Matemáticas Discretas

Ingeniería en Inteligencia Artificial Aplicada a la Agricultura

Primer Semestre

Universidad Autónoma Chapingo

28 de septiembre de 2025

Autor:
Dr. Juan Carlos Cruz González

Índice general

Capítulo 1

Fundamentos lógicos y teoría de conjuntos

1.1. Lógica proposicional

La lógica desempeña un papel fundamental en las matemáticas, ya que proporciona un marco riguroso para el razonamiento deductivo y la demostración de teoremas matemáticos. La lógica establece reglas y estructuras para analizar y evaluar la validez de los argumentos matemáticos, asegurando la coherencia y consistencia del razonamiento. Veamos las siguientes razones clave sobre la importancia de la lógica en las matemáticas:

- *Rigor y precisión*: La lógica garantiza que las afirmaciones matemáticas sean rigurosas y precisas. Ayuda a evitar ambigüedades y garantiza que los resultados matemáticos sean sólidos y confiables. La lógica proporciona un lenguaje formal y un conjunto de reglas para expresar ideas matemáticas de manera clara y sin ambigüedades.

- *Demostración de teoremas*: La lógica es fundamental para la demostración de teoremas matemáticos. Proporciona herramientas y técnicas para estructurar y presentar argumentos válidos que respalden la veracidad de las afirmaciones matemáticas. La validez lógica de un razonamiento es esencial para establecer la verdad de un teorema.

- *Consistencia y coherencia*: La lógica ayuda a mantener la consistencia y coherencia en las matemáticas. Ayuda a evitar contradicciones y paradojas en los sistemas matemáticos. Al seguir reglas lógicas sólidas, se pueden identificar inconsistencias y resolver problemas que podrían surgir en el desarrollo de teorías matemáticas.

- *Fundamentos de la matemática*: La lógica proporciona los fundamentos teóricos de la matemática. Los sistemas axiomáticos y las estructuras lógicas subyacentes permiten construir y analizar diferentes áreas de las matemáticas, como el álgebra, la geometría, el cálculo y la teoría de conjuntos.

- *Aplicaciones en la computación*: La lógica matemática es la base de la ciencia de la computación y la programación. Los principios lógicos se utilizan para construir algoritmos, diseñar sistemas de hardware y software, y garantizar la corrección y consistencia de los programas informáticos.

En conclusión a lógica es esencial en las matemáticas porque proporciona un marco riguroso para el razonamiento y la demostración de teoremas. Ayuda a mantener la consistencia y coherencia en los sistemas matemáticos, y su aplicación se extiende más allá de las matemáticas en campos como la informática y la programación.

1.1.1. Conceptos básicos

La lógica ha sido descrita como el reino de lo verdadero y lo falso en el mismo sentido que la ética es el de lo bueno y lo malo o la estética el de lo bello y lo feo.

Una **proposición** es una sentencia o expresión que puede ser verdadera o falsa, pero no ambas al mismo tiempo. Por lo tanto, una proposición tiene un **valor de verdad**, que puede ser **V** si es verdadera, o **F** si es falsa.

■ **Ejemplos 1.1.1.** ***Los siguientes ejemplos son proposiciones verdaderas:***

- *La raíz cuadrada de 16 es igual a 4:* $\sqrt{16} = 4$.
- *El producto de cualquier número real por 0 es igual a 0:* $n \cdot 0 = 0$.
- *El valor absoluto de un número negativo es siempre positivo:* $|(-n)| = n$.
- *La suma de los ángulos internos de un triángulo es siempre 180 grados:* $\alpha + \beta + \gamma = 180°$.
- *El número* π *es irracional.*
- *La suma de los ángulos externos de cualquier polígono siempre es 360 grados:* $\sum \theta_i = 360°$.
- *El producto de dos números negativos es siempre positivo:* $(-a) \cdot (-b) = ab$.

■ **Ejemplos 1.1.2.** ***Los siguientes son proposiciones falsas:***

- *El cuadrado de un número siempre es mayor que el número en sí mismo:* $n^2 > n$.
- *odos los triángulos isósceles son equiláteros.*
- *El resultado de dividir cualquier número entre cero es infinito:* $\frac{n}{0} = \infty$.
- *La suma de dos números irracionales es siempre irracional.*
- *La longitud de la circunferencia es igual al cuadrado de su radio.*

■ **Ejemplos 1.1.3.** ***Algunos ejemplos de expresiones que no son proposiciones son:***

- «*73*»
- «$x - 1 = 5$»
- «*¿Cuál es la solución de* $2x - 1 = 0$*?*»

Generalmente, para referirnos a proposiciones especificas se usan letras mayúsculas. Por ejemplo,

P : 25 es un número entero par.

Q : $3 + 5 = 8$.

R : $2x + 3$ es una ecuación.

Las proposiciones pueden contener variables como lo son: $x.y, z$, etc. Por ejemplo:

P : Para todo número real «x», existe un número real «y»tal que $y > x$.

Esta proposición es verdadera independientemente del valor de x. Entonces podemos denotarlas por:

$P(x)$: Para todo número real «x», existe un número real «y»tal que $y > x$.

Hay oraciones o expresiones matemáticas que contienen variables y no son proposiciones, por ejemplo:

$Q(a)$: a es un número entero que es divisible por 5.

Este enunciado solo adquiere el estatus de proposición cuando asignamos un valor específico a a (y así podemos determinar si es verdadera o falsa). Por ejemplo, $Q(3)$ es falsa y $Q(15)$ es verdadera. Una expresión como $Q(a)$, cuyo valor de verdad depende de una o más varibales, es lo que se llama una **expresión abierta**.

Existen proposición que no se compone de otras proposiciones, a estas proposiciones se le llaman **atomos** o **proposiciones atomicas**. Para construir otras proposiciones a partir de otras se usan lo que se conoce como **conectivos logicos** que son simbolos(con significado) que sirven para combinar proposiciones en general y de esa manera crear una nueva proposición.

■ **Ejemplo 1.1.4.** *Proposicion: Si llueve, entonces las calles estan mojadas.*

Los atomos son: Llueve, las calles estan mojadas.
Conectivo: si, entonces

■ **Ejercicio 1.1.5.** *Determina si el siguiente enunciado es no verdadero: «Esto no es una proposición».*

1.1.2. Conectivos Lógicos

Como ya se ha mencionado, un conector es una función que se aplica a proposiciones (o a sus valores de verdad), produciendo otra proposición. Pueden caracterizarse completamente mediante una tabla de verdad.

Podemos emplear la conjunción «y»para combinar dos proposiciones y generar una nueva proposición. Veamos el siguiente ejemplo:

■ **Ejemplo 1.1.6.** *Consideremos dos proposiciones P, Q como sigue:*

P : El número π es irracional.

Q : *El número* $\frac{1}{2}$ *es racional.*

R: El número π *es irracional* ***y*** *El número* $\frac{1}{2}$ *es racional.*

En el ejemplo 1.1.6 tenemos que P, Q son verdaderas, entonces también lo es R. En general, dadas dos proposiciones P y Q, podemos combinarlas para formar una nueva proposición «P y Q». Usamos el símbolo $\wedge$ para indicar la palabra «**y**». De modo que $P \wedge Q$ significa «P **y** Q». La proposición $P \wedge Q$ es verdadera si ambos lo son, en cualquier otro caso, es falsa. Esto se resume en la siguiente **tabla de verdad**.

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

En esta tabla, P y Q representan las dos proposiciones que queremos combinar con la conjunción «y»($\wedge$). La columna final muestra el resultado de la conjunción para cada combinación de los valores de P y Q. Donde «V»representa una proposición verdadera, y «F»representa una proposición falsa.

Además, es posible establecer una conexión entre dos proposiciones utilizando el término «o», generando así una proposición adicional. Esto es, dadas dos proposiciones P y Q, la afirmación «P **o** Q»significa que alguna de las dos puede ocurrir, en términos matemáticos el nuevo enunciado es verdadero si al menos una de las dos es verdadera. Se usa el símbolo $\vee$ para denotar la palabra «*o*». Así, $P \vee Q$ significa «P **0** Q». Veamos un ejemplo

■ **Ejemplo 1.1.7.** *Consideremos las proposiciones* P *y* Q *como siguen:*

P : *El número* π *es irracional*

Q : *El número* π *es racional*

$P \vee Q$: *El número* π *es irracional* ***o*** *el número* π *es racional*

En el ejemplo previo $P \vee Q$ es verdadera, pues P lo es. La tabla de verdad para $P \vee Q$ es la siguiente:

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

También, es común negar oraciones y obtener con ello su enunciado opuesto. Dada una proposición P, podemos formar una nueva proposición «**no es cierto que** P». Usamos el símbolo $\neg$ para indicar la frase «no es cierto que».

■ **Ejemplo 1.1.8.** *Usando la notación correspondiente:*

P : *Matemáticas es difícil.*

$\neg P$: *Matemáticas no es difícil.*

La tabla de verdad para $P \vee Q$ es la siguiente:

P	$\neg P$
V	F
F	V

En nuestro idioma, empleamos oraciones condicionales, es decir, cuando sucede cierto evento, se produce una consecuencia determinada. Un ejemplo de esto sería: Si no dedico tiempo al estudio, obtendré una calificación baja. Estos conectores se conocen como condicionales. En el el lenguaje matemático; dadas P y Q proposiciones, podemos formar la nueva proposición «**Si** P, **entonces** Q». La representación simbólica de esta proposición es la siguiente; $P \Rightarrow Q$, la cual también se puede leer como «P implica Q»y se conoce como **proposición condicional**. Ahora, $P \Rightarrow Q$ establece una relación entre dos proposiciones: P y Q. P puede ser una afirmación o condición inicial, mientras que Q representa la consecuencia o resultado esperado. El significado de $P \Rightarrow Q$ nos dice que la única manera esta sea falsa, es que P sea verdadera y Q falsa. Así, la tabla de verdad es:

P	Q	$P \Rightarrow Q$
V	V	V
V	F	F
F	V	V
F	F	V

Las expresiones más comunes que significan $P \Rightarrow Q$ son:

- Si P, entonces Q.
- Q, si P.
- Q, siempre que P.
- P es una condición suficiente para Q.
- Q es una condición necesaria para P.
- P, solo si Q.

Veamos un ejemplo de la implicación en algunas de sus expresiones semánticas:

■ **Ejemplo 1.1.9.** *Si estudias, entonces aprobarás el examen. P : Estudias y Q : Aprobaras el examen.*

- *Aprobaras el examen, si estudias.*
- *Aprobaras el examen, siempre que estudias.*
- *Estudias, solo si aprobaras el examen.*

La proposición recíproca de una implicación $P \Rightarrow Q$ se obtiene intercambiando las proposiciones P y Q para formar la implicación $Q \Rightarrow P$. La **contrarrecíproca** (o **contrapositiva**) de $P \Rightarrow Q$ se obtiene al negar ambas proposiciones y luego intercambiarlas para formar la implicación $\neg Q \Rightarrow \neg P$. Es importante tener en cuenta que la contrarrecíproca siempre tiene el mismo valor de verdad que la implicación original. Si la implicación original es verdadera, la contrarrecíproca también será verdadera, y si la implicación original es falsa, la contrarrecíproca también será falsa.

Ahora, dadas dos proposiciones P y Q, podemos considerar tanto $P \Rightarrow Q$ como $Q \Rightarrow P$. En primer lugar, $P \Rightarrow Q$ no es lo mismo que $Q \Rightarrow P$, pues tienen distinto significado y por lo tanto valores de verdad distintos. Si consideramos la proposición $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$, que sabemos que es verdadera cuando ambas lo son. Leemos $Q \Rightarrow P$ como «P si Q»y $P \Rightarrow Q$ como «P, solo si Q», en consecuencia, leemos $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$ como «P, **si y solo si** Q», y el símbolo que usamos para la frase «si y solo si»es $\iff$, por tanto, denotaremos a $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$ como $P \iff Q$. Una proposición de la forma $P \iff Q$ se conoce como **proposición bicondicional**.

■ **Ejemplo 1.1.10.** *Sea P : x es un número par y Q : x es divisible por 2.*

$P \Rightarrow Q$: *Si x es un número par, entonces x es divisible por 2.*

$Q \Rightarrow P$: P : *Si x es divisible por 2, entonces x es un número par.*

$P \iff Q$: *x es un número par, si y solo si, es divisible por 2.*

Usando el conocimiento que tenemos de las tablas de verdad de $\wedge$ y $\Rightarrow$ se puede obtener la tabla de verdad siguiente:

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$P \iff Q$
V	V	V	V	V
V	F	F	V	F
F	V	V	F	F
F	F	V	V	V

Por lo que la tabla de verdad de $P \iff Q$ es:

P	Q	$P \iff Q$
V	V	V
V	F	F
F	V	F
F	F	V

Toda proposición matemática tiene su tabla de verdad, hay casos especiales que merecen un nombre adecuado. Una proposición se llama **tautología** cuando su tabla de verdad es siempre verdadera y cuando es siempre falta se llama **contradicción**.

1.1.3. Equivalencias Lógicas

La equivalencia lógica se refiere a la relación entre dos proposiciones lógicas que tienen el mismo valor de verdad en todas las situaciones posibles. En otras palabras, dos proposiciones son **lógicamente equivalentes** si y solo si tienen la misma tabla de verdad.

Por ejemplo, las proposiciones $P \iff Q$ y $(P \wedge Q) \vee (\neg P \wedge \neg Q)$ son lógicamente equivalentes:

P	Q	$\neg P$	$\neg Q$	$P \wedge Q$	$\neg P \wedge \neg Q$	$P \iff Q$	$(P \wedge Q) \vee (\neg P \wedge \neg Q)$
V	V	F	F	V	F	**V**	**V**
V	F	F	V	F	F	**F**	**F**
F	V	V	F	F	F	**F**	**F**
F	F	V	V	F	V	**V**	**V**

Usamos el símbolo $\equiv$ para denotar la equivalencia lógica de dos proposiciones, en nuestro ejemplo tendremos:

$$P \iff Q \equiv (P \wedge Q) \vee (\neg P \wedge \neg Q).$$

Unas ilustración relevantes de equivalencia lógica se puede encontrar en el siguiente en los siguientes casos:

$P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P.$

$P \Rightarrow Q \equiv \neg P \vee Q.$

Para verificar estas equivalencias, examinamos sus tablas de verdad:

P	Q	$\neg P$	$\neg Q$	$P \Rightarrow Q$	$\neg Q \Rightarrow \neg P$
V	V	F	F	**V**	**V**
V	F	F	V	**F**	**F**
F	V	V	F	**V**	**V**
F	F	V	V	**V**	**V**

P	Q	$\neg P$	$P \Rightarrow Q$	$\neg P \vee Q$
V	V	F	**V**	**V**
V	F	F	**F**	**F**
F	V	V	**V**	**V**
F	F	V	**V**	**V**

1.1.4. Enunciados matemáticos

Definiciones

El concepto de **definición** es uno de los fundamentos esenciales en matemáticas y constituye uno de los primeros conceptos que se exploran en esta disciplina.. En matemáticas, una **definición** es una declaración precisa y clara que establece el significado de un concepto o término. Una definición tiene el propósito de proporcionar una descripción precisa y sin ambigüedades de un objeto, una propiedad o una relación matemática.

Una definición matemática generalmente se compone de dos partes: el término que se define y la descripción o características que lo distinguen. La descripción puede incluir propiedades, relaciones o condiciones que deben cumplirse para que el término sea aplicable.

Una buena definición en matemáticas es precisa, concisa y no ambigua, evitando cualquier tipo de ambigüedad o confusión en su interpretación. Además, es importante que una definición sea consistente con los conceptos y principios establecidos en el ámbito matemático.

Las definiciones matemáticas son fundamentales para establecer una base sólida en cualquier área de estudio matemático, ya que permiten un lenguaje preciso y comúnmente aceptado para comunicar ideas y teoremas.

Daremos, como ejemplo, algunas definiciones. Es fundamental tener en cuenta que no proporcionaremos definiciones para todo, ya que partiremos del supuesto de que el lector posee cierto nivel de familiaridad con;

- los números naturales: $\mathbb{N} : 0, 1, 2, 3, 4, 5, \ldots,$,
- los números enteros: $\mathbb{Z} : \ldots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \ldots,$,
- los racionales: $\mathbb{Q}$ que son de la forma $\frac{a}{b}$ con a y b números enteros y $b \neq 0$,
- los irracionales que son los que no son racionales,
- los números reales $\mathbb{R}$ que es la unión de todos los anteriores.

y por su puesto que conoce las operaciones suma y producto con ellos, además de algo de álgebra elemental, así como ciertos conceptos sobre estos espacios.

Definición 1.1.11. *Dados dos enteros a y b, si $b = ac$, para algún entero c, diremos que a **divide** a b, y escribimos $a|b$. En esta situación, a es un **divisor** de b, y b es **múltiplo** de a.*

Por ejemplo, 3 divide a 15, pues $15 = 3(5)$. Escribimos esto como $3|15$, sin embargo 3 no divide a 13, pues no existe un entero c tal que $13 = 3c$. Escribimos esto como $3 \not| 13$ que se lee como «3 no divide a 13».

Definición 1.1.12. *Decimos que un número natural p mayor que 1 es **primo** si sus únicos divisores positivos son 1 y p .*

Ejemplo de números primos: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29.

Proposiciones verdaderas: Teoremas, Lemas y Corolarios

En matemáticas, un **teorema** es una afirmación o proposición que ha sido demostrada rigurosamente y se considera verdadera dentro de un determinado sistema matemático. Los teoremas son fundamentales en la construcción y desarrollo de la teoría matemática, ya que proporcionan resultados importantes y establecen conexiones entre diferentes conceptos matemáticos.

Los teoremas pueden abarcar una amplia gama de áreas y ramas de las matemáticas, como el álgebra, la geometría, el cálculo, la teoría de números, la lógica y más. Algunos teoremas son conocidos por sus nombres propios, como el teorema de Pitágoras, el teorema de Fermat o el teorema fundamental del cálculo.

Los teoremas son fundamentales en matemáticas porque establecen verdades matemáticas basadas en un razonamiento lógico sólido y proporcionan las bases para el desarrollo y avance de nuevas ideas y teorías. También son utilizados para resolver problemas matemáticos y para establecer relaciones y propiedades dentro de diferentes áreas de estudio.

Los teoremas usualmente son proposiciones condicionales, es decir, del tipo $P \Rightarrow Q$, aunque a veces el enunciado del teorema o proposición a veces oculta este hecho. Para ejemplificar esto último veamos la siguiente proposición:

Teorema 1.1.13 (**Teorema de Pitágoras**). *En un triángulo rectángulo con lados de longitudes a, b y c, donde c es la hipotenusa, se cumple que*

$$a^2 + b^2 = c^2.$$

Como este enunciado, no parece ser una proposición condicional, sin embargo podemos expresarla como una proposición condicional escribiendo:

Teorema 1.1.14. *Si un triángulo es un triángulo rectángulo con lados de longitudes a, b y c, donde c es la hipotenusa, entonces se cumple que* $a^2 + b^2 = c^2$.

Cuando un teorema en matemáticas se puede expresar en forma de una condicional $P \Rightarrow Q$, la proposición P se llama **hipótesis** o conjunto de supuestos, y la consecuente(proposición) Q es la afirmación que se deduce a partir de la hipótesis, es decir, la **tesis**. En nuestro ejemplo, la hipótesis o antecedente es que el triángulo es un triángulo rectángulo con lados a, b y c, y la conclusión o consecuente es la igualdad $a^2+b^2 = c^2$. Cabe señalar que no todo teorema es una proposición condicional. Algunos tienen la forma bicondicional $P \iff Q$. Otros teoremas son simplemente proposiciones P.Por ejemplo,

Teorema 1.1.15. *Existe una infinidad de números primos*

Hay varias palabras que significan esencialmente lo mismo que la palabra «teorema». En general «teorema»se reserva para proposiciones significativas o importantes (por ejemplo, el Teorema de Pitagóricas). Una proposición verdadera, pero no significativa, se llama simplemente **proposición**, un **lema** es proposición verdadera auxiliar utilizado en la demostración de un teorema, un **corolario** es una consecuencia directa de un teorema previamente demostrado.

Una **demostración** de la veracidad de una proposición es un argumento lógico que muestra de manera clara y convincente por qué un teorema es verdadero. Las demostraciones pueden involucrar razonamientos deductivos, reglas matemáticas, propiedades de los números y objetos matemáticos, entre otros elementos. Se compone de una secuencia de afirmaciones numeradas de $(1), (2), \ldots, (n)$, donde cada afirmación está respaldada por una o más razones que justifican su validez. Estas razones pueden incluir hipótesis, definiciones, afirmaciones previas en la misma demostración o proposiciones matemáticas ya demostradas. La última afirmación de la secuencia es la tesis que se busca demostrar.

1.1.5. Demostraciones

El objetivo de una demostración es proporcionar una justificación sólida y convincente de la veracidad de una afirmación matemática. Al demostrar una proposición, se establece una verdad matemática de forma rigurosa, lo que permite su aplicación en el desarrollo de nuevas teorías, la resolución de problemas y el avance del conocimiento matemático. Existen varios tipos de demostraciones en matemáticas, cada uno de los cuales se utiliza para abordar diferentes situaciones y problemas. Veremos algunos de los tipos más comunes utilizados en distintas áreas de la matemática.

Demostración directa

La **demostración directa** es el tipo de demostración más básico y común. Consiste en presentar una secuencia lógica de pasos y argumentos que llevan directamente desde las premisas hasta la conclusión deseada. Se utiliza cuando la relación entre las premisas y la conclusión es clara y se puede establecer de manera directa. Para llevar a cabo una demostración directa, se comienza con las premisas o supuestos iniciales y se aplican reglas lógicas y propiedades matemáticas para llegar a la conclusión deseada. Se evita el uso de suposiciones adicionales o técnicas más complejas, y se busca una argumentación clara y sencilla para demostrar la validez de la afirmación. Al examinar la tabla de verdad de la implicación lógica $P \Rightarrow Q$, podemos notar que para demostrar el teorema de la proposición $P \Rightarrow Q$, basta con mostrar que cuando P es verdadero, también lo es Q. Esto se debe a que la implicación $P \Rightarrow Q$ es verdadera cuando la premisa P es falsa, sin importar el valor de verdad de Q. Por lo tanto, en una demostración directa de $P \Rightarrow Q$, asumimos que la premisa P es verdadera y utilizamos argumentos lógicos para demostrar que la conclusión Q también es verdadera. En resumen, en una demostración directa de $P \Rightarrow Q$, nos enfocamos en establecer la validez de la relación entre la premisa y la conclusión, siguiendo el siguiente esquema lógico.

Esquema para una demostración directa

Proposición 1.1.16. *Si P, entonces Q.*

Demostración. Supongamos P,

$\vdots$

En consecuencias Q. □

Los puntos suspensivos $\vdots$ indican la secuencia de razonamientos lógicos que inician con P verdadero y finaliza con Q verdadero. El inicio de la demostración se inicia con *Demostración* o a veces solo colocamos la abreviación **Dem.** y se finaliza con el símbolo □ o también podemos finalizar con la expresión $Q.E.D$ que significa «Queda entonces demostrado». Como ejemplo, demostremos la siguiente proposición.

Proposición 1.1.17. *Si x es una solución de la ecuación $ax^2 + bx + c = 0$ con $a \neq 0$, entonces*

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Dem.
Supongamos que x es una solución de la ecuación $ax^2 + bx + c = 0$, es decir, satisface la ecuación.

Factorizamos a:

$$a\left(x^2 + \frac{b}{a}x + \frac{c}{a}\right) = 0.$$

Sumamos un cero dentro de los paréntesis como sigue $\left(\left(\frac{b}{2a}\right)^2 - \left(\frac{b}{2a}\right)^2 = 0\right)$:

$$a\left(x^2 + \frac{b}{a}x + \left(\frac{b}{2a}\right)^2 - \left(\frac{b}{2a}\right)^2 + \frac{c}{a}\right) = 0.$$

Como $\left(x+\frac{b}{2a}\right)^2 = x^2 + 2\frac{b}{2a}x + \left(\frac{b}{2a}\right)^2 = x^2 + \frac{b}{a}x + \left(\frac{b}{2a}\right)^2$, entonces

$$a\left(\left(x+\frac{b}{2a}\right)^2 - \left(\frac{b}{2a}\right)^2 + \frac{c}{a}\right) = 0.$$

Como $a \neq 0$, entonces $\frac{1}{a}a = 1$, así;

$$\left(x+\frac{b}{2a}\right)^2 - \left(\frac{b}{2a}\right)^2 + \frac{c}{a} = \frac{1}{a}a\left(\left(x+\frac{b}{2a}\right)^2 - \left(\frac{b}{2a}\right)^2 + \frac{c}{a}\right) = \frac{1}{a}0 = 0.$$

Esto es,

$$\left(x+\frac{b}{2a}\right)^2 - \left(\frac{b}{2a}\right)^2 + \frac{c}{a} = 0.$$

Despejamos el termino $\left(x+\frac{b}{2a}\right)^2$ para obtener: $\left(x+\frac{b}{2a}\right)^2 = \left(\frac{b}{2a}\right)^2 - \frac{c}{a} = \frac{b^2}{4a^2} - \frac{c}{a} = \frac{b^2-4ac}{4a^2}$. Así, sacando raíz cuadrada de ambos lados de la ecuación, obtenemos (sin olvidar el terminó $\pm$) lo siguiente:

$$x + \frac{b}{2a} = \pm\sqrt{\frac{b^2-4ac}{4a^2}} = \pm\frac{\sqrt{b^2-4ac}}{2a}.$$

Esto implica que:

$$x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}.$$

Q.E.D

Demostración por contrapositiva

La demostración por contrapositiva (o contrarecírpoca) es un método utilizado para demostrar una afirmación condicional $P \Rightarrow Q$ usando su equivalencia lógica $\neg Q \Rightarrow \neg P$. En otras palabras, en una demostración por contrapositiva, se supone inicialmente la negación de la conclusión ($\neq Q$) de la afirmación condicional y luego se muestra que esto implica la negación de la premisa ($\neq P$). Si se puede demostrar que la negación de la premisa es verdadera, entonces se concluye que la afirmación condicional original es verdadera. En resumen, es probar la proposición $\neg Q \Rightarrow \neg P$ de manera directa. Una demostración por contrapositiva sigue el siguiente esquema:

Esquema para una demostración por contrapositiva

Proposición 1.1.18. *Si P, entonces Q.*

Demostración. (por contrapositiva) Supongamos $\neg Q$,

$\vdots$

En consecuencias $\neg P$. □

Como ejemplo, demostraremos una misma proposición usando los dos métodos vistos hasta ahora.

Proposición 1.1.19. *Si x es un número entero divisible por 6, entonces x es divisible por 2 y por 3.*

Dem. (Directa).
Supongamos que x un número entero divisible por 6. Esto es, $x = 6k$, donde k es un número entero. Como $6 = (2)(3)$, entonces

$$x = 6k$$
$$x = (2)(3)k$$
$$x = 2(3k) = 3(2k)$$

Dado que $3k$ y $2k$ son números entero, concluimos que x es divisible por 2 y por 3. Por lo tanto, la afirmación condicional es verdadera.

$Q.E.D$

Dem. (Por contrapositiva).
Supongamos que x es un número entero que no es divisible por 2 o no es divisible por 3. Si x no es divisible por 2, entonces no puede ser divisible por 6, ya que 6 es divisible por 2. De manera similar, si x no es divisible por 3, entonces tampoco puede ser divisible por 6, ya que 6 es divisible por 3. Por lo tanto, si un número no es divisible por 2 o no es divisible por 3, no puede ser divisible por 6. Concluimos que x no es divisible por 6, y por lo tanto, la afirmación condicional original también es verdadera.

$Q.E.D$

Es importante tener en mente que **no hay una «mejor»demostración en general**, ya que la elección del método de demostración depende del contexto, la naturaleza del problema y las premisas dadas. Tanto la demostración directa como la demostración por contrapositiva son métodos válidos y ampliamente utilizados en matemáticas.

En algunos casos, la demostración directa puede ser más simple y directa, especialmente si se tienen todas las premisas necesarias para llegar a la conclusión deseada. Es un enfoque lineal y fácil de seguir, lo que lo hace más intuitivo y comprensible.

Sin embargo, en otros casos, la demostración por contrapositiva puede ser más efectiva. Puede ser útil cuando no se dispone de información directa o cuando se quiere evitar un razonamiento más complejo. La demostración por contrapositiva puede proporcionar una alternativa más clara o más sencilla para demostrar la afirmación condicional. El siguiente ejemplo, muestra que es más facil probarlo por contrapositiva.

Proposición 1.1.20. *Si x^2 es par, entonces x es par.*

Dem.(Por contrapositiva).
Sea $P : x^2$ es par y $Q :x$ es par. Supongamos $\neg Q$, esto es, x es impar. Existe a entero tal que

$$x = 2a + 1.$$

Así,

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

Por tanto, x^2 es impar, es decir, $\neg P$ es verdadera.

$Q.E.D$

En última instancia, la «mejor»demostración dependerá de las circunstancias específicas y de los objetivos de la demostración. Lo más importante es elegir un enfoque que sea lógico, riguroso y que permita demostrar la veracidad de la afirmación de manera clara y convincente.

Demostración por contradicción

La demostración por contradicción es otro método comúnmente utilizado en matemáticas para demostrar una proposición o teorema. Consiste en suponer inicialmente la negación de la afirmación que se desea demostrar y luego derivar una contradicción lógica o matemática a partir de esa suposición. Si se llega a una contradicción, se concluye que la afirmación original es verdadera.

Supongamos que queremos demostrar que una proposición P es verdadera. Una **demostración por contradicción** comienza suponiendo que P es falsa, esto es, $\neg P$ es verdadera, y finaliza deduciendo que para una cierta proposición C, se cumple también $\neg C$, en otras palabras, es una contradicción $(C \wedge \neg C)$. Por lo que una demostración por contradicción sigue el siguiente esquema.

Esquema para una demostración por contradicción

Proposición 1.1.21. *P.*

Demostración. (por contradicción) Supongamos $\neg P$.

$\vdots$

En consecuencias $C \wedge \neg C$. □

En este método, no está especificado claramente qué representa la proposición C. Sin embargo, el proceso de demostración por contradicción comienza asumiendo que la negación de la proposición P, $\neg P$, es verdadera y mediante razonamiento lógico se obtienen nuevas proposiciones que eventualmente conducen a una proposición C y su negación, $\neg C$. Veamos un ejemplo de esto.

Proposición 1.1.22. *El número $\sqrt{2}$ es irracional.*

Dem. (Por contradicción).
Sea P : el número $\sqrt{2}$ es irracional. Supongamos $\neg P$, esto es, $\sqrt{2}$ no es irracional. Entonces $\sqrt{2}$ es racional, entonces existen enteros a y $b$con $b \neq 0$ tales que

$$\sqrt{2} = \frac{a}{b}. \tag{1.1}$$

De hecho podemos suponer que la fracción $\frac{a}{b}$ está completamente simplificada. Esto es, a y b no tienen factores comunes. En particular, $2 \not| a$ y $2 \not| b$. Elevamos al cuadrado a ambos lados de la ecuación 1.1, obtenemos

$$2 = \frac{a^2}{b^2}. \tag{1.2}$$

esto es,

$$a^2 = 2b^2. \tag{1.3}$$

Esto implica que a^2 es par, entonces a es par (ver un ejemplo anterior). Como sabemos que a y b no son ambos pares, entonces b es impar, sea $C : b$ es impar, tenemos que C es verdadero. Ahora, existe r número entero tal que $a = 2r$, Así

$$4r^2 = 2b^2 \Rightarrow 2r^2 = b^2,$$

Esto es, b^2 es par, por lo que b es par, es decir, se cumple $\neg C$, En consecuencia $C \wedge \neg C$, es decir, una contradicción.

$Q.E.D$

Como mencionamos anteriormente, en muchas (casi todas) ocasiones nos encontramos con teoremas en forma de condicionales, es decir, de la forma $P \Rightarrow Q$. entonces ¿como se prueba por contradicción una condicional $P \Rightarrow Q$? Para responder esta cuestión, es importante recordar la equivalencia lógica antes mencionada $P \Rightarrow Q \equiv \neg P \vee Q$, por lo que $\neg(P \Rightarrow Q) \equiv P \wedge \neg Q$, así que el esquema de demostración por contradicción de $P \Rightarrow Q$ es la siguiente:

Esquema de demostración por contradicción de la proposición condicional

Proposición 1.1.23. *P.*

Demostración. (por cotradicción) Supongamos P y $\neg Q$.

$\vdots$

En consecuencias $C \wedge \neg C$. □

Como ejemplo, vamos a demostrar una proposición condicional que ya ha sido demostrada, pero esta vez utilizando el método de la contradicción.

Proposición 1.1.24. *Si x^2 es par, entonces x es par.*

Dem.(Por contradicción).
Sea $P : x^2$ es par y $Q : x$ es par. Supongamos P y $\neq Q$, es decir, que x^2 es par y que x no es par, es decir, x es impar. Entonces, existe a entero tal que

$$x = 2a + 1.$$

Así,

$$\begin{aligned} x^2 &= (2a+1)^2 = 4a^2 + 4a + 1 \\ &= 2(2a^2 + 2a) + 1 \\ &= 2k + 1 \quad (k = 2a^2 + 2a). \end{aligned}$$

Esto es, x^2 es impar, es decir, $\neg P$ (aquí la proposición C es P). Por lo tanto, $P \wedge \neg P$ (contradicción).

$Q.E.D$

Demostración de bicondicionales

Sabemos que una proposición bicondicional *P si y solo si Q* es lógicamente equivalente a

(Si P, entonces Q) y (si Q, entonces P).

Por lo tanto, para demostrar una proposición de este estilo, debemos demostrar las dos proposiciones; $P \Rightarrow Q$ ((Si P, entonces Q) y $Q \Rightarrow P$ (si Q, entonces P). Así, la demostración de una bicondicional tiene el siguiente esquema:

Esquema de demostración de una proposición bicondicional

Proposición 1.1.25. $P \iff Q$.

Demostración. (No olvidar que $P \iff Q \equiv (P \Rightarrow Q) \wedge (Q \Rightarrow P)$)

Demostrar $P \Rightarrow Q$ (usando demostración directa, por contradicción, contrapositiva)

Demostrar $Q \Rightarrow Q$ (usando demostración directa, por contradicción, contrapositiva) □

Tipos de proposiciones

Podemos decir que hay tres tipos de proposiciones matemáticas:

1. **Proposiciones verdaderas (ya han sido probadas)**: Teoremas, lemas, corolarios y lo que llamamos de manera redundante proposiciones.

2. **Conjeturas:** Una conjetura es una afirmación o proposición que se cree que es verdadera, pero que aún no ha sido demostrada o verificada de manera rigurosa. En otras palabras, es una suposición o idea que se plantea como posible solución a un problema o como una afirmación que podría ser cierta, pero que aún requiere una demostración formal. Cabe mencionar que pueden resultar falsas.

3. **Proposiciones falsas.** Por ejemplo, «todos los números primos son impares»es falso, pues el 2 es par y es primo.

La última categoría nos lleva a la cuestión, ¿como probamos que una proposición es falsa? Para demostrar que una proposición es falsa, es necesario encontrar un contraejemplo, es decir, un caso en el cual la proposición no se cumpla. En otras palabras, se busca encontrar una situación, una configuración o un conjunto de valores que contradigan la afirmación que se está evaluando.

El proceso para demostrar que una proposición es falsa generalmente implica lo siguiente:

1. Entender la proposición: Comprender claramente cuál es la afirmación o proposición que se está evaluando. Es importante analizar todas las condiciones y suposiciones asociadas a la afirmación para tener una comprensión precisa de lo que se está afirmando.

2. Buscar un contraejemplo: Se procede a buscar un caso o una situación específica que contradiga la afirmación. Esto implica encontrar un conjunto de valores o condiciones que cumplan todas las condiciones de la proposición, pero que no satisfagan su conclusión. En otras palabras, se busca un caso que muestre que la proposición no se cumple en todos los casos posibles.

3. Presentar el contraejemplo: Una vez que se ha encontrado un contraejemplo, se debe presentar claramente y de manera precisa. Esto implica mostrar cómo los valores o las condiciones del contraejemplo contradicen la afirmación de la proposición. Es fundamental proporcionar una descripción detallada y explicar por qué el contraejemplo es válido y cómo refuta la proposición.

4. Concluir la falsedad de la proposición: Basándose en el contraejemplo presentado, se puede concluir que la proposición es falsa, ya que se ha encontrado al menos un caso en el cual no se cumple.

Es importante tener en cuenta que la existencia de un contraejemplo es suficiente para demostrar que una proposición es falsa. Sin embargo, si no se puede encontrar un contraejemplo, no se puede concluir que la proposición es necesariamente verdadera. En ese caso, la proposición puede requerir una prueba rigurosa o puede necesitar ser evaluada en un contexto más amplio.

En resumen, para demostrar que una proposición es falsa, se busca encontrar un contraejemplo que contradiga la afirmación. Esto implica encontrar un caso específico en el cual las condiciones de la proposición se cumplan, pero la conclusión no se satisfaga. Al presentar un contraejemplo válido, se puede concluir que la proposición es falsa.

1.1.6. Sintaxis de la logica proposicional

En sintaxis, tanto el la logica formal como en los lenguajes de programación se debe de determinar qué expresiones constituyen cadenas bien estructuradas (fórmulas o programas), sin atender a su interpretación semántica ni a su finalidad práctica. Esta determinación se formaliza mediante una definición recursiva, en primer lugar, cuáles son las fórmulas atómicas, y posteriormente precisa las reglas a través de las cuales es posible componer fórmulas más complejas a patir de ellas.

Definición 1.1.26. *Sea $\mathcal{D}$ una colección de proposiciones atomicas. Definimos $\mathcal{E}_\mathcal{D}$ como el conjunto de fórmulas sintacticamente correctas que cumple con las siguientes:*

- $\mathcal{D} \subseteq \mathcal{E}_\mathcal{D}$.
- *Si $f, g \in \mathcal{E}_\mathcal{D}$, entonces $(f \vee g), (f \wedge g), (\neg f) \in \mathcal{E}_\mathcal{D}$.*

En palabras, $\mathcal{E}_\mathcal{D}$ consiste en proposiciones atómicas (átomos), así como aquellas construidas mediante los conectores $\vee, \wedge, \neg$. Es importante mencionar y observar que los conectores $\rightarrow, \leftrightarrow, \oplus$ no forman parte explicita de la sintaxis básica, pero si que estan incluidos de manera implicita, pues pueden expresarse como equivalencias logicas usando unicamente los conectores básicos.

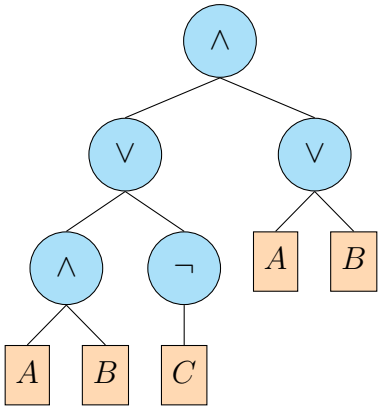
■ **Ejemplo 1.1.27.** *Las siguientes son ejemplos de formulas sintácticamente correctas. (De momento, no es posible omitir paréntesis en su escritura).*

- A
- $(\neg A)$
- $(A \vee B)$
- $(A \wedge B)$
- $(\neg (A \wedge B))$
- $T := (((A \wedge B) \vee (\neg C)) \wedge (A \vee B))$

La estructura de la fórmula T puede representarse mediante una «gráfica» denominado **árbol sintáctico**. En este árbol, cada subárbol corresponde a una subfórmula (es decir, a una subcadena que constituye por sí misma una fórmula bien formada). Las subfórmulas de P son:

$$\{A, B, C, (A \wedge B), (\neg C), ((A \wedge B) \vee (\neg C)), (A \vee B), F\}$$

El árbol sintáctico de T es el siguiente:



Considerando la exigencia estricta de pedir colocar los parentesis entonces las fórmulas $P \vee Q \vee R$, $P \wedge Q \vee R$ no son correctas, pues hacen falta parentesis. La pertinencia de admitir la omisión de los paréntesis o no está condicionada a que el valor de verdad de la expresión lógica se vea o no afectado por su disposición de estos. La semantica nos ayudara a resolver esto, es decir, nos ayudara a determinar determinar cuando si o cuando no se puede precendir de los parentesis. Basicamente es cuando no tenga cavidad la ambiguedad.

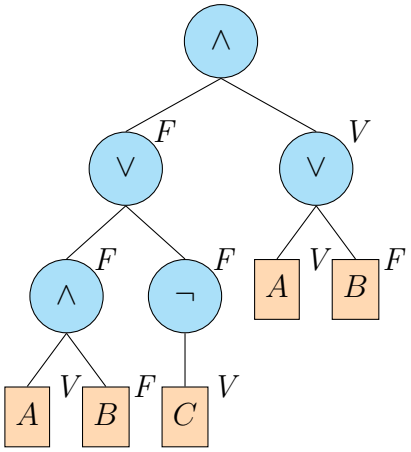
1.1.7. Semantica de la logica proposicional

Definición 1.1.28. *Sea $\mathcal{D}$ una colección de átomos. Se denomina* ***función asignación (de verdad)*** *a la función $\mathcal{A} : \mathcal{D} \longrightarrow \{F, V\}$ que asocia a cada átomo un valor de verdad.*

Ahora, dada una colección de átomos $\mathcal{D}$, la sintaxis $\mathcal{E}_{\mathcal{D}}$ y una asignación $\mathcal{A} : \mathcal{D} \longrightarrow \{F, V\}$. ¿Como construimos una asignación a toda la sintaxis? Bueno, digamos que se puede pensar que la asignación $\mathcal{A}$ se puede prolongar a cualquier fórmula bien formada, determinando su valor de verdad a partir de los valores asignados a los átomos y de las reglas semánticas correspondientes a los conectivos lógicos involucrados. Cuando veamos funciones, se entendera que significa «prolongar o extender». De momento usaremos la misma letra para referirnos la extención de la asignación dada.

■ **Ejemplo 1.1.29.** *Sea $\mathcal{D} = \{A, B, C\}$ una colección de fórmulas atómicas. Consideremos la asignación $\mathcal{A} : \mathcal{D} \longrightarrow \{F, V\}$ dada por $\mathcal{A}(A) = V$, $\mathcal{A}(B) = F$ y $\mathcal{A}(C) = V$.*

¿Cuál es el valor de $\mathcal{A}(T)$ con $T = (((A \wedge B) \vee (\neg C)) \wedge (A \vee B))$? Observese que es la misma formula T usada para ejemplificar el árbol sintáctivo. Enconces, usando el árbol sintáctico para encontrar $\mathcal{A}(T)$ y se usa evaluando de abajo hacia arriba, observe la siguiente figura:



Por lo tanto, $\mathcal{A}(T) = F$.

Definición 1.1.30 (Comportamiento semántico/Vector de verdad)**.** *El comportamiento semántico o vector de verdad de una proposición es la lista de valores de verdad para todas las asignaciones posibles de sus fórmulas atómicas.*

El comportamiento semantico se puede puede expresar completamente en una tabla de verdad.

Decimos que dos fórmulas son *semánticamente equivalentes* si producen el mismo resultado con la misma entrada. Las fórmulas equivalentes pueden intercambiarse entre sí en cualquier contexto lógico; son «lógicamente equivalentes».

Definición 1.1.31 (Equivalencia semantica)**.** *Sean* G *y* H *fórmulas sintacticamente correctas. Diremos que* H *es semanticamente equivalente a* G *si cualquier asignación posible de valores de verdad a sus componentes atómicos, ambas expresiones resultan con el mismo valor de verdad. Esta relación se representa mediante la notación* $G \equiv H$ *(ó* $G \iff H$*).*

Observación. Note que si G es una tautología, entonces para cualquier asignación $\mathcal{A}$, $\mathcal{A}(G) = V$. Similarmente si G es una formula insatisfacible(contradicción) , entonces para cualquier asignación $\mathcal{A}$, $\mathcal{A}(G) = F$.

Como ejemplo de equivalencia semantica tenemos:

$$P \to Q \equiv \neg Q \to \neg P.$$

Definición 1.1.32. *Definimos las formulas*

$\boldsymbol{F} \equiv (A \wedge (\neg A))$,

$\boldsymbol{V} \equiv (A \vee (\neg A))$.

Definición 1.1.33. *Si una formula* $\mathbb{F}$ *es semánticamente equivalente a* $\boldsymbol{F}$*,* $\mathbb{F} \equiv \boldsymbol{F}$*, entonces* $\mathbb{F}$ *se llama insatisfacible. Y si es semánticamente equivalente a* $\boldsymbol{V}$*,* $\mathbb{F} \equiv V$ *entonces decimos que* $\mathbb{F}$ *es una tautología.*

Denotaremos XOR con el simbolo $\oplus$. Se deja al lector verificar las siguientes equivalencias:

$$P \oplus Q \equiv ((P \wedge (\neg Q)) \vee ((\neg P) \wedge Q))$$

Y para la bicondicional tendremos:

$$P \leftrightarrow Q \equiv (A \wedge B) \vee ((\neg A) \wedge (\neg B)) .$$

Observación. La equivalencia semantica es una relación de equivalencia, este último concepto lo veremos en la sección de teoria de conjuntos.

Teorema 1.1.34. *Sean G y H formulas. $G \equiv H$ si y solo si $G \leftrightarrow H$ es una tautología.*

Dem.
Sean G y H formulas.

$\Rightarrow$) Supongamos que $G \equiv H$. Sea $\mathcal{A}$ cualquier asignación, entonces

$$\mathcal{A}(G) = \mathcal{A}(H) \text{ (por hipotesis).}$$

Así, $\mathcal{A}(G \leftrightarrow H) = V$, esto es, $G \leftrightarrow H$ es una tautología.

$\Leftarrow$) Supongamos que $G \leftrightarrow H$ es una tautología. Veamos que $G \equiv H$. Si $G \not\equiv H$, entonces existe una asignación $\mathcal{A}$ tal que $\mathcal{A}(G) \neq \mathcal{A}(H)$.

- Si $\mathcal{A}(G) = V$, entonces $\mathcal{A}(H) = F$. Así, $\mathcal{A}(G \leftrightarrow H) = F$.
- Si $\mathcal{A}(G) = F$, entonces $\mathcal{A}(H) = V$. Así, $\mathcal{A}(G \leftrightarrow H) = F$.

Esto implica que $\mathcal{A}(G \Leftrightarrow H) = F$, lo cual no es posible pues $G \Leftrightarrow H$ es una tautología.

$Q.E.D$

La siguiente lista contiene ejemplos importantes de equivalencias logicas a las que llamamos **leyes logicas**.

Idempotencia:

$$P \wedge P \equiv P$$
$$P \vee P \equiv P$$

Ley de identidad:

$$P \wedge \mathbf{V} \equiv P$$
$$P \vee \mathbf{F} \equiv P$$

Ley de contradicción:

$$P \wedge \mathbf{F} \equiv \mathbf{F}$$
$$P \vee \mathbf{V} \equiv \mathbf{V}$$

Leyes de la negación:

$$\neg(\neg P) \equiv P$$
$$P \wedge \neg P \equiv \mathbf{F}$$
$$P \vee \neg P \equiv \mathbf{V}$$

Leyes conmutativas:

$$P \wedge Q \equiv Q \wedge P$$
$$P \vee Q \equiv Q \vee P$$

Leyes asociativas:

$$(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$$
$$(P \vee Q) \vee R \equiv P \vee (Q \vee R)$$

Leyes distributivas:

$$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$$
$$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$$

Doble negación:

$$(\neg (\neg P)) \equiv P$$

De Morgan:

$$(\neg (P \wedge G)) \equiv ((\neg P) \vee (\neg Q))$$
$$(\neg (P \vee G)) \equiv ((\neg P) \wedge (\neg Q))$$

La verificación se plantea como ejercicio adicional.

Hasta ahora nos hemos apegado a la escritura y notación definida despues de la sintaxis. Pero es momento de introducir algunas notaciones y simplificaciones que nos ayudarán de mucho con la notación.

- Considerando la definición de sintaxis no estan explicitamente dichos conectres que hemos tratado, a saber: $\oplus, \rightarrow, \leftrightarrow$, sin embargo, los hemos introducido desde la primera parte, ahora sabemos que son equivalentes a fórmulas con los conectores básicos $(\neg, \wedge, \vee)$.
- Como tal los paréntesis no cambian el comportamiento semantico de una formula, es decir, su tabla de verdad, entonces pueden omitirse ciertos paréntesis siempre que no exista confusion o ambiguedad.

  Por ejemplo, debido a la asociatividad, podemos escribir $A \wedge B \wedge C$ en lugar de $((A \wedge B) \wedge C)$. En general, esto nos permite introducir la siguiente notación:

$$\bigwedge_{i=1}^{n} A_i \equiv A_1 \wedge A_2 \wedge \cdots \wedge A_n,$$

$$\bigvee_{i=1}^{n} A_i \equiv A_1 \vee A_2 \vee \cdots \vee A_n.$$

- Ahora, que hemos dicho que podemos omitir ciertos parentesis, es necesario introducimos las siguientes reglas de prioridad (precedencia de operadores, algo así como la gerarquia de operaciones vista a nivel básico en preparatoria) sería de la siguiente manera: operadores básicos primero; $\neg$, luego $(\wedge, \vee)$, y después $(\oplus, \leftarrow, \rightarrow, \leftrightarrow)$. Nuevamente, los paréntesis pueden omitirse y la fórmula se lee de acuerdo con estas reglas de prioridad. Por ejemplo:

  $$P \wedge \neg Q \rightarrow R$$

  representa

  $$((P \wedge (\neg Q)) \rightarrow R)\,.$$

1.1.8. Formas normales

Cuando tenemos una fórmula lógica correctamente escrita (sintácticamente correcta), podemos determinar su comportamiento semantico realizando su tabla de verdad. Esta tabla nos dice exactamente cuándo la fórmula es verdadera y cuándo es falsa según los valores de sus variables.

La pregunta que surge ahora es: ¿podemos hacer lo contrario? Es decir, si nos dan la tabla de verdad con todas las entradas correspondientes en cada fila (a las filas de una tabla de verdad se le llama **vector de verdad**), ¿es posible construir una fórmula lógica que produzca exactamente esos valores de verdad?

La respuesta es sí, y existen métodos sistemáticos para hacerlo. Los que veremos aquí, se conocen como: la **Forma normal disyuntiva (FND)** o la **forma normal conjuntiva (FNC)**, que consiten basicamente en tomar cada fila de la tabla de verdad donde la fórmula debe ser verdadera (para FND) o falsa (para FNC) y construir una expresión que reproduzca exactamente esos resultados.

Para entenderlas, nos apoyaremos de un ejemplo para mostrar paso a paso cómo se construye dicha formula usando la FND o la FNC, claro todo a partir de una tabla de verdad dada, y hay que aseguranos que la fórmula resultante sea sintácticamente correcta y tenga el mismo comportamiento semántico que la dada en la tabla de verdad.

■ **Ejemplo 1.1.35.** *Consideremos tres variables proposicionales P, Q y R, y la fórmula $\mathcal{F}$, así como la asignación $\mathcal{A}$ que produce la siguiente tabla de verdad:*

P	Q	R	$\mathcal{F}$
V	V	V	V
V	V	F	V
V	F	V	F
V	F	F	F
F	V	V	V
F	V	F	F
F	F	V	V
F	F	F	F

Para construir la Forma Normal Disyuntiva (FND) de $\mathcal{F}$ vamos a considerar todas las filas donde $\mathcal{F}$ es verdadera. Cada fila verdadera genera una fórmula obtenida de las proposiciones involucradas y son conectadas mediante $\wedge$ colocando la proposición o su negación dependicendo de si es verdadera o falsa, según sea el caso. Esto es,

- *Para la fila 1, tenemos que:* $\mathcal{A}(P) = V, \mathcal{A}(Q) = V, \mathcal{A}(R) = V$. *Entonces la formula que le asociamos es:*

$$P \wedge Q \wedge R$$

- *Para la fila 2, tenemos que:* $\mathcal{A}(P) = V, \mathcal{A}(Q) = V, \mathcal{A}(R) = F$. *Así, la formula asociada es:*

$$P \wedge Q \wedge \neg R$$

- *Para la fila 5, tenemos que:* $\mathcal{A}(P) = F, \mathcal{A}(Q) = V, \mathcal{A}(R) = V$. *Por lo que la formula que le asociamos es:*

$$\neg P \wedge Q \wedge R$$

- *Para la fila 7, tenemos que:* $\mathcal{A}(P) = F, \mathcal{A}(Q) = F, \mathcal{A}(R) = V$. *Onteniendo la formula:*

$$\neg P \wedge \neg Q \wedge R$$

Unimos estas conjunciones mediante $\vee$ *para obtener la FND:*

$$\mathcal{F} \equiv (P \wedge Q \wedge R) \vee (P \wedge Q \wedge \neg R) \vee (\neg P \wedge Q \wedge R) \vee (\neg P \wedge \neg Q \wedge R)$$

A esto se le conoce como ***Forma Normal Disyuntiva Canonica****, está forma se puede llevar a una más simple usando las leyes logicas pero sin perder la forma de disyucion de conjunciones.*

Agrupando términos:

$$\mathcal{F} \equiv ((P \wedge Q) \wedge (R \vee \neg R)) \vee ((\neg P \wedge R) \wedge (Q \vee \neg Q))$$

Como $R \vee \neg R = \boldsymbol{V}$ *y* $Q \vee \neg Q = \boldsymbol{V}$. *Entonces,*

$$\mathcal{F} \equiv (P \wedge Q) \vee (\neg P \wedge R).$$

A esta forma se le llama ***Forma Normal Disyuntiva Simplificada (FNDS)****.*

Ahora, para construir la ***Forma Normal Conjuntiva (FNC)*** *de* $\mathcal{F}$ *vamos a considerar* todas las filas donde $\mathcal{F}$ es falsa*. Cada fila falsa genera una fórmula (una disyunción de las proposiciones involucradas) que se hace falsa exactamente en esa fila. La regla práctica para formar la fórmula a partir de una fila es:* ***si la proposición es*** V ***en la fila, tomamos la negación de la proposición; si es*** F***, tomamos la proposición.***

Así, para cada fila falsa:

- ***Fila 3:*** $\mathcal{A}(P) = V,\ \mathcal{A}(Q) = F,\ \mathcal{A}(R) = V,\ \mathcal{A}(\mathcal{F}) = F$. *Fórmula:*

$$(\neg P \vee Q \vee \neg R).$$

- ***Fila 4:*** $\mathcal{A}(P) = V,\ \mathcal{A}(Q) = F,\ \mathcal{A}(R) = F,\ \mathcal{A}(\mathcal{F}) = F$. *Fórmula:*

$$(\neg P \vee Q \vee R).$$

- ***Fila 6:*** $\mathcal{A}(P) = F,\ \mathcal{A}(Q) = V,\ \mathcal{A}(R) = F,\ \mathcal{A}(\mathcal{F}) = F$. *Fórmula:*

$$(P \vee \neg Q \vee R).$$

- ***Fila 8:*** $\mathcal{A}(P) = F,\ \mathcal{A}(Q) = F,\ \mathcal{A}(R) = F,\ \mathcal{A}(\mathcal{F}) = F$. *Fórmula:*

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

Unimos estas fórmulas mediante $\wedge$ *para obtener la* ***FNC canónica****:*

$$\mathcal{F} \equiv (\neg P \vee Q \vee \neg R) \ \wedge \ (\neg P \vee Q \vee R) \ \wedge \ (P \vee \neg Q \vee R) \ \wedge \ (P \vee Q \vee R).$$

Esta es la ***Forma Normal Conjuntiva Canónica****. Al igual que la FND, podemos llevarla a una más simple haciendo uso de las leyes logicas. Como sigue:*

- *De* $(\neg P \vee Q \vee \neg R)$ *y* $(\neg P \vee Q \vee R)$ *se obtiene la fórmula más corta*

$$\neg P \vee Q.$$

- *De* $(P \vee \neg Q \vee R)$ *y* $(P \vee Q \vee R)$ *se obtiene la fórmula*

$$P \vee R.$$

Por tanto la FNC se reduce a

$$\mathcal{F} \equiv (P \vee R) \ \wedge \ (\neg P \vee Q).$$

A esta forma se le llama ***Forma Normal Conjuntiva Simplificada (FNCS)****. Nótese que ambas representaciones (la FNC canónica y la FNC simplificada) son semanticamente equivalentes a* $\mathcal{F}$*.*

Veamos las tablas de verdad de la FNDS y la FNCS para compararlas y verificar que son sementicamente equivalentes a $\mathcal{F}$*:*

P	Q	R	$P \wedge Q$	$\neg P \wedge R$	***FNDS***	$P \vee R$	$\neg P \vee Q$	***FNCS***
V	V	V	V	F	V	V	V	V
V	V	F	V	F	V	V	V	V
V	F	V	F	F	F	V	F	F
V	F	F	F	F	F	V	F	F
F	V	V	F	V	V	V	V	V
F	V	F	F	F	F	F	V	F
F	F	V	F	V	V	V	F	V
F	F	F	F	F	F	F	F	F

Hemos construido la ***FND*** *y la* ***FNC*** *de* $\mathcal{F}$ *a partir de su tabla de verdad, mostrando paso a paso cómo cada fila verdadera o falsa contribuye a formar las formas normales.*

Definamos de manera general las formas normales FND y FNC.

Definición 1.1.36 (Literal)**.** *Si* $L \in \mathcal{D}$ *es un atomo, entonces* L *y* $\neg L$ *se llaman literales. Una* ***literal*** *es un átomo o la negación de un átomo.*

Definición 1.1.37 (Forma Normal Conjuntiva)**.** *Una fórmula $\mathcal{F}$ está en* ***Forma Normal Conjuntiva (FNC)*** *si existe $n \in \mathbb{N}$ y para cada $i \in \{1, 2, \ldots, n\}$ existe $m_i \in \mathbb{N}$ y hay literales $L_{i,j}$ tales que:*

$$\begin{aligned}\mathcal{F} = &\bigwedge_{i=1}^{n} \left(\bigvee_{j=1}^{m_i} L_{i,j} \right) \\ = &(L_{1,1} \vee L_{1,2} \vee \cdots \vee L_{1,m_1}) \\ &\wedge (L_{2,1} \vee \cdots \vee L_{2,m_2}) \\ &\vdots \\ &\wedge (L_{n,1} \vee \cdots \vee L_{n,m_n}) .\end{aligned}$$

Definición 1.1.38 (Forma Normal Conjuntiva)**.** *Una fórmula $\mathcal{F}$ está en* ***Forma Normal Disyuntiva (FND)*** *si existe $n \in \mathbb{N}$ y para cada $i \in \{1, 2, \ldots, n\}$ existe $m_i \in \mathbb{N}$ y hay literales $L_{i,j}$ tales que:*

$$\mathcal{F} = \bigvee_{i=1}^{n} \left(\bigwedge_{j=1}^{m_i} L_{i,j} \right)$$

Observese que en estas definiciones colocamos igualdad ($=$) y no equivalencia semantica ($\equiv$), pues las formas normales son tambien nociones sintacticas.

1.1.9. Modelos y conclusión semántica

1.1.10. El cálculo de resolución

1.2. Teoría de conjuntos

1.2.1. Álgebra de conjuntos

1.2.2. Relaciones y funciones

1.2.3. Relaciones de orden

1.2.4. Retículas

1.2.5. carnalidad

El concepto de función es muy importante en la matemática, su entendimiento facilita muchas cosas.

Ahora, antes de iniciar este primer capitulo, es necesario recordar algunos significados de ciertos símbolos matemáticos que se usaran en todo el curso:

- $=$ significa: «igual a».
- $\neq$ significa: «diferente a» o «no es igual a».
- $\approx$ significa: «aproximadamente igual a».

- Dos puntos (:) o una barra vertical (|) se usan para decir: «tal que» o «tales que». Así mismo $t.q.$ significa lo mismo («tal que» o «tales que»)
- $i.e.$ o $e.d.$ significa: «es decir».
- $\in$ significa: «pertenece a».
- $\notin$ significa: «no pertenece a».

1.3. Definición de conjuntos y ejemplos

Definición 1.3.1. *Un **conjunto** es una colección de objetos.*

Si pensemos en alguna analogía del concepto de conjunto sobre el mundo físico, sería algo así como un contenedor de objetos o una bolsa que contiene ciertos objetos. Ahora, al considerar un conjunto, se nos viene a la mente los miembros o elementos que lo constituyen (que están dentro de), de tal forma que desde el inicio hay una relaciÓn entre los elementos y los conjuntos, a saber, un elemento estar dentro o no de un conjunto dado. Para denotar esto, es necesario introducir notación matemática.

Se usan las llaves:{} para denotar a los conjuntos y dentro de dichas llaves escribimos los elementos que están dentro de este conjunto o escribimos los elementos que cumplen alguna propiedad. Consideremos los siguientes ejemplos para su mayor entendimiento.

■ **Ejemplo 1.3.2.** *El conjunto de las vocales, se puede escribir de dos maneras diferentes y son:*

- $\{x : x \text{ es una vocal}\}$
- $\{a, e, i, o, u\}$

En el ejemplo previo, ambos hacen referencia al mismo conjunto, pero escrito de diferente manera, en una las enlistan completamente y en la otra considera los elementos que cumplen la condición (o propiedad) que sean una vocal.

■ **Ejemplo 1.3.3.** *El conjunto de* $\square, \triangle, *$ *se escribe como:*

$$\{\square, \triangle, *\}$$

■ **Ejemplo 1.3.4.** *El conjunto de los numeros* $1, \pi, e, \sqrt{7}, -\frac{1}{2}$ *se escribe como:*

$$\left\{1, \pi, e, \sqrt{7}, -\frac{1}{2}\right\}$$

Ahora, estar escribiendo las llaves y los elementos un conjunto tiene dentro se vuelve complicado. imagina que estemos trabajando una y otra vez con el mismo conjunto y tengamos que escribir todos cada que lo mencionamos, se volvería tedioso y cansado, es por ello que se prefiere darles nombres(bautizar a los conjuntos) y por lo general usamos las letras mayúsculas del abecedario: $A, B, C, \ldots, X, Y, Z$, por ejemplo, sea $A = \{\pi, e\}$, entonces a dicho conjunto ya lo podemos identificar como A, así, cada que nos refiramos al conjunto A sabemos que se refiere al conjunto que tiene los elementos π, e sin necesidad de volver a escribirlos todos. Ahora, existen conjuntos bien conocidos de su curso de Álgebra I y son los siguientes:

- El conjunto de números naturales cuya representación es $\mathbb{N}$. Sin embargo, existe una controversia aquí y es si el cero se considera número natural o no, la respuesta a está incognita es lo que te digan que es, pues hay quienes lo consideran natural y quienes no, en otras palabra, dependerá de quien aborde el tema, para evitar controversias con eso usaremos las siguientes notaciones:
  - $\mathbb{N} := \{1, 2, 3, 4, \dots\}$ (No incluye al cero)
  - $\mathbb{N}_0 := \{0, 1, 2, 3, 4, \dots\}$ (Incluye al cero)
- Los números enteros: $\mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\}$.
- Los racionales: $\mathbb{Q} := \left\{\frac{a}{b} : a, b \in \mathbb{Z} \text{ con } b \neq 0\right\}$. Estos números tienen la particularidad que al escribirlos en su expansión decimal son finitos o infinitos pero periódicos.
- Hay números cuya expansión en punto decimal son infinitos y sin periodo (patrón). A estos números se les llaman números irracionales. Es decir, los números que no son racionales se llaman irracionales y se denotan como $\mathbb{I}$. Ejemplos de estos número son: π, e, $\sqrt{p}$ con p número primo.
- Finalmente, los números reales que cotejan todos los números que conocemos a nivel básico y se denotan como $\mathbb{R}$.

Con base en el conocimiento previo de Álgebra I, se sabe que todo número natural es entero, todo entero es racional y todo racional es real. Entonces de alguna manera necesitamos introducir un concepto que nos indique cuando todos los elementos de un conjunto están en otro.

Definición 1.3.5. *Dados A y B conjuntos. Diremos que A está contenido en B, si todos los elementos de A están en B y se denota como: $A \subseteq B$. En símbolos,*

$$A \subseteq B \text{ si y solo si para cada } x \in A, x \in B$$

■ **Ejemplo 1.3.6.** $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$ *y* $\mathbb{I} \subseteq \mathbb{R}$

Definición 1.3.7. *Dos conjuntos A y B son inguales si $A \subseteq B$ y $B \subseteq A$.*

1.4. Operaciones en conjuntos

Dado 2 conjuntos X, Y, ¿Como genero otros a partir de ellos? Si bien hay mcuhas maneras de hacerlos veremos unicamente algunas operaciones importante de esto.

Definición 1.4.1 (**Union de conjuntos**). *Dados A y B conjuntos, se define la unión de A con B como la colección de elementos de A junto con los de B y se denota como $A \cup B$. En símbolos,*

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

Capítulo 2

Teoría de Números, Álgebra Abstracta y Criptografía

2.1. Teoría de Números Avanzada

2.1.1. Números primos

2.1.2. Factorización

2.1.3. Test de primalidad

2.1.4. Congruencias

2.1.5. Raíces primitivas

2.2. Estructuras Algebraicas

Para hablar de las estructuras básicas del álgebra moderna es necesario introducir un concepto muy importante y es la de *operación binaria*, que definiremos enseguida.

Definición 2.2.1. *Sean A, B, C conjuntos no vacíos. Una asociación $\circ : A \times B \longrightarrow C$ se llama **operación binaria** si se cumple que:*

$$\forall (a, b) \in A \times B, \circ(a, b) \in C.$$

Como ejemplo tenemos las operaciones de suma y procucto que se conocen en $\mathbb{R}$, $\mathbb{C}$, $\mathcal{M}_{n\times n}(\mathbb{K})$, etc. Es importante mencionar que $\circ(a, b)$ por lo general lo denotamos como $a \circ b$ por simplicidad.

Definición 2.2.2. *Sea $(S, \circ)$ un par, donde S es un conjunto no vacío y $\circ : S \times S \longrightarrow S$ es una operación binaria. Diremos que $(S, \circ)$ es un semigrupo si cumple la siguiente:*

- *Asociatividad: $\forall a, b, c \in S$,*

$$a \circ (b \circ c) = (a \circ b) \circ c.$$

Como ejemplo tenemos los pares $(\mathbb{N}, +), (\mathbb{N}, \cdot)$ donde $+$ y $\cdot$ son las operaciones de suma y producto de los numeros naturales, respectivamente. Sabemos de la suma y multiplicación de los reales que a cualquier numero real r al sumarle 0 no lo modifica, esto es,

$r+0 = 0+r = r$ o que al multiplicarlo por 1 tampoco lo modifica, es decir, $1 \cdot r = r \cdot 1 = r$. A estos se les conoce como neutros. Si a un semigrupo le pedimos que tenga un elemento de esa naturaleza entocnes se comvierte en algo que llamamos monoide.

Definición 2.2.3. *Sea $(M, \circ)$ un semigrupo. Diremos que $(M, \circ)$ es un monoide si existe $e \in M$ tal que para cada $a \in M$, $a \circ e = e \circ a = a$.*

En otras palabras, $(M, \circ)$ es un monoide si cumple las siguientes:

1) Asociatividad: para cada $a, b, c \in M$,

$$a \circ (b \circ c) = (a \circ b) \circ c.$$

2) Existencia del neutro: existe $e \in M$, tal que para todo $a \in M$,

$$e \circ a = a \circ e = a$$

Como ejemplo de monoide tenemos a $(\mathbb{N}, \cdot)$ cuyo neutro es el 1. Tambien en los reales para cada numero real r tenemos que $r - r = 0$ y si ademas, $r \neq 0$, entocnes $r\left(\frac{1}{r}\right) = rr^{-1} = 1$, a esto se les llama inversos aditivos y multiplicativos, repectivamente. Cuando le exigimos a un monoide que todos sus elementos tenga un opuesto, se conjetura una estructura llamada grupo. En la siguiente subsección hablaremos de esta estructura con un poco de detalle, digo poco, pues estudiaremos lo necesario y suficiente para desarrorar los algoritmos que veremos en este curso.

2.2.1. Grupos

Definición 2.2.4. *Sea G un conjunto no vació y $\circ : G \times G \longrightarrow G$ una operción binaria. Diremos que $(G, \circ)$ es un grupo si cumple las siguientes:*

1) Asociatividad: para cada $a, b, c \in M$,

$$a \circ (b \circ c) = (a \circ b) \circ c.$$

2) Existencia del neutro: existe $e \in M$, tal que para todo $a \in M$,

$$e \circ a = a \circ e = a$$

3) Cerrado bajo inversos: Para cada $a \in G$

2.2.2. Anillos

2.2.3. Campos

2.3. Criptográfica

2.3.1. Cifrado simétrico

2.3.2. Cifrado asimétrico

2.3.3. Protocolos criptográficos

Capítulo 3

Combinatoria Avanzada y Teoría de Probabilidad

3.1. Funciones generadoras

3.1.1. Funciones generadoras ordinarias

3.1.2. Funciones generadoras exponenciales

3.2. Teoría de probabilidad

3.2.1. Espacios de probabilidad

3.2.2. Variables aleatorias

3.2.3. Distribuciones de probabilidad discretas

3.2.4. Distribuciones de probabilidad continuas

3.2.5. Esperanza, varianza y momentos

3.2.6. Teorema del limite central

3.2.7. Ley de los grandes números

3.3. Procesos estocásticos

3.3.1. Cadenas de Markov

Capítulo 4

Teoría de Gráficas y optimización combinatoria avanzada

4.1. Teoría de Gráficas

4.1.1. Gráficas, gráficas dirigidas

4.1.2. Gráficas ponderadas

4.1.3. Conectividad

4.1.4. Caminos más cortos

4.1.5. flujos en redes

4.1.6. Emparejamientos

4.1.7. Planaridad

4.1.8. Coloración

4.2. Optimización combinatoria

4.2.1. Programación lineal entera

4.2.2. Algoritmos de ramificación y acotamiento

4.2.3. Algoritmos heurísticos y metaheurísticos

Capítulo 5

Complejidad Computacional y teoría de la computabilidad

5.1. Complejidad computacional

5.1.1. Clases de complejidad

5.1.2. Reducciones

5.1.3. Problemas intratables

5.2. Teoría de la computabilidad

5.2.1. Maquinas de turing

5.2.2. Funciones computables

5.2.3. Problemas indecidibles

Capítulo 6

Teoría de Códigos, Autómatas y Lenguajes Formales

6.1. Teoría de Códigos

6.2. Autómatas y Lenguajes Formales Avanzados

Los automatas finitos se útilizan como mode