. *Si G tiene un ciclo hamiltoniano, éste debe tener* 9 *aristas y debemos poder eliminar* 3 *aristas de la gráfica G tal que la gráfica resultante H es un ciclo de longitud* $|V(G)| = 9$. *Nótese que*

$$A(H) \subset A(G) \text{ y } |A(G) \setminus A(H)| = 3.$$

Por lo tanto, si hay vértices de grado 2, *entonces las aristas incidentes a estos vértices deben estar en la gráfica H, por lo que*

$$\{1,2\},\{2,3\},\{4,5\},\{5,6\},\{7,8\},\{8,9\} \in A(H).$$

Ahora, consideramos el conjunto de aristas $A = \{\{1,4\},\{4,7\},\{1,7\}\}$. *Si* $|A \cap A(H)| < 2$, *entonces, en la gráfica H se tiene que* $d(u) = 1$ *para algún* $u \in \{1,4,7\}$, *lo cual contradice que H es un ciclo. Por lo que* $|A \cap A(H)| \geq 2$. *En este caso* $d(u) = 3$ *para algún* $u \in \{1,4,7\}$, *lo cual contradice que H es un ciclo.*

Por lo anterior la gráfica G no tiene un ciclo de longitud 9 *como subgráfica y G resulta no hamiltoniana.*

La condición del teorema 3.4.11 es una condición suficiente, pero no es necesaria (ver ejercicio 3.51).

Teorema 3.4.11. *Sea G una gráfica de orden* $n \geq 3$. *Si* $d(v) \geq n/2$ *para todo vértice* $v \in V(G)$, *entonces G es hamiltoniana.*

Demostración. Prueba por reducción al absurdo.

Supongamos que existen gráficas con $n \geq 3$ vértices y grado mínimo $\delta \geq n/2$ que no son hamiltonianas. Sea G una gráfica con $n \geq 3$ vértices y grado mínimo $\delta \geq n/2$ maximal no hamiltoniana (si a¿adimos otra arista resulta hamiltoniana). Considera dos vértices no adyacentes u, v. Como G es maximal, entonces $G \cup uv$ sí es hamiltoniana y todo ciclo hamiltoniano de $G \cup uv$ contiene la arista uv y G tiene una trayectoria hamiltoniana (si hubiera un ciclo hamiltoniano C que no contiene la arista uv, entonces C sería un ciclo hamiltoniano de G). Sea $P = (u = v_1, v_2, \ldots, v_n = v)$ una trayectoria hamoiltoniana de G. Vamos a construir las siguientes dos conjuntos $S = \{v_i : \{v_i, v_n\} \in A(G)\}$, es decir S es el conjunto de vértices de P que son vecinos del vértice x_n y considera el conjunto $T = \{v_i \in$

$V(P) : \{v_{i+1}, v_1\} \in A(G)\}$, T es el conjunto de vértices de P tales que el siguiente vértice en la sucesión de vértices de la trayectoria P es vecino del vértice v_1. Si $S \cap T \neq \emptyset$ entonces hay un vértice v_i tal que las aristas $v_1v_{i+1}, v_iv_n \in A(G)$, en este caso $(v_1, v_{i+1}, v_{i+2}, v_n, v_i, v_{i-1}, v_{i-2}, v_1)$ es un ciclo hamiltoniano, lo cual contradice la elección de la gráfica G. Se sigue que $|S \cap T| = 0$.

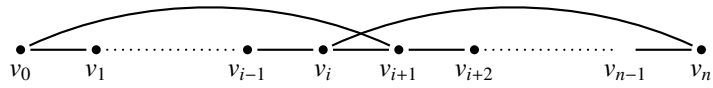


Figura 3.30: Construcción de un ciclo hamiltoniano.

Además $v_n \notin S \cup T$, por lo que $|S \cup T| < n$. Así tenemos que

$$d(u) + d(v) = |S| + |T| = |S \cup T| + |S \cap T| < n.$$

Por hipótesis $d(u), d(v) \geq n/2$ y $d(u)+d(v) \geq n$. Y hemos llegado a la contradiccción de $d(u) + d(v) < n$ y $d(u) + d(v) \geq n$.

Por lo tanto no existen gráficas con $n \geq 3$ vértices, grado mínimo $\delta \geq n/2$ que no son hamiltonianas. Y el resultado sigue. □

El problema del agente viajero

Supón que debes recorrer ciertos lugares de una ciudad (por ejemplo para repartir algún periódico a los vendedores en los semáforos) o estas planeando un viaje y quieres visitar ciertas ciudades. El "**costo**" de los recorridos entre los lugares se puede medir en términos del tiempo, distancia, costo etc.

Para resolver el problema le asignamos una gráfica $G = (V, A)$ donde conjunto de vértices representa los puntos o ciudades a visitar y las aristas las posibles conexiones y la función de pesos $\varphi : A(G) \to \mathbb{R}$ le asigna a cada arista el costo de recorrer el tramo correspondiente. El problema se transforma en encontrar un ciclo hamiltoniano de peso mínimo.

El problema del agente viajero (Salesmann) es una variación del problema de encontrar un ciclo hamiltoniano. En el problema del agente viajero consiste en encontrar un ciclo hamiltoniano de peso mínimo en una gráfica con una función de pesos $\varphi : A(G) \to \mathbb{R}$ y es un problema NP-completo, aunque existen algoritmos que encuentran soluciones buenas aunque no aseguran que la solución es óptima. El problema del agente viajero tiene aplicaciones en áreas tales como rutas para la entrega de mercancía, planificación, logística y en la fabricaci?n de microchips. Una versión modificada del problema del agente viajero tiene aplicaciones en la tareas de determinar la secuencia de ADN.

3.4.3 Ejercicios

Ejercicio 3.27. *Un químico va a empacar los químícos A, B, C, D, E, F y G. Quiere usar el menor número de cajas posible. Algunos quimicos no pueden ser empacados en la misma caja porque reaccionan entre sí. En particular cualesquiera dos de los químicos A, B, C y G reaccionan entre sí, además tanto A como E reaccionan con F y D. Usa una gráfica para describir la relación entre los químicos. Usa la gráfica para determinar el mínimo número de cajas que se requiere para empacar los químicos.*

Ejercicio 3.28. *Susana invita a sus amigas María, Patricia, Nadyelli y Alicia a un reunión en su casa. Prepara tortas para la reunion: una de atún, una de jamón, dos de pavo y una de pollo. A María le gustan las tortas de pollo, a Patricia las de pollo y las de jamón, Nadyelli prefiere las de pavo y las de atún, Alicia prefiere las de atún y pavo y a Susana le gustan las tortas de Pollo, atún y jamón.*
¿Será posible que cada una de las invitada puedan comer una torta que le gusta?.

Ejercicio 3.29. *En un mini Zoológico hay antílopes A, jirafas J, focas F, hipopótamos H, pingüinos P y un Tigre de Bengala T. Los antílopes y las jirafas no pueden compartir jaula con los hipopótamos y lo tigres no pueden compartir jaula con ningún otro animal.*
Construya una gráfica que modela esta situación y usa la gráfica para determinar cuál es el mínimo número de jaulas que se necesita para el mini zoológico.
Indica la relación que determinan las adyacencias y explica cómo usaste la gráfica para determinar la solución (Indíca claramente cuales son las características y/o propiedades que le buscas en término de la gráfica para encontrar una solución).

Ejercicio 3.30. *Representa mediante una gráfica el organigrama de la unidad Cuajimalpa.*

Ejercicio 3.31. *Encuentra una "buena" coloración del mapa de la República Mexicana.*

Ejercicio 3.32. *Calcula el número de aristas de una gráfica completa con n vértices.*

Ejercicio 3.33. *Una gráfica conexa G es un ciclo si y solo si $d(v) = 2$ para todo $v \in V(G)$.*

Ejercicio 3.34. *Una gráfica G es bipartita si y solo si G no tiene ciclos de orden impar.*

Ejercicio 3.35. *Una gráfica G es bipartita si y solo si los vértices de G se pueden colorear con dos colores tal que no hay vértices adyacentes del mismo color.*

Ejercicio 3.36. *Cuál es el máximo número de aristas en una gráfica bipartita.*

Ejercicio 3.37. *Si se elimina una arista de cada una de las gráficas $K_{3,3}$ y K_5, entonces ellas son planas.*

Ejercicio 3.38. *Investiga cuales son los sólidos platónicos. ¿Son gráficas planas?*

Ejercicio 3.39. *En la gráfica G de la figura 3.6 encuentra un camino que no es paseo y un paseo que no es trayectoria.*

Definición 3.4.12. *Decimos que una gráfica es* **conexa** *si hay un camino entre cualquier par de vértices de la gráfica.*

Ejercicio 3.40. *Una gráfica es conexa si y solo si hay una trayectoria entre cualquier par de vértices de la gráfica.*

Ejercicio 3.41. *Una gráfica conexa con grado mínimo δ tiene una trayectoria de longitud al menos δ y un ciclo de longitud al menos $\delta + 1$.*

Ejercicio 3.42. *Explica con tus propias palabras cuando una gráfica es euleriana.*

Ejercicio 3.43. *Menciona un criterio para determinar si una gráfica es euleriana (la definición no es un criterio).*

Ejercicio 3.44. *Sea G una gráfica conexa y euleriana con 28 aristas. Si $d(v) > 3$ para todo $v \in V$, ¿qué puedes afirmar con respecto al número de vértices?*

Ejercicio 3.45. *Sea $A = \{a, b, c, d, e\}$ un conjunto. Definimos los vértices de la gráfica G como el conjunto de subconjuntos de orden 2 del conjunto A, y definimos las aristas de la gráfica como las parejas de 2-conjuntos ajenos. Construye la gráfica y determina si es euleriana: en caso afirmativo muestra el circuito euleriano, en caso contrario explica por qué no es euleriano. Si no es una gráfica euleriana, determina si tiene un paseo euleriano: en caso afirmativo muestra el paseo euleriano, en caso contrario explica por qué no tiene un paseo euleriano.*

Ejercicio 3.46. *¿Cuáles de los sólidos platónicos son gráficas eulerianas? Si no es euleriana, ¿tiene un paseo euleriano? ¡Justifíca cada una de tu respuestas!*

Ejercicio 3.47. *Construye todas las gráficas eulerianas con 10 aristas que:*

1. *Son regulares.*
2. *Tienen exactamente dos vértices de grado dos y todos los demas vértices tienen en mismo grado*

Ejercicio 3.48. *Considera las gráficas de la figura 3.31. Determina cuales son gráficas eulerianas. Las gráficas que no son eulerianas, ¿tienen un paseo euleriano? ¡Justifíca cada una de tu respuestas!*

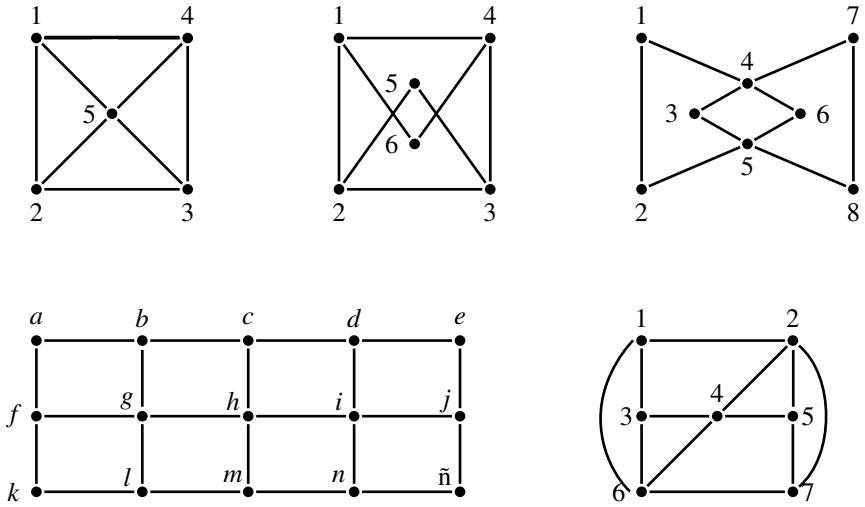


Figura 3.31: Las gráficas de los ejercicios 3.48, 3.49.

Ejercicio 3.49. *Considera las gráficas de los ejecicios 3.47, 3.45 y de la figura 3.31. Determina cuales son gráficas hamiltonianas. En caso de no ser una gráfica hamiltoniana, ¿tiene una trayectoria hamiltoniana? ¡Justifíca cada una de tu respuestas!*

Ejercicio 3.50. *Para cada inciso, encuentra una gráfica que:*

i) *es hamiltoniana y euleriana,*

ii) *es hamiltoniana pero no euleriana,*

iii) *es euleriana pero no hamiltoniana,*

iv) *no es hamiltoniana y tampoco euleriana,*

Ejercicio 3.51. *Encuentra una gráfica que es hamiltoniana, pero no satisface la condición (sufuciente) del teorema 3.4.11.*

Ejercicio 3.52. *¿Considera las gráficas de la figura 3.32, ¿son hamiltonianas?*

Ejercicio 3.53. *Supón que eres vigilante de un museo y en tu turno de vigilancia tienes que recorrer todas las salas. Para minimizar el recorrido habrá que pasar el mínimo número de veces por cada sala. ¿Cómo puedes representar éste problema con una gráfica y qué le pides a la solución en términos de la gráfica?*

Ejercicio 3.54. *Considera los dos planos de casas de un solo piso, con un jardin que las rodea, figura 3.33. Para cada plano construya una gráfica que refleja el problema y contestar las siguientes preguntas en términos de la gráfica*:

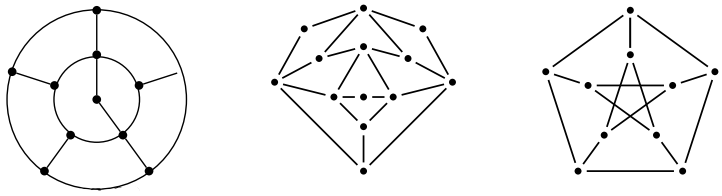


Figura 3.32: Las gráficas del ejercicio 3.52.

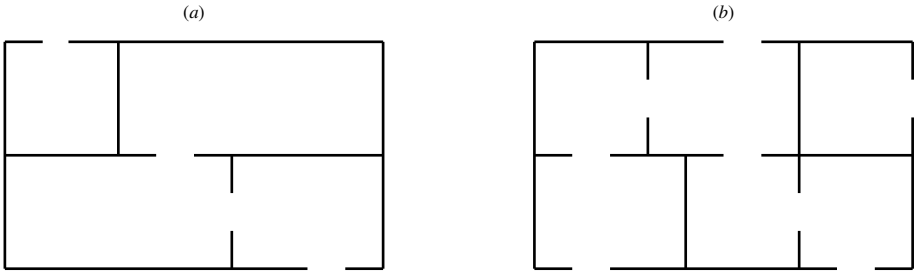


Figura 3.33 Los dos planos de las casas del ejercicio 3.54.

i) *Se puede hacer un recorrido de modo que pasamos por todas las puertas, sin pasar por la misma puerta dos veces y regresar al punto de partida.*

ii) *Se puede hacer un recorrido de modo que pasamos por todas las puertas, sin pasar por la misma puerta dos veces sin importar regresar al punto de partida.*

iii) *Se puede hacer un recorrido de modo que pasamos por todos los cuartos y por el jardin sin pasar por el misma cuartos ni por el jardin dos veces y regresar al punto de partida.*

iv) *Se puede hacer un recorrido de modo que pasamos por todos los cuartos y por el jardin sin pasar por el misma cuartos ni por el jardin dos veces sin importar regresar al punto de partida.*

v) *Sea G la gráfica que encontraron. ¿Es la gráfica G plana?, ¿Es la gráfica G bipartita?*

Ejercicio 3.55. *En la figura 3.34 se encuentra el plano de un museo de historia natural. Construyan una gráfica que refleja el problema y contesta las siguientes preguntas en términos de la gráfica:*

i) *Se puede recorrer el museo pasando por todas las puertas del museo, sin*

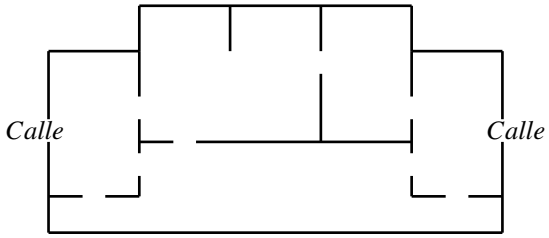


Figura 3.34: Plano del museo de historia natural del ejercicio 3.55.

ii) *Se puede recorrer todas las salas del museo, sin pasar dos veces por la misma sala iniciando en la calle y terminando en la calle.*

iii) *Sea G la gráfica que encontraron. ¿Es la gráfica G plana?, ¿Es la gráfica G bipartita?*

3.5 Proyectos

Distancias en gráficas y el algoritmo de Dijkstra.

Se pueden definir diferentes métricas en gráficas. Considerar la función

$$d(x, y) = \text{mín}\{long(P) : P\ es\ una\ uv - trayectoria\}.$$

La función d $(x; y)$ le asigna a cada par de vértices la longitud de la trayectoria mas corta entre ellos. Prueba que d $(x; y)$ es una métrica.

Define las conceptos excentricidad, radio, diámetro y centro en gráficas y traza analogías con las definiciones correspondientes en la geometría. Analiza y explica tres aplicaciones de los conceptos definidos en áreas distintos del conocimiento.

Para mayor información ver sección 9.7 [11] y [6].

Teoría de juegos

Supón que n personas deben elegir un elemento x del conjunto X. El conjunto X puede constar de diferentes situaciones. Las n personas deben establecer cuales son las preferencias de algunas situaciones de X sobre las demás. Rara vez están todos de acuerdo en elegir una misma situación,aunque sería el mejor escenario posible. Por eso lo que se considera es, mas bien, que un subconjunto de las n personas pueden imponer la preferencia de x sobre y, y lo llamamos

preferencia efectiva. Si definimos la gráfica dirigida D, cuyos vértices son los elementos de X, y las flechas son inducidas de manera natural por la relación de preferencia efectiva, es decir, si x es efectivamente preferido sobre y, entonces $y \rightarrow x$, es decir, $(y; x) \in F(D)$. Si una gráfica dirigida D tiene núcleo, basta elegir un elemento del núcleo.

El juego de *NIM* tiene sus antecedentes en el juego antiguo chino llamada Fan Tan; el primer registro en matemáticas de juegos de *NIM* fue Bouton quien precisamente generalizó el juego Fan Tan. Hoy en día hay muchos ejemplos de juegos *NIM* en la literatura de las matemáticas.

Leer, entender y explicar la nota "*poisoned cooky*" en [3].

Algoritmo de Dijkstra y programación de tareas

En un proyecto grande con muchas tareas, se puede perder mucho tiempo y dinero si no se programan bien las tareas que se van a realizar. Si algunas tareas se entrelazan y algunas pueden ser realizados simultáneamente mientras otros tienen un orden preestablecido, tal programación puede resultar complicada. pero se puede modelar mediante una gráfica dirigida. Por ejemplo, en la construcción de un edificio, la instalación de los bajos no pueden empezar hasta que está terminado la instalación de tuberías. El objetivo de modelar la programación de tareas mediante una gráfica dirigida es poder minimizar el tiempo que se tarda en completar el proyecto y además detectar las tareas que deban ser prioridad para que el proyecto termine a tiempo.

En el método llamado método de trayectoria crítica, se conoce el tiempo en que se realiza cada actividad y la única herramienta que se requiere es el algoritmo de Dijkstra y un algoritmo modificado del algoritmo de Dijkstra.

Explica como funciona el algoritmo de Dijkstra y explica su aplicación al método de trayectoria crítica mediante un ejemplo particular. Para mayor información ver sección 12.4 [10].

4 Introducción a los Árboles

Los árboles juegan un papel fundamental en el estudio de redes conexas, son importantes para entender la estructura de una gráfica y para los algoritmos que procesan información. Para el último caso es importante determinar la mejor forma de almacenar la información y en muchos casos la mejor forma tiene estructura de árbol. Además, los árboles tienen aplicaciones en áreas como conteo, teoría de desición, estructura de datos, ordenamiento, la teoría de la codificación, problemas de optimización, ordenar y relacionar datos en bases de datos etc.

Iniciamos con algunas aplicaciones de los árboles usando un lenguaje intuitivo.

Definición 4.0.1. *Una gráfica G es un* **árbol** *si G es acíclica y conexa.*

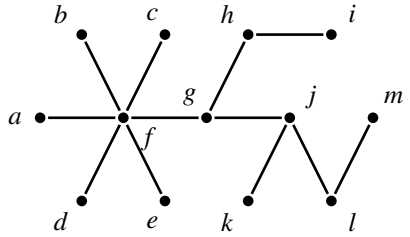


Figura 4.1: Un árbol con 13 vértices.

Ejemplo 4.0.1. *Organigrama (relación jerárquica).*

Ejemplo 4.0.2. *Liguilla del fútbol Mexicano: Clausura 2011 (ver figura 4.2).*

4.1 Terminología y Caracterización

En esta sección revisamos algunas propiedades y caracterizaciones de árboles. La prueba de algunas propiedades se deja como ejercicio. Sea G una grafica´. Decimos que $v \in V(G)$ es una **hoja** si $d(v) = 1$ y decimos que $v \in V(G)$ es un **vértice de corte** si $G - v$ tiene mas componentes conexas que G (si G es conexa $G - v$ no es conexa). Decimos que una arista $e \in A(G)$ es un **puente** si $G - e$ tiene mas componentes conexas que G (si G es conexa $G - a$ no es conexa).

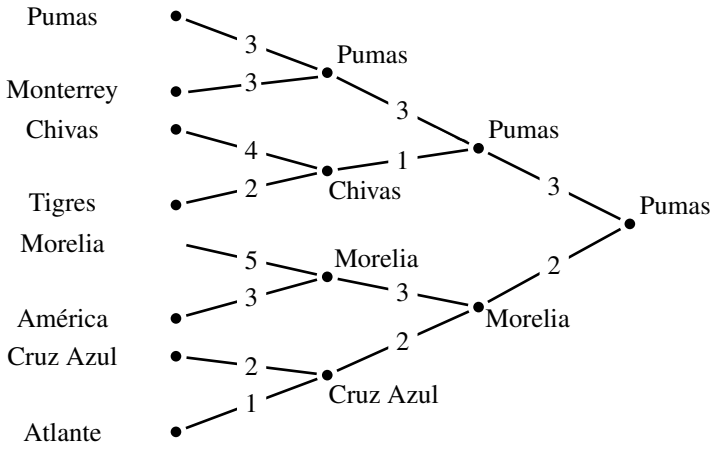


Figura 4.2: Ligilla de futbol - apertura 2011.

Proposición 4.1.1. *Toda arista en un árbol T es un puente de T.*

Demostración. Sea $a = \{u, v\}$ una arista del árbol T. Si a no es puente de T, entonces hay una trayectoria P entre el vértice u y el vértice v. Sea $P = (u = u_0, u_1, \ldots, u_n = v)$. Entonces, si le pegamos la arista a a la trayectoria P, obtenemos el ciclo $C = (u = u_0, u_1, \ldots, u_n = v, u)$, lo cual contradice que T es acíclica. Por lo tanto, toda arista en un árbol T es un puente de T. □

Proposición 4.1.2. *Sea T en un árbol. Entre cualquier par de vértices $u, v \in V(T)$ hay una única trayectoria.*

Demostración. Sean $u, v \in V(T)$ tale que hay dos uv-trayectorias P, P'. Como P, P' son dos trayectorias diferntes, entonces podemos asumir que hay una arista a en $A(P) - A(P')$. La arista a no es puente lo cual contradice la proposición 4.1.1. □

Teorema 4.1.3. *Sea $T = (V, A)$ un árbol con n vértices. Entonces T tiene $n - 1$ aristas.*

Demostración. Prueba por inducción matemática sobre el número de vértices del árbol.

Base:
Sea G un árbol con un solo vértice. Claramente G no tiene arista. Por lo que $n = 1$ y $m = 0$. Sea G un árbol con dos vértices. Claramente G tiene una sola arista. Por lo que $n = 2$ y $m = 1$. En ambos casos, G satisface el teorema.
Hipótesis de inducción:
Sea G es un árbol con k vértices, $k \in \{1, 2, \ldots, n-1\}$. Entonces G tiene $k - 1$ aristas.
Paso inductivo:
Sea G un árbol con n vértices. Pd. G tiene $n - 1$ aristas. Sea $a = \{u, v\}$ una arista de G. Por la Proposición 4.1.1, $G - a$ no es conexa, mas aún $G - a$ es la unión de dos árboles G_u, G_v tales que $u \in V(G_u)$ y $v \in V(G_v)$. Sea $n_u = |V(G_u)|$ y $n_v = |V(G_v)|$. Cada árbol G_u, G_v tiene a lo mas n vértices. Entonces por la hipótesis de inducción G_u, G_v tiene $n_u - 1$ y $n_v - 1$ aristas respectivamente.

El número de vértices de G es la suma de los vértices de G_u y G_v. Así $n = n_u + n_v$.

El número de aristas de G es la suma de las aristas de G_u y G_v mas 1 (la arista a). Así

$$|A(G)| = (n_u - 1) + (n_v - 1) + 1 = (n_u + n_v) - 1 = n - 1.$$

Por el principio de inducción matemática generalizada hemos probado que un árbol T con n vértices tiene $n - 1$ aristas. □

Teorema 4.1.4. *Sea G una grafica con n vértices y m = n − 1 aristas, entonces las siguientes afirmaciones son equivalentes.*

1. *G es un árbol.*
2. *G es conexa.*
3. *G es acíclica.*

Demostración. Probamos que 1. ⇒ 2., 2. ⇒ 3. y 3. ⇒ 1.

Las implicaciones 1. ⇒ 2. y 1. ⇒ 3. y 2. ∧ 3. ⇒ 1. se cumplen por definición.

Vamos a probar que 2. ⇒ 3. Sea G una grafica conexa con n vértices y $m = n - 1$ aristas. Vamos a probar que G es acíclica.

Procedemos por contradicción, suponiendo que G tiene un ciclo C de longitud k, entonces C contiene k vértices y k aristas. Para cada vértice $v \in V(G) \setminus V(C)$ hay una trayectoria de v al ciclo C considera P_v una trayectoria de longitud mínima del vértice v al ciclo C con $P_v = (v = v_0, v_1, \ldots, v_l)$ con $v_l \in V(C)$. Las arista $\{v, v_1\}$ son distintos dos a dos por lo que $m \geq n$, una contradicción con la hipótesis de que $m = n - 1$.

Para terminar probamos que 3. ⇒ 1. Sea G una grafica acíclica con n vértices y $m = n - 1$ aristas. Vamos a probar que G es conexa. Procedemos por contradicción, suponiendo que G tiene $k \geq 2$ componentes conexas $C_1, C_2 \ldots C_k$. Como cada componente conexa es acílico, entonces cada componente es un árbol y por el teorema 4.1.3, la componente i-esima tiene n_i vértices y

$N_i - 1$ aristas. En este caso el número total de vértices es $n = n_1 + n_2 + \cdots + n_k$ y el número de aristas es $n - 1 = m = (n_1 - 1) + n_2 - 1) + \cdots + (n_k - 1) = n_1 + n_2 + \cdots + n_k - k = n - k$. Como $k \geq 2$, entonces $m < n - 1$, una contradiccón con la hipótesis de que $m = n - 1$. □

Como consecuencia tenemos las siguientes dos caracterizaciones de árbol

Teorema 4.1.5. *Una gráfica G con al menos dos vértices es un árbol si y sólo si*

1. *G es conexa minimal.*
2. *G es acíclica maximal.*

Teorema 4.1.6. *Todo árbol con al menos dos vértices tiene al menos un vértice terminal (de grado* 1*).*

Demostración. Sea T un árbol y sea $P = (u_0, u_1, \ldots, u_k)$ una trayectoria de longitud máxima. Probaremos que $d(u_0) = 1$. Supongamos por contradicción que $d(u_0) \geq 2$. Sea $v \in V(T) \setminus \{u_1\}$ tal que $v \in N(u_0)$. Hay dos casos: $v \in V(P)$ o $v \in V(T) \setminus V(P)$. Si $v \in V(P)$, entonces $v = u_i$ para alguna $2 \leq i \leq k$. En este caso se forma el ciclo $(u_0, u_1, \ldots, u_i = v, u_0)$, lo cual contradice que T es un árbol. Por lo que $v \notin V(P)$ y $v \in V(T) \setminus V(P)$. En este caso $P' = (v, u_0, u_1, \ldots, u_k)$ es una trayectoria más larga que P, lo cual contradice la manera que eligimos la trayectoria P (P es una trayectoria de longitud máxima). □

4.1.1 Árbol generador

Supón que tienes una red de computadoras en la que se dañaron las conecciones entre las computadoras. Ahora se busca reestablecer algunas conexiones de modo que cualquier computadora se puede comunicar con cualquier otra computadora; por cuestón de costos se busca usar el menor número de conecciones. Si cada computadora es representado por un vértice y cada conección por una arista, entonces estamos buscando una subgráfica conexa con el menor número de aristas, es decir, una subgráfica generadora, conexa y acíclica.

Definición 4.1.7. Una subgráfica H de una gráfica conexa G es un **árbol generador** si H es una subgráfica conexa, acíclica que contiene a todos los vértices de la gráfica.

Surgen de manera natural preguntas como:

1. *¿Cómo podemos generar todos los árboles generadores de una gráfica.*
2. *¿Cuántos árboles generadores tiene una gráfica?*
3. *A partir de un árbol generador, ¿cómo se puede obtener otro árbol generador de la gráfica.*
4. *¿Cómo se ve un árbol generador en la matriz de incidencia/adyacencia?*

Está fuera del alcance del temario de la UEA Matemáticas Discretas II contestar estas preguntas, aunque tienen suficientes conocimientos para contastar una o varias de ellas.

Teorema 4.1.8. *Toda gráfica conexa tiene un árbol generador.*

Demostración. Ejercicio 4.13 □

Teorema 4.1.9. *Dada una gráfica conexa, se puede calcular el número de árboles generadores a partir de la matriz de adyacencia A_G.*

Demostración. Usando algebra lineal, se puede probar que todos los cofactores de una matriz de adyacencia A_G coinciden y es justo el número de árboles generadores de G. □

4.1.2 Árbol de peso mínimo

Recordamos el ejemplo de la red de computadoras de la sección de árboles generadoras con la información adicional del costo de reestablecer cada una de las conexiones. Es decir, ahora tenemos una gráfica G con una función de pesos $f : A(G) \to \mathbb{R}$, y quere-mos encontrar un árbol generador de peso mínimo, y definimos el peso de una gráfica (o subgráfica) como la suma de los pesos de las aristas de la gráfica (subgráfica).

El árbol de peso mínimo tiene aplicaciones tales como la forma mas barata de restablecer la comunicación en una red, por ejemplo de computadoras, teléfonos o carreteras.

4.1.3 Algoritmos de Árbol de Peso Mínimo

Sea $G = (V; A)$ una gráfica simple, conexa, con n vértices y sea $\omega : A(G) \to \mathbb{R}$ la función de peso que le asigna a cada arista $\{u,v\} \in A(G)$ su peso correspondiente ω_{uv}. Así, cada arista $\{u,v\} \in A(G)$ tiene un peso ω_{uv} asignado, el peso puede reflejar la distancia que se recorre, el costo por mantener la conección activa, el número de usuarios que lo usan o le que se busca minimizar.

El peso de una gráfica G es la sumas de los pesos de las aristas de G. Dado una gráfica $G(V, A)$ queremos encontrar un árbol generador T de G, tal que el peso de T sea mínimo, es decir, minimizar el número $\omega(T) = \sum_{a \in A(T)} \omega(a)$ sobre el conjunto de todos los árboles generadores de G.

Definición 4.1.10. *Un* **árbol de peso mínimo** *es un árbol en donde la suma de los pesos de las aristas es el menor posible.*

Cabe mencionar que el árbol de peso mínimo no siempre es único. Para poder asegurar la unicidad del árbol de peso mínimo tendríamos que pedir que los pesos de las aristas de la gráfica fueran distintos entre sí (ver ejercicio 4.14).

Revisaremos dos algoritmos, que resuelven el problema de encontrar un árbol de peso mínimo: Algoritmo de Kruskal y el algoritmo de Prim ambos son de los años de 1950.

Algoritmo de Kruskal para encontrar un árbol de peso mínimo

La idea del algoritmo es añadir aristas con la restricción de que no se formen ciclos. En cada paso el número de componentes conexas disminuye en uno hasta que se obtiene un solo componente.

El algoritmo de Kruskal inicia con un bosque que contiene n árboles, cada en donde cada árbol tiene un solo vértice. En cada paso del algoritmo dos árboles (componentes conexas) se conectan mediante una arista y así en cada paso obtenemos un nuevo bosque con un árbol menos y con árboles que cada vez tengan mas vértices, hasta que finalmente obtenemos un solo árbol. En cada paso elegimos la arista con menor peso. Si la arista elegida tiene ambos vértices terminales en un mismo árbol, entonces se descarta porque la arista genera un ciclo en nuestro bosque (y no volvemos a revisar tal arista). Si la arista tiene sus vértices terminales en dos diferentes árboles, entonces será la arista de menos peso que conecta dos árboles diferentes en nuestro bosque y al añadirla al bosque, convertimos dos árboles pequeñas en un árbol más grande.

Pseudocódigo para el algoritmo de Kruskal.

Sea $G = (V, A)$ una gráfica conexa con n vértices. Sea A_1 el conjunto de aristas del bosque del generador y A_2 el conjunto de aristas que no han sido revisado.

Begin
  $A_1 := \emptyset$, $A_2 := A$
  While $|A_1| < n - 1$ *do*
    Eligir la arista $a = \{u, v\}$ *de menor peso de* A_2
    $A_2 =: A_2 - \{a\}$
    If *u y v no son vértices del mismo árbol, entonces* $A_1 =: A_1 \cup \{a\}$.
    End
  End
End

Algoritmo de Prim para encontrar un árbol de peso mínimo

La idea del algoritmo es a partir de un vértice *v,* extender la componente conexa al cual pertence *v*, añadiendo aristas con la restricción de que no se formen ciclos. En cada paso el número de vértices de la componente de *v* aumenta en uno hasta que todos los vértices pertenecen al componente conexa del vértice *v*.

El algoritmo de Prim inicia con un árbol que tiene un solo vértice. En cada paso del algoritmo conectamos un nuevo vértice al arbol, hasta que finalmente obtenemos un árbol generador. En cada paso elegimos la arista con menor peso que conecta un vértice del árbol con un vértice que no esta en el árbol.

Pseudocódigo para el algoritmo de Prim.

Sea $G = (V, A)$ una gráfica conexa con n vértices. Sea V_1 el conjunto de vértices del árbol, V_2 el conjunto de vértices fuera del árbol y A' el conjunto de aristas del árbol.
Begin $V_1 := \{v_1\}$, $V_2 := V \setminus V_1$, $A' = \emptyset$.
  While $V_1 \neq V$ *do*
    Eligir la arista $a = \{u, v\}$ *de menor peso tal que* $u \in V_1$ *y* $v \in V_2$
    $V_1 := V_1 \cup \{v\}$, $V_2 := V_2 - \{v\}$, $A' := A' \cup \{a\}$.
  End
End

4.1.4 Ejercicios

Ejercicio 4.1. *Representa el árbol geneológico de las últimas tres generaciones de tu familia.*

Ejercicio 4.2. *Considera la seriación del mapa curricular en tu carrera. ¿Es un árbol? ¿Tiene ciclos? ¿Cuál(es)? ¿Es conexa? (justifica tu respuesta).*

Ejercicio 4.3. *Encuentra todas los árboles no isomorfas de orden* 7 *(son* 11*).*

Ejercicio 4.4. *Encuentra una gráfica G que* **no** *es un árbol tal que G tiene* 7 *vértices y* 6 *aristas.*

Ejercicio 4.5. *¿Cómo son los árboles que tienen exactamente dos vértices terminales?.*

Ejercicio 4.6. *Prueba (sin usar el Teorema 4.1.6) por inducción que todo árbol con al menos* 2 *vértices tiene al menos dos vértice terminales (de grado* 1*).*

Una gráfica es un árbol si la gráfica es conexa, si no es una gráfica conexa, entonces es una colección de árboles. Una gráfica acíclica no conexa es un bosque.

Ejercicio 4.7. *Sea G un bosque con*

1. 6 *árboles y* 43 *aristas, ¿Cuantos vértices tiene al bosque G?*
2. 50 *vértices y* 38 *aristas, ¿Cuantas componentes conexas tiene al bosque G?*

Ejercicio 4.8. *Sea G un bosque con n vértices, m aristas y k componentes conexas. ¿Qué relación hay entre n, m y k?*

Ejercicio 4.9. *¿Cuántos árboles generadores no isomorfos tiene un ciclo?*

Ejercicio 4.10. *Encuentra dos árboles generadores no ismorfos de la gráfica K_5 (ver figura 3.24) y dos árboles generadores no ismorfos de la gráfica $K_{2,3}$.*

Ejercicio 4.11. *Encuentra un árbol generador de la gráfica de la figura 3.26.*

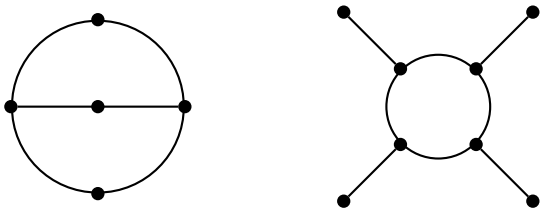


Figura 4.3: Gráficas del ejercicio 4.12.

Ejercicio 4.12. *Encuentra todos los árboles generadores no isomorfos de las siguientes gráficas.*

Ejercicio 4.13. *Toda gráfica conexa tiene un árbol generador.*

Ejercicio 4.14. *Si los pesos de las aristas en una gráfica conexa son distintos entre si, entonces el árbol de peso mńimo es único.*

4.2 Caminos y árboles especiales

En diversas aplicaciones de los árboles conviene contar con un vértice distinguido llamado raíz. Un **árbol con raíz** es un árbol con un vértice distinguido llamado raíz. Las figuras 4.2, 4.4 y 4.5 son ejemplos de árboles con raíz. Muchos programas computacionales utilizan una estructura de árbol con raíz para analizar todas las posibles casos y para organizar datos. Los árboles de conteo son ejemplos de árboles con raíz.

La **profundidad de un árbol** es la excentricidad de la raíz, es decir la longitud de la trayectoria más grande iniciando en la raíz.

Sea T un árbol con raíz r y profundidad k, definimos los niveles del árbol T como:

$$N_1 = \{v \in T : d(r, v) = 1\}$$
$$N_2 = \{v \in T : d(r, v) = 2\}$$
$$\vdots$$
$$N_k = \{v \in T : d(r, v) = k\}$$
$$\textit{El ancho del árbol } T \textit{ es } \max_{i \leq k} |N_i|$$

Ejemplo 4.2.1. *En el ejemplo 4.0.2, el ancho del árbol de la figura 4.2 es ocho, porque el nivel N_3 tiene ocho vértices. En el ejemplo 4.2.5, el ancho del árbol de conteo de la figura 4.5 es cuatro, porque el nivel N_3 tiene cuatro vértices.*

Podemos hablar de un orden de los sucesores (hijos) y antecesores (padres) al conjunto de todos los vértices anteriores tambien se les llama ancestros. Llamareos un árbol m-ario completo si cada vértice no terminal tiene m-hijos.

4.2.1 Árboles binarios

Un árbol binario es un árbol en el que la raíz tiene grado 2 y los vértices restantes tienen grado 1; 2 o 3 (los vértices terminales son aquellos que tienen grado 1), es decir, tienen a lo más dos vértices en el siguiente nivel. La estructura de un árbol binario es muy frequente en estructuras de datos usados en computo. Un árbol T es binario completo si cada vértice no terminal tiene dos hijos, es decir, tiene exactamente dos vértices en el siguiente nivel. Los árbol geneológicos son árboles binarios completos, pues cada persona tiene exactamente dos padres biológicos (aunque no siempre conoce ambos).

Ejemplo 4.2.2. *En algunos casos, un problema de conteo se puede resolver mediante un* **árbol de conteo**. *Por ejemplo, si queremos contar cuantos posibles resultados se puede obtener al lanzar tres volados (lanzar un moneda tres veces) podemos construir el árbol de conteo figura 4.4.*

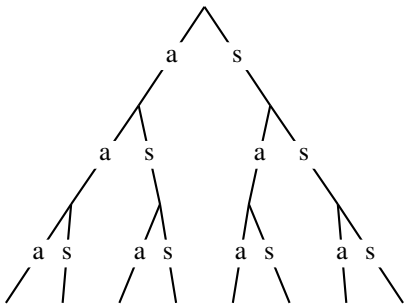


Figura 4.4: Árbol de conteo de los posibles resultados al lanzar tres monedas.

Como resultado tenemos 8 posibles resultados si tomamos en cuenta el orden, pero solo 4 si no nos importa el orden.

Ejemplo 4.2.3. *Las carpetas y archivos en el disco duro de una computadora tienen la estructura de árbol.*

Ejemplo 4.2.4. *Si queremos determinar que resultado sale el mayor número de veces y no nos importa el orden, podemos usar el árbol de la figura 4.4 del ejemplo 4.2.2 y como resultado tenemos que el resultado dos águilas y un sol aparece tres veces igual que el caso dos soles y un águila.*

Ejemplo 4.2.5. *Supón que tienes cinco monedas y sabes que exactamente una de ellas es falsa. ¿Cuál es el mánimo número de veces que debas pesar las monedas para asegurar que encuentres la moneda falsa?*
En el caso que sabes que la moneda falsa pesa menos, ¿puedes determinarlo mas rápido cuál es la moneda falsa?

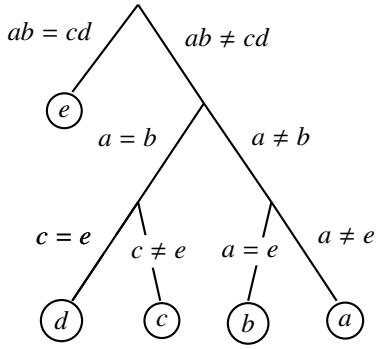


Figura 4.5: Árbol de conteo de los posibles resultados al pesar las monedas del acertijo

Ejemplo 4.2.6. [11] *¿De cuántas maneras se pueden colocar n de reynas en un tablero de ajedréz de n × n. Revisamos el caso particular cuando tenemos 4 reynas y un tablero de* 4×4.

Códigos Huffmann

Un **Código Huffmann** es una codificación de una plabra o mensaje en términos de un árbol y una cadena de 0's y 1's. Es decir, si conoces el árbol y la palabra codificada, se puede recuperar la palabra original. Viceversa, con una plabra y un árbol fijo, con ciertas propiedades, se puede extraer la codificación en términos de un árbol.

Dado un árbol binario completo con raíz, le asignamos a cada arista el valor de 0 o 1 según si ésta es la opción de la izquierda o la derecha respectivamente y a cada vértice terminal le asignamos un letra (sin repetir que se repita una letra aunque sí podemos omitir letras). Dada una palabra o frase, le podemos asignar una cadena de 0's y 1's segun´ el camino que se recorre apartir de la raíz (Nótese que este camino es única por ser un árbol). Por ejemplo, en el árbol de la figura 4.6 la letra *a* se representa mediante la cadena 1001.

Ejemplo 4.2.7. Considera el árbol binario de la figura 4.6 y encuentra las palabras 10111100001001 y 1101100001001101. Primero partimos el código en trayectorias maximales 101|11|10000|1001 y queda la palabra reta y 11|01|10000|1001|101 y queda la palabra "estar".

Cómo construir un árbol óptimo para el código de Huffmann

Dado una palabra o una frase, un árbol de Huffmann es un **árbol óptimo de Huffmann** si el código de la palabra o de la frase tiene el mínimo nímero posible de caracteres.

Vamos a usar un ejemplo para explicar el procedimiento para construir un árbol óptimo para el código de Huffmann. Consideramos la palabra "popocatepetl"

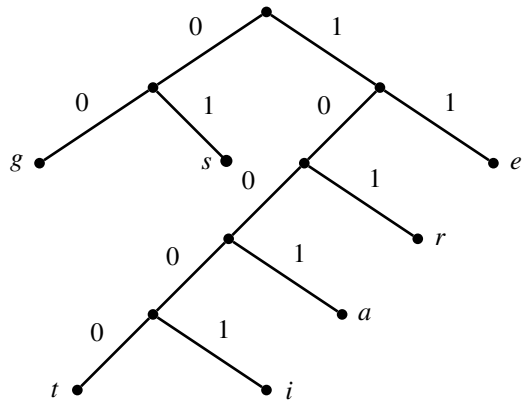


Figura 4.6: Árbol del ejercicio 4.2.7.

(sin acentos). En total hay 12 letras, hacemos una tabla de la frecuencia de cada letra y ordenamos las frecuencias en orden no decreciente:

Cuadro 4.1: Frecuencias de las letras en la palabra "*popocatepetl*".

p	o	c	a	t	e	l
3	2	1	1	2	2	1

1	1	1	2	2	2	3
	1	2	2	2	2	3
		2	2	2	3	3
			2	3	3	4
				3	4	5
					5	7

Luego construimos un árbol binario yendo de abajo para arriba, recuperando en cada paso los números que se sumaron para modificar la secuencia de números

Es importante destacar que el árbol óptimo no es único. Los dos árboles de la figura 4.8 son óptimos para la palabra popocatepetl.

El árbol de Huffmann se obtiene poniendo en cada vértice terminal una letra que corresponda a la frecuencia de la (única) arista que incide en él.

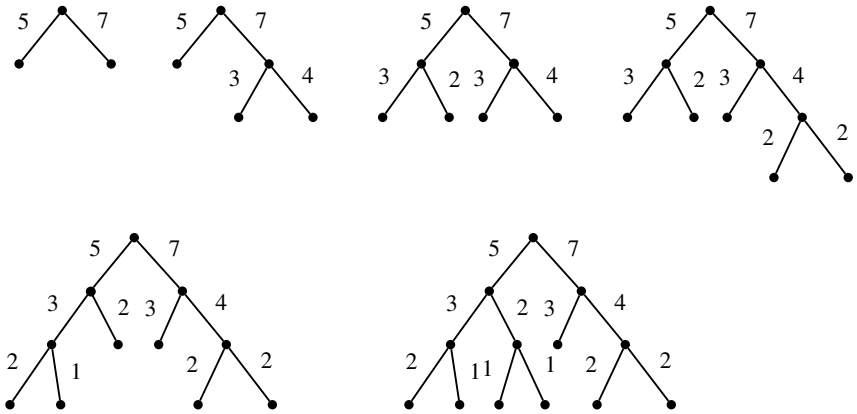


Figura 4.7: Construcción de un árbol óptimo para la palabra popocatepetl.

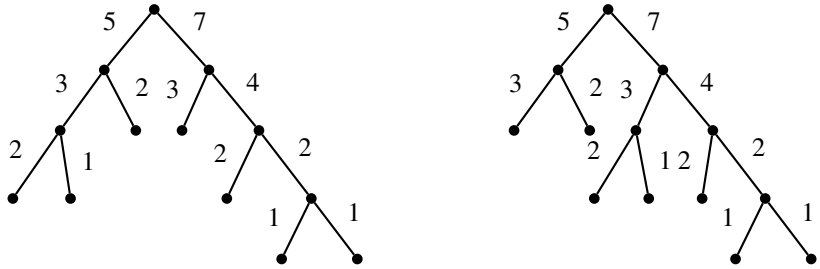


Figura 4.8: Construcción de otros dos árboles óptimos para la palabra popocatepetl.

4.2.2 Ejercicios

Ejercicio 4.15. *Representa el árbol geneológico de las últimas tres generaciones de tu familia.*

Ejercicio 4.16. *Considera la seriación del mapa curricular en tu carrera. ¿Es un árbol? ¿Tiene ciclos? ¿Cuál(es)? ¿Es conexa? (justifica tu respuesta).*

Ejercicio 4.17. *Encuentra todas los árboles no isomorfas de orden* 7 *(son* 11*).*

Ejercicio 4.18. *Encuentra una gráfica G que* **no** *es un árbol tal que G tiene* 7 *vértices y* 6 *aristas.*

Ejercicio 4.19. *Sea T un árbol m-ario completo con n vértices y h vértices terminales y i vértices internos. Entonces*

1. $n = mi + 1$,

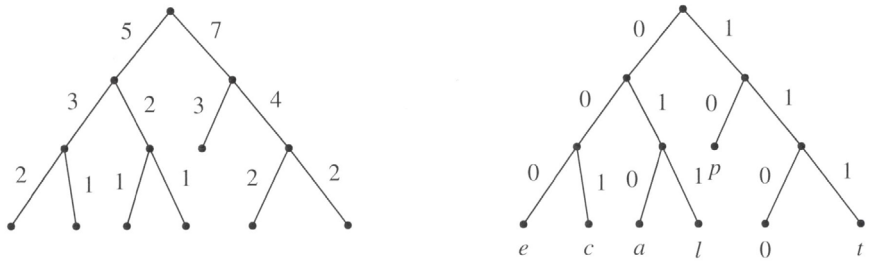


Figura 4.9: Árbol óptimo de Huffmann para la palabra popocatepetl.

2. $h = (m-1)i + 1$
3. $i = (h-1)/(m-1) = (n-1)/m$

Ejercicio 4.20. *Una aula tiene* 25 *computadoras que deben conectarse a un enchufe de pared con* 4 *salidas. Se hacen las conexiones mediante cables de extensión con* 4 *salidas cada uno. ¿Cuál es el mínimo número de cables que se necesitan para poder utilizar todas las computadoras?*

Ejercicio 4.21. *Prueba que un árbol es una gráfica bipartita.*

Ejercicio 4.22. *Para cada inciso, construye un árbol óptimo para la codificación de Hoffmann así como su codificación.*

1. *las tres palabras:* resistir, raros, restos.
2. *la frase: "*tres tristes tigres*".*

Ejercicio 4.23. *Construye un árbol óptimo para la codificación de Hoffmann para codificar la frase: "*tres tristes tigres*". Sin construir un árbol óptimo para la frase "*tres tristes tigres tragaban trigo en un trigal*", determina cuántos vértices internos tiene tal árbol.*

Hint: Usar el ejercicio 4.19.

Ejercicio 4.24. *Construye un árbol óptimo para la codificación de Hoffmann para codificar el cuento de Augusto Monterrosa (sin importar los acentos)*

"Cuando despertó, el dragón seguía allí "

4.3 Proyectos

Árboles de peso mínimo.

Investiga qué aplicaciones tienen los árboles de peso mínimo. Prueba que los álgoritmos Prim y Kruskal siempre encuentra un árbol de peso mínimo. Para cada álgoritmo determina el número de pasos del peor caso. Finalmente, implementa los álgoritmo Prim y Kruskal para encontrar un árbol de peso mínimo. Ver sección 3.6 en [6].

Árboles de decisión y tiempo mínimo para ordenar

Los árboles de decisión constituyen una herramienta para analizar los estados y consecuencias de una serie de decisiones secuenciadas y tienen aplicaciones en diversas áreas del conocimiento desde diagnósticos médicos hasta reconocimiento de caracteres. Un árbol de decisión es un árbol con raíz, que nos ayuda a representar y visualizar todos los posibles eventos cuando conocemos todas las posibles opciones de una decisiones. Cada vértice representa el momento de la decisión y normalmente se representa con un cuadrado con la pregunta en su interior. Por cada posible decisión hay una arista al siguiente nivel o bien a la siguiente desición secuenciada. En el árbol de decisión se pueden incluir costos o probabilidades de que suceda cierto evento o no.

Prueba que si usas un algoritmo que ordena n objetos, el número de comparaciones es en el peor caso es $\Omega(n \lg n)$.

Analiza y explica la aplicación de árboles de decisión en tres áreas distintos. Ver sección 9.7 [11].

Búsquedas en árboles con raíz.

Compara los dos algoritmos de búsqueda a profundidad y búsquedas a lo ancho y determina en que casos el algoritmos de búsqueda a profundidad es el mejor y en que caso el algoritmos de búsqueda a lo ancho es el mejor.

- Búsqueda a profundidad (hasta llegar a una hoja, regresar por el camino que venías hasta encontrar un vértice con una arista no usada y seguir). Sección 3.3 en [6].
- Búsqueda a lo ancho (se revisa todos los elementos de cada nivel antes de buscar en el siguiente nivel). Sección 3.5 en [6].

Bibliografía

[1] C. Balbuena, Notas sobre un curso de Álgebra lineal aplicada a Teoría de gráficas. DCNI, UAM-Cuajimalpa (2016).

[2] Berge, C., Rao, A.R., A combinatorial problem in logic, Discrete Math. 17 *(1977), 23–26.*

[3] Berge, C., Combinatorial games on a graph, Discrete Math. 151 *(1996), 59-65.*

[4] Cárdenas, H., Lluis, E, Raggi, F, y Tomas, F. Álgebra Superior, Trillas, 2007.

[5] Caballero, R, Hortalá, T, Martí N, Nieva, S, Pareja A y Rodriguez, M, Matemáticas Discretas para Informáticos. Ejercicios resueltos. Pearson Educación S.A., Madrid 2007.

[6] Chartrand, G., Oellerman, O. R., Applied and Algorithmic Graph Theory, McGrawHill Inc., 1993.

[7] Comellas, F., Fábrega, J., Sánchez A. y Serra, O. Matemática Discreta. Ediciones UPC, 2002.

[8] Goodaire E., Parmenter M., Discrete Mathematics with Graph Theory, (3º ed) Addison Wesley, 2005.

[9] Grimaldi, R. Matemáticas Discreta y Combinatoria: una introducción con aplicaciones, Prentice Hall, 1998.

[10] Gross, J. L., Yellen, J.,Graph Theory and its Applications, Chapmann & Hall/CRC, 2006.

[11] Johnsonbaugh, R., Matemáticas Discretas, (6º ed.). Prentice Hall, 2005.

[12] Klima R.E., Sigmon, N., Stitzinger E. Applications of Abstract Algebra with Maple, CRC Press, 2000.

[13] Oteyza, E., Lam, E., Hernández, C., Carrillo, Á., Temas Selectos de Matemáticas, Prentice Hall, 2002.

Índice alfabético

Notas de la UEA Matemáticas Discretas II se terminó de imprimir en la Ciudad de México en octubre de 2017. La producción editorial e impresión estuvo a cargo de Literatura y Alternativas en Servicios Editoriales S.C. Avenida Universidad 1815-c, Depto. 205, Colonia Oxtopulco, C. P. 04318, Delegación Coyoacán, Ciudad de México. RFC: LAS1008162Z1. En su composición se usaron tipos Times New Roman y Helvetica. Se tiraron 100 ejemplares sobre papel Prisma Bright, papel certificado FSC (Forest Stewardship Council®) Ref EP.01.00028.

Casa abierta al tiempo

UNIVERSIDAD AUTÓNOMA METROPOLITANA

Unidad Cuajimalpa