

æ
æ

Algebra

Dra. María Teresa Alcalde Cordero
Dr. César Burgueño Moreno

Depto. de Matemática y Estadística
Facultad de Ingeniería, Ciencias y Administración
Universidad de La Frontera

Segunda Edición
Marzo de 2008

Índice de materias

Prólogo	5
1 Lógica y Teoría de conjuntos	7
1.1 Proposiciones Lógicas	7
1.2 Conectivos lógicos	9
1.2.1 La equivalencia	9
1.2.2 El conectivo "no"	10
1.2.3 Los conectivos "y", "o"	10
1.2.4 El conectivo "implica"	11
1.3 Concepto de Teorema	13
1.4 Teoremas lógicos básicos	15
1.5 Conectivos básicos	18
1.6 Demostraciones algebraicas	20
1.7 Métodos de demostración	23
1.7.1 Demostración directa de " $p \Rightarrow q$ "	24
1.7.2 Demostración indirecta de " $p \Rightarrow q$ "	24
1.7.3 Demostración por contradicción de " $p \Rightarrow q$ "	24
1.8 Circuitos Lógicos	28
1.8.1 Descripción lógica de circuitos	28
1.9 Teoría de conjuntos	38
1.9.1 Cuantificadores	39
1.9.2 Negación de los cuantificadores	41
1.9.3 Ejemplos y contraejemplos	44
1.9.4 Operaciones entre conjuntos	44
1.9.5 Unión e intersección	46
1.9.6 Conjunto Potencia	48
1.9.7 Conjuntos numéricos	50

1.9.8	Diferencia simétrica	51
1.10	Ejercicios Propuestos	52
2	Sumatorias y Recurrencia	59
2.1	Sumatorias	59
2.1.1	Propiedades de la sumatoria	62
2.1.2	Progresiones aritméticas	70
2.1.3	Progresiones Geométricas	72
2.1.4	Sumas de cuadrados	74
2.2	Inducción o recurrencia	75
2.2.1	Los números naturales	75
2.3	Ejercicios Propuestos	84
3	Binomio de Newton	87
3.1	Factorial	87
3.2	Número combinatorio	89
3.2.1	Triángulo de Pascal	92
3.3	Desarrollo del binomio	101
3.4	Ejercicios Propuestos	111
4	Relaciones Binarias	113
4.1	Producto Cartesiano	113
4.2	Conceptos básicos	115
4.3	Grafos	120
4.4	Propiedades de las relaciones binarias	122
4.4.1	Reflexividad	122
4.4.2	Simetría	125
4.4.3	Transitividad	129
4.4.4	Antisimetría	130
4.5	Relaciones de equivalencia	140
4.5.1	Introducción y definición	140
4.5.2	Clases de Equivalencia y conjunto cociente . .	146
4.5.3	Congruencias en \mathbb{Z}	151
4.6	Relaciones de orden	160
4.7	Ejercicios Propuestos	163

5	Funciones	165
5.1	Definiciones básicas	165
5.2	Propiedades de una función	171
5.3	Imagen recíproca	172
5.4	Inyectividad, epiyectividad y biyectividad	174
5.5	Composición de funciones	175
5.6	Función inversa	176
5.7	Funciones biyectivas sobre conjuntos finitos o permutaciones	181
5.7.1	Permutaciones de I_n	182
5.8	Funciones sobre conjuntos finitos	185
5.8.1	Propiedades	185
5.8.2	Número de funciones entre dos conjuntos finitos	188
5.9	Algunas funciones sobre conjuntos no finitos	189
5.10	Ejercicios Propuestos	195
6	Estructuras Algebraicas	197
6.1	Ley de composición interna	197
6.1.1	Propiedades de una l.c.i. en un conjunto	199
6.2	Subestructuras	208
6.3	Grupos, anillos y cuerpos	210
6.4	Subgrupos	214
6.5	Estructura de \mathbb{Z}_n	217
6.6	Estructura de S_n	218
6.7	Aritmética	223
6.8	Ejercicios Propuestos	227
7	Números complejos	229
7.1	Construcción	229
7.2	Estructura algebraica de $(\mathbb{C}, +, \cdot)$	232
7.3	Valor absoluto y distancia	236
7.4	Forma polar o trigonométrica de un número complejo	241
7.5	Multiplicación de números complejos	242
7.6	Elevación a potencia	243
7.7	Inversos multiplicativos.	245
7.8	Extracción de raíces	246
7.9	Forma exponencial de un número complejo	250

7.10	Ejercicios Propuestos	254
8	Polinomios	259
8.1	Definiciones	259
8.2	Función polinómica	265
8.2.1	Raíces de un polinomio	266
8.3	Divisibilidad en el conjunto de polinomios	271
8.3.1	Teorema de la descomposición única	275
8.4	División Euclidiana	275
8.4.1	Teorema de la División Euclidiana o Algoritmo de la División	276
8.5	Descomposición en $\mathbb{C}[X]$	278
8.6	Descomposición en $\mathbb{R}[X]$	279
8.7	Descomposición en $\mathbb{Q}[X]$	281
8.8	Fracciones Racionales	287
8.9	Ejercicios Propuestos	293
	Bibliografía	297

Prólogo

Este libro ha sido pensado para ti que vienes llegando a la Universidad, después de haber tenido una formación matemática en la Educación Media. Esperamos que esta sea una linda experiencia para ti y que tengas mucho éxito en tus estudios.

El texto contiene gran cantidad de ejercicios resueltos, con la finalidad de ayudarte a comprender mejor cada una de las materias del curso. Puede que algunos ejercicios te parezcan muy sencillos, pero es conveniente que los desarrolles y los entiendas en profundidad.

Aparentemente este curso es fácil, pero requiere de mucho estudio de parte tuya. Es importante que estudies todos los días cada uno de los ramos que estas siguiendo, hasta lograr una disciplina de estudio que te permita sentirte bien contigo mismo y lograr un buen rendimiento.

Por nuestra parte estamos dispuestos a ayudarte en las dudas que te vayan surgiendo, para ello debes acercarte a nosotros y solicitar dicha ayuda.

El contenido del curso abarca las materias correspondiente al curso de álgebra de primer semestre. Dichas materias también las puedes encontrar en muchos otros libros, pero el tratamiento que hacemos aquí corresponde a la forma en que te expondremos la materia. Evidentemente que es conveniente que consultes otros textos y hagas los ejercicios que se proponen.

Queremos agradecer a nuestro amigo y colega Dr. Cristián Mallol Comandari por la ayuda prestada, siendo algunos temas y ejercicios inspiraciones personales de él.

Agradecemos a Dios por ayudarnos a escribir este libro el cual ha sido un trabajo muy agradable y se lo dedicamos a nuestros hijos.

Dra. María Teresa Alcalde Cordero

Dr. César Burgueño Moreno

Depto. de Matemática y Estadística

Facultad de Ingeniería, Ciencias y Administración

Universidad de La Frontera

Temuco, Marzo de 2008

Capítulo 1

Lógica y Teoría de conjuntos

En este curso, veremos solamente algunos conceptos básicos y aprenderemos a trabajar algebraicamente con estos conceptos.

Veremos lo justo y necesario para vuestros estudios y vida profesional.

1.1 Propositiones Lógicas

Nota Trabajaremos solamente con frases a las cuales se les pueda asignar el valor de verdadera o falsa.

Diremos que a una frase se le puede asignar un valor de verdad si se puede decir: "esta frase es verdadera" o "esta frase es falsa".

Definición 1.1.1 *Una **proposición** es una frase a la cual se le puede asignar un valor de verdad.*

Ejemplos de proposiciones

1. Temuco es más grande que Santiago.
2. Juan ama a Francisca.
3. No es una proposición: ¿Ama Ignacio a Francisca?

4. Loreto canta hermoso.
5. No es una proposición: ¡Vamos al Lago Budi!

Definición 1.1.2 *Hay frases, oraciones o secuencias de oraciones a modo de historias, a las cuales no se les puede asignar un valor de verdad. Estas son llamadas **paradojas**.*

Ejemplos

1. Una paradoja muy famosa es aquella conocida como "La paradoja del mentiroso". Esta paradoja dice:
"Yo soy mentiroso"
Si una persona te dice esta frase, tú no sabes si esta frase es verdadera o falsa.
2. Otra paradoja muy conocida es la "paradoja del barbero". Esta paradoja dice así:
"En un pueblo, había un barbero, el cual afeitaba a todos aquellos que no se afeitaban a si mismo".
Uno se pregunta: ¿Quién afeitaba al barbero?
Si el como persona no se afeitaba a si mismo, entonces por el hecho de ser "el barbero" del pueblo, debía afeitarse. Contradicción.
Si él se afeitaba a si mismo, esto no podía ser, pues por el hecho de ser el barbero, no podía afeitarse a si mismo. Nuevamente llegamos a una contradicción.
3. La siguiente historia, también es una paradoja. Dice así:
"Había un botero, que llevaba a la gente desde una isla, al continente. Ocurre que éste botero preguntaba a los isleños sobre qué iban a comprar al continente. Si **no** respondían la verdad, entonces ellos eran guillotinado.
Resulta que un isleño le dijo:
"Voy al continente a ser guillotinado".
O también:

1.2 Conectivos lógicos

Nota Una proposición, se puede unir con otra proposición, a través de los **conectivos lógicos**. Los conectivos lógicos son:

La negación, la conjunción (y), la disyunción (o), la implicación y la equivalencia.

1.2.1 La equivalencia

Definición 1.2.1 *Dos proposiciones p y q son lógicamente equivalentes, denotado $p \equiv q$, si ellas tienen el mismo valor de verdad.*

Si p y q son dos proposiciones, entonces $p \equiv q$, también es una proposición y su valor de verdad, puede ser determinado con la ayuda, de lo que llamaremos "tabla de verdad".

La tabla de verdad de la equivalencia es la siguiente

p	q	$p \equiv q$
V	V	V
V	F	F
F	V	F
F	F	V

En esta tabla, la columna del lado derecho, contiene el valor de verdad de " $p \equiv q$ ", para todas las combinaciones posibles de los valores de verdad de p y q .

Ejemplo. Son equivalentes los pares de proposiciones siguientes:

1. a) "Juan es más alto que Loreto"
b) "Loreto es más baja que Juan"
2. a) "Temuco es más grande que París"
b) "París es más pequeño que Temuco"

1.2.2 El conectivo "no"

Definición 1.2.2 Si " p " es una proposición, el valor de verdad de la proposición " $\text{no } p$ ", queda determinada por la siguiente tabla de verdad

p	$\text{no } p$
V	F
F	V

Ejemplos

1. p : Ignacio ama a Francisca.
 $\text{no } p$: Ignacio no ama a Francisca.
2. p : Julieta no ama a Romeo.
 $\text{no } p$: Julieta ama a Romeo.

1.2.3 Los conectivos "y", "o"

Definición 1.2.3 Si " p " y " q " son dos proposiciones, las proposiciones " $p \text{ y } q$ " y " $p \text{ o } q$ ", están determinadas por las siguientes tablas de verdad.

p	q	$p \text{ y } q$
V	V	V
V	F	F
F	V	F
F	F	F

p	q	$p \text{ o } q$
V	V	V
V	F	V
F	V	V
F	F	F

En español, es algo ambiguo el uso del monosílabo "o". Generalmente es usado en sentido excluyente, pero en matemáticas puede incluir ambas proposiciones.

Ejemplos

1. "Escuchemos el pronóstico del tiempo para saber si mañana el día estará bonito o feo".

Este es exactamente el "o" que dejaremos de usar.

2. Un papá matemático, ofrece a su hijo Juan, conocedor del "o matemático": "helados de frutilla o helados de chocolate". Su hijo Juan responde

"Quiero que me des helados de frutilla y también helados de chocolate".

3. La frase "Loreto es alta o baja" es matemáticamente verdadera.

4. La frase "Temuco es más grande que Níamey y Temuco es más pequeño que Níamey" es falsa pues una de las dos proposiciones iniciales es falsa.

Notaciones. El conectivo *y* se denota por \wedge , y el conectivo *o* por \vee .

1.2.4 El conectivo "implica"

Si p y q son dos proposiciones, entonces la proposición " p implica q ", denotada por $p \Rightarrow q$, está definida por la siguiente tabla de verdad:

p	q	$p \Rightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

En lenguaje de la vida diaria, esto es usual expresarlo diciendo:

"si p , entonces q "

o bien:

" p es condición suficiente para q "

o bien:

" q es condición necesaria para p "

Ejemplos

1. p : está lloviendo

q : se está mojando el campo

" $p \Rightarrow q$ ": "Si está lloviendo, entonces se está mojando el campo".

o bien:

"Es suficiente que esté lloviendo, para que se esté mojando el campo"

o bien:

"Basta que esté lloviendo, para que se esté mojando el campo"

2. $p : n$ es múltiplo de 6.

$q : n$ es múltiplo de 2.

La proposición " $p \Rightarrow q$ ", es verdadera, pues "basta ser múltiplo de 6, para ser múltiplo de 2".

o bien:

"Si n es múltiplo de 6, entonces n es múltiplo de 2".

3. "Si un polígono regular tiene 2^n , $n \geq 2$, lados, entonces puede ser construido con regla y compás"

Nótese que el triángulo equilátero puede ser construido con regla y compás.

También el pentágono, el hexágono, o el polígono regular de 17 lados.

Pero, basta que tenga 2^n , $n \geq 2$, lados, para que pueda ser construido con regla y compás.

Es decir

(Un polígono regular tiene 2^n , $n \geq 2$ lados) \Rightarrow (puede ser construido con regla y compás)

4. "Si Juan se lee la Enciclopedia Británica en un día, entonces Francisca andaría en bicicleta"

p: "Juan lee la Enciclopedia Británica en un día"

q: "Francisca andaría en bicicleta"

" $p \Rightarrow q$ " es una proposición considerada verdadera, pues "p no es verificado, luego no podemos contradecir q.

5. $a = b \Rightarrow a + 5 = b + 5$

6. Si n es divisible por 2, entonces n^2 es divisible por 4.

1.3 Concepto de Teorema

Definición 1.3.1 Una **tautología** es una proposición que siempre es verdadera, independientemente de la veracidad o falsedad de las proposiciones iniciales.

Ejemplo. " p o (no p)" es una tautología

p	no p	p o (no p)
V	F	V
F	V	V

Ejemplo. "Castro está en Chiloé o el día está asoleado".

Esta proposición es una tautología pues, es siempre verdadera, independiente si el día está soleado o no lo está. Ocurre que "Castro está en Chiloé" es siempre verdadera y ambas proposiciones están conectadas por el conectivo "o"

Definición 1.3.2 Una **contradicción** es una proposición que siempre es falsa, independientemente de la veracidad o falsedad de las proposiciones iniciales.

Ejemplos

1. " p y no p " es una contradicción

p	$\text{no } p$	$p \text{ y } (\text{no } p)$
V	F	F
F	V	F

2. "El lago Llanquihue está en el norte de Chile y tú tienes una calculadora en el bolsillo"

Puesto que la primera proposición es siempre falsa y que están conectadas por la conjunción "y" entonces la proposición final es siempre falsa.

$$F \text{ y } V \equiv F; \quad F \text{ y } F \equiv F$$

Definición 1.3.3 *Un **axioma** o un **postulado** es una proposición que hemos supuesto verdadera.*

Ejemplo. "Una cantidad es igual a si misma".

Ejemplo. 5^o Postulado de Euclides: "Por un punto fuera de una recta se puede trazar una única recta paralela a ella".

Definición 1.3.4 *Un **teorema** es una proposición que necesita ser demostrada.*

Demostrar un teorema consiste en poner en evidencia su veracidad a partir de proposiciones conocidas o axiomas.

Definición 1.3.5 *Diremos que una proposición es **trivial** u **obvia** si es fácil pensar la demostración.*

En general estas dos palabras se usan de manera abusiva. Es típico que la proposición: " p es trivial" es usada para significar: "Yo no puedo pensar en una demostración de p , pero yo estoy seguro que es verdadera".

1.4 Teoremas lógicos básicos

Teorema 1.4.1 (Idempotencia)

$$i) \quad p \vee p \equiv p$$

$$ii) \quad p \wedge p \equiv p$$

p	$p \vee p$	$p \wedge p$
V	V	V
F	F	F

Las tres columnas tienen el mismo valor de verdad, luego las tres proposiciones son equivalentes.

Teorema 1.4.2 (Doble negación) $no(no \ p) \equiv p$

Demostración.

p	$no \ p$	$no \ (no \ p)$
V	F	V
F	V	F

La primera columna coincide con la tercera, luego ambas proposiciones tienen el mismo valor de verdad, es decir, son equivalentes.

Teorema 1.4.3 (Conmutatividad)

$$i) \quad p \vee q \equiv q \vee p$$

$$ii) \quad p \wedge q \equiv q \wedge p$$

Teorema 1.4.4 (Asociatividad)

$$i) \quad p \vee (q \vee r) \equiv (p \vee q) \vee r$$

$$ii) \quad p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$$

Luego podemos borrar los paréntesis.

Teorema 1.4.5 (Distributividad)

$$i) \ p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$$

$$ii) \ p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$$

Teorema 1.4.6 (Ley de Absorción)

$$i) \ p \wedge (p \vee q) \equiv p$$

$$ii) \ p \vee (p \wedge q) \equiv p$$

Demostración i)

p	q	$p \vee q$	$p \wedge (p \vee q)$
V	V	V	V
V	F	V	V
F	V	V	F
F	F	F	F

La primera columna coincide con la cuarta columna, luego ambas proposiciones son equivalentes.

Demostración ii)

p	q	$p \wedge q$	$p \vee (p \wedge q)$
V	V	V	V
V	F	F	V
F	V	F	F
F	F	F	F

La primera y la cuarta columna coinciden, luego las proposiciones son equivalentes.

Teorema 1.4.7 (Leyes de Morgan)

$$i) \ no(p \vee q) = (no\ p) \wedge (no\ q)$$

$$ii) \text{ no}(p \wedge q) = (\text{no } p) \vee (\text{no } q)$$

Demostración *i)*

p	q	$p \vee q$	$\text{no}(p \vee q)$	$\text{no } p$	$\text{no } q$	$(\text{no } p) \wedge (\text{no } q)$
V	V	V	F	F	F	F
V	F	V	F	F	V	F
F	V	V	F	V	F	F
F	F	F	V	V	V	V

Demostración *ii)* De la misma manera que *i)*.

Notación: $\text{no } p$ será abreviada por \bar{p}

Lema. Si p es una proposición, entonces se tiene

$$i) \quad V \vee p \equiv V$$

$$ii) \quad V \wedge p \equiv p$$

$$iii) \quad F \vee p \equiv p$$

$$iv) \quad F \wedge p \equiv F$$

Demostración *i)*

V	p	$V \vee p$
V	V	V
V	F	V

Las otras demostraciones son análogas.

Teorema 1.4.8 (Tercero Excluído) " $p \vee \bar{p}$ " es una tautología, es decir, $p \vee \bar{p} \equiv V$

Demostración. Mediante tabla de verdad.

Teorema 1.4.9 La proposición $p \equiv q$ tiene el mismo valor de verdad que la proposición $(p \Rightarrow q) \wedge (q \Rightarrow p)$

Demostración.

p	q	$p \equiv q$	$p \Rightarrow q$	$q \Rightarrow p$	$(p \Rightarrow q) \wedge (q \Rightarrow p)$
V	V	V	V	V	V
V	F	F	F	V	F
F	V	F	V	F	F
F	F	V	V	V	V

La tercera y la sexta columna son iguales, luego se tiene demostrado el teorema.

Notación. El símbolo $p \Leftrightarrow q$ resume la proposición:

$$(p \Rightarrow q) \wedge (q \Rightarrow p)$$

Decimos p si y sólo si q .

Observación. El teorema anterior nos dice que es equivalente escribir $p \equiv q$ que $p \Leftrightarrow q$

1.5 Conectivos básicos

Nota En esta sección veremos que a partir de los conectivos "no" y "o", se pueden obtener los otros tres conectivos. De la misma manera, a partir de "no" e "y".

Teorema 1.5.1 (Reducción de " \Rightarrow " a "no" y "o")

$$(p \Rightarrow q) \equiv (\bar{p} \vee q)$$

Demostración.

p	q	$p \Rightarrow q$	\bar{p}	$\bar{p} \vee q$
V	V	V	F	V
V	F	F	F	F
F	V	V	V	V
F	F	V	V	V

La tercera y quinta columna coinciden, luego ambas proposiciones tienen el mismo valor de verdad.

Muy Importante: Los teoremas anteriores ustedes los van a utilizar a lo largo de sus estudios, es decir, siempre!. Necesitarán **recordar** los enunciados.

Ejercicios.

1. Reducción del " \Leftrightarrow " a "no", "o" e "y"

En efecto

$$i) p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p) \equiv (\bar{p} \vee q) \wedge (\bar{q} \vee p)$$

$$\text{Es decir } p \Leftrightarrow q \equiv (\bar{p} \vee q) \wedge (\bar{q} \vee p)$$

Otra posibilidad es:

$$ii) p \Leftrightarrow q \equiv (\bar{p} \vee q) \wedge (\bar{q} \vee p)$$

$$\equiv ((\bar{p} \vee q) \wedge \bar{q}) \vee ((\bar{p} \vee q) \wedge p)$$

$$\equiv (\bar{p} \wedge \bar{q}) \vee (q \wedge \bar{q}) \vee (\bar{p} \wedge p) \vee (q \wedge p)$$

$$\equiv (\bar{p} \wedge \bar{q}) \vee F \vee F \vee (p \wedge q)$$

$$\equiv (\bar{p} \wedge \bar{q}) \vee (p \wedge q)$$

es decir

$$p \Leftrightarrow q \equiv (p \wedge q) \vee (\bar{p} \wedge \bar{q})$$

2. Reducción de "y" a "no" y "o" En efecto

$$p \wedge q \equiv \overline{\overline{p \wedge q}} \equiv \overline{\bar{p} \vee \bar{q}}$$

es decir

$$p \wedge q \equiv \overline{\bar{p} \vee \bar{q}}$$

3. Reducción de " \Leftrightarrow " a "no" y "o": En efecto

$$p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p) \equiv$$

$$\equiv (\bar{p} \vee q) \wedge (\bar{q} \vee p) \equiv \overline{(\overline{\bar{p} \vee q}) \vee (\overline{\bar{q} \vee p})}$$

Nota Los conectivos "y", " \Rightarrow ", " \Leftrightarrow " pueden ser expresados a partir de "no" y "o", o bien a partir de "no" e "y".

4. (Tarea.) Describa $p \vee q$, $p \Rightarrow q$, $p \Leftrightarrow q$ a partir de los conectivos "no" e "y".

1.6 Demostraciones algebraicas

1. Demostremos que $p \Rightarrow (p \vee q)$ es una tautología, es decir es siempre verdadera.

Demostración.

$$\begin{aligned} (p \Rightarrow (p \vee q)) &\equiv (\bar{p} \vee (p \vee q)) \\ &\equiv ((\bar{p} \vee p) \vee q) \\ &\equiv V \vee q \\ &\equiv V \end{aligned}$$

2. Demostremos que $(p \wedge (p \Rightarrow q)) \Rightarrow q$.

Demostración.

$$\begin{aligned} p \wedge (p \Rightarrow q) \Rightarrow q &\equiv (\overline{p \wedge (\bar{p} \vee q)}) \vee q \\ &\equiv (\bar{p} \vee (\bar{p} \vee q)) \vee q \\ &\equiv (\bar{p} \vee q) \vee (\bar{p} \vee q) \\ &\equiv V \end{aligned}$$

3. Teorema (contrarecíproco): $(p \Rightarrow q) \equiv (\bar{q} \Rightarrow \bar{p})$.

Demostración.

$$\begin{aligned} p \Rightarrow q &\equiv \bar{p} \vee q \\ &\equiv q \vee \bar{p} \\ &\equiv \bar{\bar{q}} \vee \bar{p} \\ &\equiv \bar{q} \Rightarrow \bar{p} \end{aligned}$$

Nota Esta última proposición es muy usada, es por esto que lleva el nombre de teorema.

Observación. Recordemos el ejemplo:

p : está lloviendo

q : se está mojando el campo

Es equivalente decir:

”Si está lloviendo, entonces se está mojando el campo”

y

"Si no se está mojando el campo, entonces no está lloviendo"

Observe que el negar p no conduce a ninguna deducción, pues

"si no está lloviendo", puede ocurrir que "se esté mojando el campo" o bien, "que no se esté mojando el campo"

Ejercicios Resueltos

$$1. \quad ((p \vee q) \wedge \bar{q}) \Rightarrow p$$

Solución.

$$\begin{aligned} ((p \vee q) \wedge \bar{q}) \Rightarrow p &\equiv \overline{((p \vee q) \wedge \bar{q})} \vee p \\ &\equiv (\bar{p} \vee \bar{q}) \vee q \vee p \\ &\equiv (\bar{p} \vee \bar{q}) \vee (p \vee q) \\ &\equiv V \end{aligned}$$

$$2. \quad (p \Rightarrow (q \wedge \bar{q})) \Rightarrow \bar{p}$$

Solución.

$$\begin{aligned} (p \Rightarrow (q \wedge \bar{q})) \Rightarrow \bar{p} &\equiv (p \Rightarrow F) \Rightarrow \bar{p} \\ &\equiv (\bar{p} \vee F) \vee \bar{p} \\ &\equiv (p \wedge V) \vee \bar{p} \\ &\equiv p \vee \bar{p} \\ &\equiv V \end{aligned}$$

En palabras, si una proposición induce una contradicción, entonces uno concluye que la proposición verdadera es la negación de la proposición inicial.

$$3. \text{ Ley de simplificación: } p \wedge q \Rightarrow p.$$

Solución.

$$\begin{aligned} (p \wedge q) \Rightarrow p &\equiv \overline{p \wedge q} \vee p \\ &\equiv (\bar{p} \vee \bar{q}) \vee p \\ &\equiv (p \vee \bar{p}) \vee \bar{q} \\ &\equiv V \vee \bar{q} \\ &\equiv V \end{aligned}$$

Nota Si tenemos dos proposiciones verdaderas unidas por un "y", ¡obvio! que cada una de ellas es también verdadera.

Se dice: "en particular" cada una de ellas es verdadera.

Por Ejemplo:

"Ignacio tiene alguien que lo ama y Juan tiene alguien que lo ama", en particular Juan tiene alguien que lo ama.

Esto es lo que se llama un "caso particular".

4. Teorema de Reducción al Absurdo.

$$p \Rightarrow q \equiv (p \wedge \bar{q}) \Rightarrow \bar{p}$$

Solución.

$$\begin{aligned} (p \wedge \bar{q}) \Rightarrow \bar{p} &\equiv \overline{p \wedge \bar{q}} \vee \bar{p} \\ &\equiv (\bar{p} \vee q) \vee \bar{p} \\ &\equiv \bar{p} \vee q \\ &\equiv p \Rightarrow q \end{aligned}$$

5. Primer Teorema de Demostración por casos.

$$((p \Rightarrow q) \wedge (\bar{p} \Rightarrow q)) \Rightarrow q$$

es un tautología.

Solución.

$$\begin{aligned} ((p \Rightarrow q) \wedge (\bar{p} \Rightarrow q)) \Rightarrow q &\equiv \overline{(p \Rightarrow q \wedge \bar{p} \Rightarrow q)} \vee q \\ &\equiv \overline{(\bar{p} \vee q) \wedge (p \vee q)} \vee q \\ &\equiv \overline{(\bar{p} \wedge p) \vee q \vee q} \\ &\equiv \bar{F} \vee q \vee q \\ &\equiv \bar{q} \vee q \\ &\equiv V \end{aligned}$$

6. Segundo Teorema de Reducción al Absurdo.

$$p \Rightarrow q \equiv (p \wedge \bar{q}) \Rightarrow q$$

Solución.

$$\begin{aligned} (p \wedge \bar{q}) \Rightarrow q &\equiv \overline{p \wedge \bar{q}} \vee q \\ &\equiv (\bar{p} \vee q) \vee q \\ &\equiv \bar{p} \vee q \\ &\equiv p \Rightarrow q \end{aligned}$$

7. Segundo Teorema de Demostración por casos.

$$[(p \Rightarrow r) \wedge (q \Rightarrow r)] \Rightarrow [(p \vee q) \Rightarrow r]$$

Solución.

$$\begin{aligned} (p \Rightarrow r) \wedge (q \Rightarrow r) &\Rightarrow ((p \vee q) \Rightarrow r) \equiv \\ &\equiv \overline{p \Rightarrow r \wedge q \Rightarrow r} \vee ((p \vee q) \Rightarrow r) \\ &\equiv \overline{(\overline{p} \vee r) \wedge (\overline{q} \vee r)} \vee ((\overline{p \vee q}) \vee r) \\ &\equiv \overline{(\overline{p} \wedge \overline{q}) \vee r} \vee (\overline{p \vee q} \vee r) \\ &\equiv ((\overline{p \vee q}) \vee r) \vee (\overline{p \vee q} \vee r) \\ &\equiv V \end{aligned}$$

8. $(p \Rightarrow q) \equiv ((p \vee q) \Leftrightarrow q)$

Solución.

$$\begin{aligned} ((p \vee q) \Leftrightarrow q) &\equiv ((p \vee q) \Rightarrow q) \wedge (q \Rightarrow p \vee q) \\ &\equiv (\overline{p \vee q} \vee q) \wedge (\overline{q} \vee p \vee q) \\ &\equiv (\overline{p \vee q} \vee q) \wedge V \\ &\equiv \overline{p \vee q} \vee q \\ &\equiv (\overline{p} \wedge \overline{q}) \vee q \\ &\equiv (\overline{p} \vee q) \wedge (\overline{q} \vee q) \\ &\equiv (\overline{p} \vee q) \wedge V \\ &\equiv \overline{p} \vee q \\ &\equiv (p \Rightarrow q) \end{aligned}$$

1.7 Métodos de demostración

Nota La mayoría de los teoremas tienen una de las dos formas siguientes:

$$"p \Rightarrow q" \text{ o } "p \Leftrightarrow q"$$

La segunda de estas formas, realmente consiste en dos teoremas en uno y es usualmente probado en dos partes. Se demuestra separadamente " $p \Rightarrow q$ " y " $q \Rightarrow p$ ".

El primer tipo de demostración que veremos es llamado:

1.7.1 Demostración directa de " $p \Rightarrow q$ "

En este caso se supone verdadero p y se trata de deducir la veracidad de q .

No es necesario preocuparse cuando p es falso, pues en este caso la implicación " $p \Rightarrow q$ " es siempre verdadera.

Ejemplo.

Teorema: Sea n un número entero, entonces

$$n \text{ par} \Rightarrow n^2 \text{ par}$$

Demostración directa: n par $\Rightarrow n$ tiene la forma $n = 2t$, cierto t número entero $\Rightarrow n^2 = 4t^2 = 2(2t^2) = 2s$, donde $s = 2t^2$ es un número entero $\Rightarrow n^2$ es un número par.

1.7.2 Demostración indirecta de " $p \Rightarrow q$ "

Este método consiste en demostrar el contrarecíproco: $\bar{q} \Rightarrow \bar{p}$

Entonces suponemos la veracidad de \bar{q} y se trata de deducir la veracidad de \bar{p} .

Ejemplo.

Teorema: Sea n un número entero, entonces

$$n^2 \text{ par} \Rightarrow n \text{ par}$$

Demostración indirecta: Por demostrar n impar $\Rightarrow n^2$ impar.

En efecto n impar $\Rightarrow n = 2k + 1$, cierto k número entero $\Rightarrow n^2 = 4k^2 + 4k + 1 \Rightarrow n^2 = 2(2k^2 + 2k) + 1 = 2t + 1$, donde $t = 2k^2 + 2k$ el cual es un número entero $\Rightarrow n^2$ impar.

1.7.3 Demostración por contradicción de " $p \Rightarrow q$ "

Este método consiste en la reducción al absurdo:

" p y ($no\ q$)"

Suponemos la veracidad de " p y ($no\ q$)" al mismo tiempo y buscamos una contradicción. Luego " $p \wedge \bar{q}$ " es falso, luego $\overline{p \wedge \bar{q}} \equiv \bar{p} \vee q \equiv (p \Rightarrow q)$ es verdadero.

Ejemplo.

Proposición. $n = \sqrt{2} \Rightarrow n$ es un número irracional.

Demostración por contradicción: Recordemos que un número racional es un número de la forma $\frac{n}{m}$, con n y m números enteros y $m \neq 0$.

Un número es irracional si y sólo si no puede ser escrito como fracción.

Supongamos que $\sqrt{2} = \frac{n}{m}$ está en su forma reducida

$\Rightarrow 2m^2 = n^2 \Rightarrow n^2$ par $\Rightarrow n$ par $\Rightarrow n = 2t$, cierto t número entero
 $\Rightarrow 2m^2 = 4t^2 \Rightarrow m^2 = 2t^2 \Rightarrow m^2$ par $\Rightarrow m$ par $\Rightarrow m = 2s$, cierto s número entero
 $\Rightarrow \sqrt{2} = \frac{2t}{2s} = \frac{t}{s}$ lo cual es una contradicción, pues habíamos supuesto que $\sqrt{2}$ estaba escrita en su forma reducida.

Llegamos a una contradicción ¿Cuál fue el error que cometimos?. El error fue suponer que $\sqrt{2}$ podía ser escrito como una fracción.

Conclusión: $\sqrt{2}$ es un número irracional.

Ejercicios Resueltos

1. Demostremos que: $((p \vee q) \wedge \bar{q}) \Rightarrow p$ es siempre verdadera.

Solución.

$$\begin{aligned} ((p \vee q) \wedge \bar{q}) \Rightarrow p &\equiv^{(1)} \overline{((p \vee q) \wedge \bar{q})} \vee p \\ &\equiv^{(2)} ((\overline{p \vee q}) \vee \bar{\bar{q}}) \vee p \\ &\equiv^{(3)} (\bar{p} \vee \bar{q}) \vee (p \vee q) \\ &\equiv^{(4)} V \end{aligned}$$

(1) $r \Rightarrow t \equiv \bar{r} \vee t$, (2) Leyes de Morgan, (3) doble negación y asociatividad de \vee , (4) $\bar{\bar{t}} \vee t \equiv V$.

O bien,

$$((p \vee q) \wedge \bar{q}) \equiv (p \wedge \bar{q}) \vee (q \wedge \bar{q}) \equiv (p \wedge \bar{q}) \vee F \equiv p \wedge \bar{q}$$

Pero $p \wedge \bar{q} \Rightarrow p$

2. Demostremos que: $\overline{(p \wedge \bar{q}) \vee (\bar{p} \wedge q)} \equiv (p \Leftrightarrow q)$.

Solución.

$$\begin{aligned} \overline{(p \wedge \bar{q}) \vee (\bar{p} \wedge q)} &\equiv \overline{p \wedge \bar{q}} \wedge \overline{\bar{p} \wedge q} \\ &\equiv (\bar{p} \vee \bar{\bar{q}}) \wedge (\bar{\bar{p}} \vee \bar{q}) \\ &\equiv (\bar{p} \vee q) \wedge (p \vee \bar{q}) \\ &\equiv (\bar{p} \vee q) \wedge (\bar{q} \vee p) \\ &\equiv (p \Rightarrow q) \wedge (q \Rightarrow p) \\ &\equiv p \Leftrightarrow q \end{aligned}$$

3. Neguemos la proposición: $p \Leftrightarrow q$

Solución.

$$\begin{aligned} \overline{p \Leftrightarrow q} &\equiv \overline{(p \wedge q) \vee (\bar{p} \wedge \bar{q})} \\ &\equiv \overline{(p \wedge q)} \wedge \overline{(\bar{p} \wedge \bar{q})} \\ &\equiv (\bar{p} \vee \bar{q}) \wedge (p \vee q) \\ &\equiv (p \vee q) \wedge (\bar{p} \vee \bar{q}) \end{aligned}$$

4. Simplifiquemos la expresión lógica: $(p \vee q) \wedge (\bar{p} \vee q) \wedge t$.

Solución.

$$\begin{aligned} (p \vee q) \wedge (\bar{p} \vee q) \wedge t &\equiv ((p \vee q) \wedge (\bar{p} \vee q)) \wedge t \\ &\equiv ((p \wedge \bar{p}) \vee q) \wedge t \\ &\equiv (F \vee q) \wedge t \\ &\equiv q \wedge t \end{aligned}$$

5. Demostremos que: $\overline{(p \wedge \bar{q} \Rightarrow r)} \Leftrightarrow ((\bar{r} \Rightarrow p) \wedge (\bar{q} \Rightarrow r))$.

Solución. Comencemos con el primer lado de la equivalencia y demostremos que es equivalente al segundo lado

$$\begin{aligned} \overline{(p \wedge \bar{q} \Rightarrow r)} &\equiv \overline{(p \wedge \bar{q}) \vee r} \\ &\equiv \overline{(p \wedge \bar{q})} \wedge \bar{r} \\ &\equiv (\bar{p} \vee q) \wedge (\bar{q} \vee r) \\ &\equiv (\bar{p} \Rightarrow r) \wedge (\bar{q} \Rightarrow r) \\ &\equiv (\bar{r} \Rightarrow p) \wedge (\bar{q} \Rightarrow r) \end{aligned}$$

6. Demostremos que: $((p \vee q) \Rightarrow (p \wedge q)) \equiv (p \Leftrightarrow q)$.

En palabras:

Solución. Comencemos por el lado izquierdo

$$((p \vee q) \Rightarrow (p \wedge q)) \equiv \overline{(p \vee q)} \vee (p \wedge q) \equiv (\bar{p} \wedge \bar{q}) \vee (p \wedge q) \equiv p \Leftrightarrow q$$

7. La siguiente expresión algebraica: $(p \Rightarrow q \wedge q \Rightarrow r) \Rightarrow (p \Rightarrow r)$ escribámosla en función de los conectivos "o" y "no".

Solución.

$$\begin{aligned} ((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r) &\equiv \overline{((p \Rightarrow q) \wedge (q \Rightarrow r))} \vee (p \Rightarrow r) \\ &\equiv \overline{p \Rightarrow q} \vee \overline{q \Rightarrow r} \vee \bar{p} \vee r \\ &\equiv \bar{p} \vee q \vee \bar{q} \vee r \vee \bar{p} \vee r \end{aligned}$$

8. Expresar solamente con los conectivos "o" y "no":

$$(\bar{p} \Leftrightarrow q) \Rightarrow (p \wedge q)$$

Solución.

$$\begin{aligned} (\bar{p} \Leftrightarrow q) \Rightarrow (p \wedge q) &\equiv \overline{(\bar{p} \Leftrightarrow q)} \vee (p \wedge q) \\ &\equiv \overline{(\bar{p} \Rightarrow q) \wedge (q \Rightarrow \bar{p})} \vee (p \wedge q) \\ &\equiv \overline{(\bar{p} \vee q) \wedge (\bar{q} \vee \bar{p})} \vee (p \wedge q) \\ &\equiv \overline{\bar{p} \vee q} \vee \overline{\bar{p} \vee \bar{q}} \vee \bar{p} \vee \bar{q} \\ &\equiv p \vee \bar{q} \vee \bar{p} \vee q \end{aligned}$$

9. Demostremos que: $(p \vee q) \wedge (\bar{p} \vee \bar{q}) \equiv (p \wedge \bar{q}) \vee (\bar{p} \wedge q)$.

Solución.

$$\begin{aligned} (p \vee q) \wedge (\bar{p} \vee \bar{q}) &\equiv ((p \vee q) \wedge \bar{p}) \vee ((p \vee q) \wedge \bar{q}) \\ &\equiv (p \wedge \bar{p}) \vee (q \wedge \bar{p}) \vee (p \wedge \bar{q}) \vee (q \wedge \bar{q}) \\ &\equiv F \vee (\bar{p} \wedge q) \vee (p \wedge \bar{q}) \vee F \\ &\equiv (\bar{p} \wedge q) \vee (p \wedge \bar{q}) \end{aligned}$$

10. Demostremos que: $((p \wedge q) \Rightarrow p) \wedge (p \Rightarrow (p \wedge q)) \Leftrightarrow (p \Rightarrow q)$.

Solución. Comencemos por el lado izquierdo

$$\begin{aligned}
 ((p \wedge q) \Rightarrow p) \wedge (p \Rightarrow (p \wedge q)) &\equiv (\overline{(p \wedge q)} \vee p) \wedge (\overline{p} \vee (p \wedge q)) \\
 &\equiv (\overline{p} \vee \overline{q} \vee p) \wedge (\overline{p} \vee p) \wedge (\overline{p} \vee q) \\
 &\equiv (V \vee \overline{q}) \wedge V \wedge (\overline{p} \vee q) \\
 &\equiv V \wedge V \wedge (\overline{p} \vee q) \equiv \overline{p} \vee q \\
 &\equiv (p \Rightarrow q)
 \end{aligned}$$

11. Transitividad del \Rightarrow : $(p \Rightarrow q \wedge q \Rightarrow r) \Rightarrow (p \Rightarrow r)$.

Solución.

$$\begin{aligned}
 (p \Rightarrow q \wedge q \Rightarrow r) \Rightarrow (p \Rightarrow r) &\equiv \overline{(p \Rightarrow q \wedge q \Rightarrow r)} \vee (p \Rightarrow r) \\
 &\equiv \overline{((\overline{p} \vee q) \wedge (\overline{q} \vee r))} \vee (\overline{p} \vee r) \\
 &\equiv (\overline{\overline{p} \vee q}) \vee (\overline{\overline{q} \vee r}) \vee (\overline{p} \vee r) \\
 &\equiv (p \wedge \overline{q}) \vee (q \wedge \overline{r}) \vee (\overline{p} \vee r) \\
 &\equiv ((p \wedge \overline{q}) \vee \overline{p}) \vee ((q \wedge \overline{r}) \vee r) \\
 &\equiv (V \wedge (\overline{p} \vee \overline{q})) \vee ((q \vee r) \wedge V) \\
 &\equiv (\overline{p} \vee \overline{q}) \vee (q \vee r) \\
 &\equiv (q \vee \overline{q}) \vee \overline{p} \vee r \\
 &\equiv V \vee (\overline{p} \vee r) \\
 &\equiv V
 \end{aligned}$$

12. Demostremos que $(p \Leftrightarrow q \wedge q \Leftrightarrow r) \Rightarrow (p \Leftrightarrow r)$

Solución.

$$\begin{aligned}
 (p \Leftrightarrow q \wedge q \Leftrightarrow r) &\equiv (p \Rightarrow q) \wedge (q \Rightarrow p) \wedge (q \Rightarrow r) \wedge (r \Rightarrow q) \\
 &\equiv ((p \Rightarrow q) \wedge (q \Rightarrow r)) \wedge ((r \Rightarrow q) \wedge (q \Rightarrow p)) \\
 &\Rightarrow ((p \Rightarrow r) \wedge (r \Rightarrow p)) \\
 &\equiv (p \Leftrightarrow r)
 \end{aligned}$$

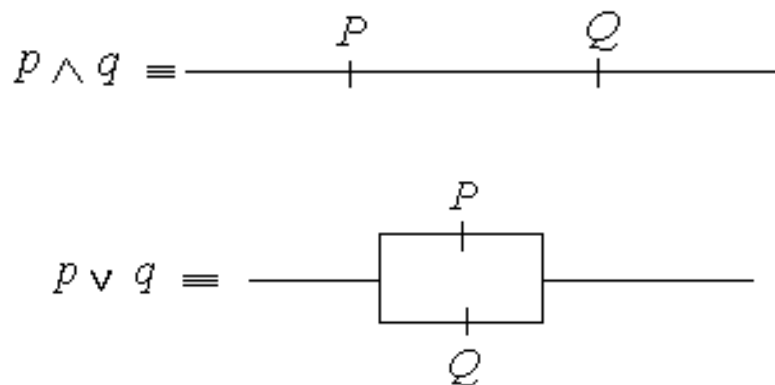
1.8 Circuitos Lógicos

1.8.1 Descripción lógica de circuitos

A un interruptor P , le vamos a asociar la proposición lógica p , de la manera siguiente:

p	p
V	Pasa la corriente
F	NO pasa la corriente

Podemos interpretar la conjunción como un circuito en serie y la disyunción lógica como un circuito en paralelo, es decir tenemos:



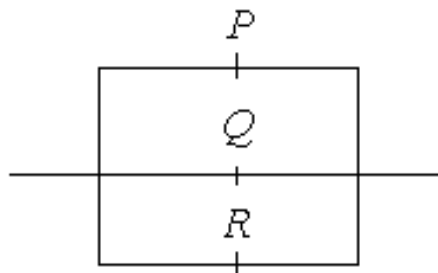
Dado un interruptor P , designamos por \overline{P} otro interruptor por el cual "pasa corriente si y sólo si por P no pasa corriente".

obviamente a \overline{P} le asignamos la proposición \bar{p} .

Ejercicios

1. Representemos en un circuito, la proposición lógica $p \vee q \vee r$.

Solución.



2. Representemos en un circuito, la proposición $(p \wedge q) \vee (\bar{p} \wedge \bar{q})$

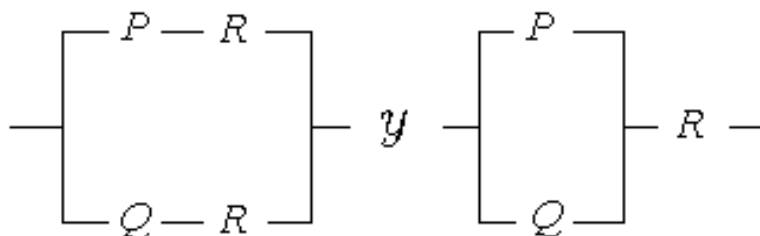
Solución.



Observación. Sabemos que

$$((p \wedge r) \vee (q \wedge r)) \equiv ((p \vee q) \wedge r)$$

Luego, son equivalentes los circuitos



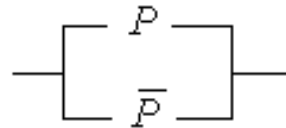
Podemos concluir también que hemos reducido el circuito.

Definición 1.8.1 Reducir un circuito, es sacar interruptores que no son necesarios.

Observación. Nosotros sabemos que

$$p \vee \bar{p} \equiv V$$

esto significa que por el circuito

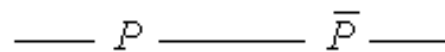


siempre pasa la corriente

Observación. Sabemos que

$$p \wedge \bar{p} \equiv F$$

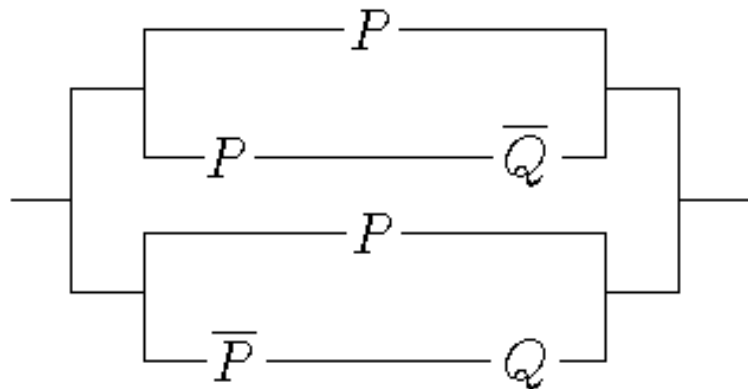
En lenguaje de circuito, significa que por el circuito



nunca pasa la corriente.

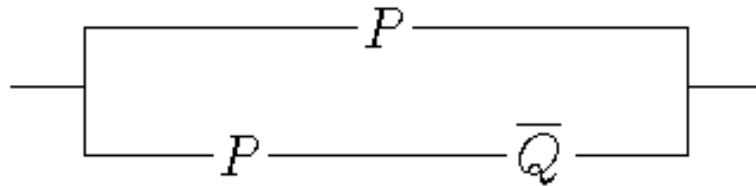
Ejercicios Resueltos

1. Simplifiquemos el siguiente circuito



Solución. Vamos resolviéndolo por partes, ¿te parece?

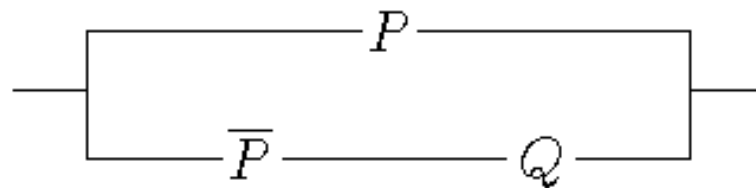
- i. Tomando la parte superior del circuito



en lenguaje algebraico tenemos

$$p \vee (p \wedge \bar{q}) \equiv p \quad (\text{ley de absorción})$$

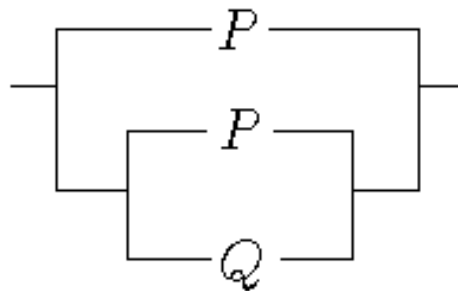
ii. Tomando la parte inferior del circuito



en lenguaje algebraico tenemos

$$p \vee (\bar{p} \wedge q) \equiv (p \vee \bar{p}) \wedge (p \vee q) \equiv V \wedge (p \vee q) \equiv p \vee q$$

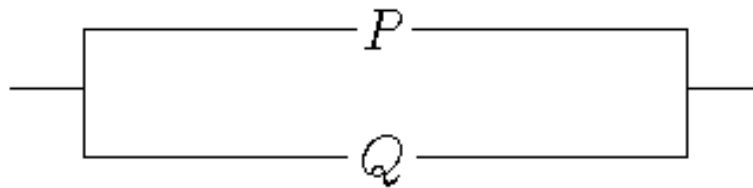
Luego, el circuito queda



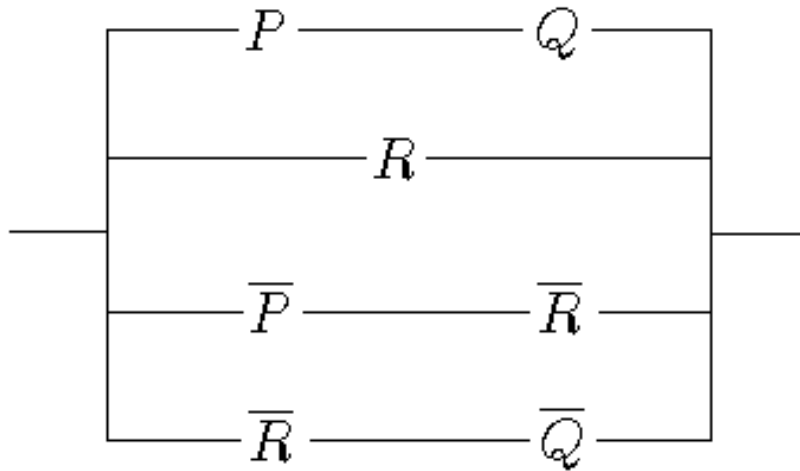
En forma de proposiciones lógicas tenemos

$$p \vee (p \vee q) \equiv (p \vee p) \vee q \equiv p \vee q$$

Luego, su simplificación máxima es



2. Reduzcamos el circuito



Solución. Comencemos por escribir su expresión algebraica:

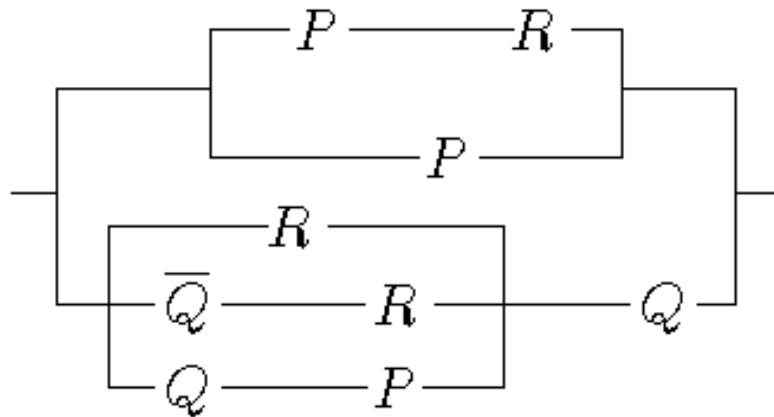
$$\begin{aligned} (p \wedge q) \vee r \vee (\bar{p} \wedge \bar{r}) \vee (\bar{r} \wedge \bar{q}) &\equiv (p \wedge q) \vee r \vee (\bar{r} \wedge (\bar{p} \vee \bar{q})) \\ &\equiv (p \wedge q) \vee r \vee (\bar{r} \wedge \overline{(p \wedge q)}) \\ &\equiv ((p \wedge q) \vee r) \vee \overline{(r \vee (p \wedge q))} \\ &\equiv V \end{aligned}$$

Es decir, por este circuito siempre pasa corriente.

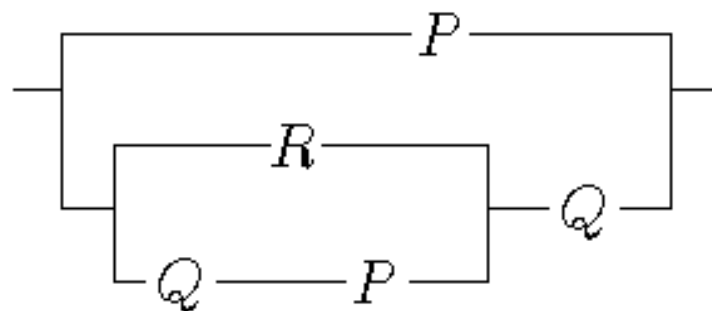
Luego, la reducción queda

es decir, un cable sin interruptores. Es lo máximo en simplificación.

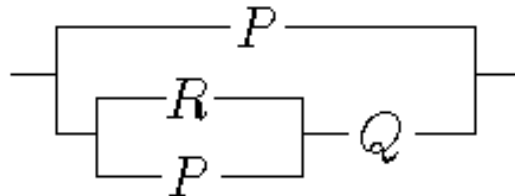
3. Reduzcamos el circuito



Solución. Usando la ley de absorción, lo reducimos al siguiente circuito:



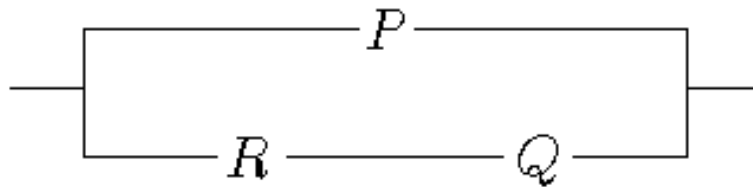
Luego, lo reducimos a



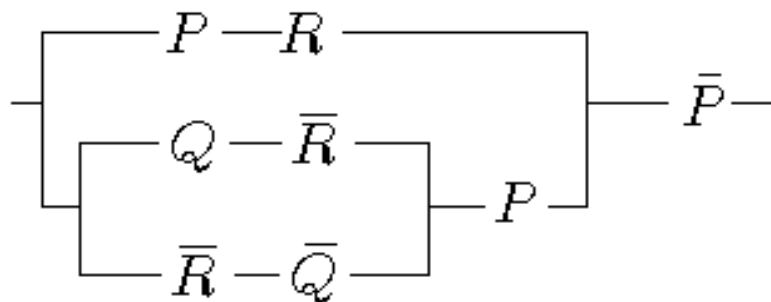
Algebraicamente, tenemos

$$\begin{aligned} p \vee ((r \vee p) \wedge q) &\equiv (p \vee r \vee p) \wedge (p \vee q) \\ &\equiv (p \vee r) \wedge (p \vee q) \\ &\equiv p \vee (r \wedge q) \end{aligned}$$

Su reducción máxima es:



4. Estudiemos el siguiente circuito. Es decir, veamos si lo podemos reducir, o si pasa siempre corriente, o nunca, o si depende de algún interruptor.



Solución. El lado izquierdo del circuito es:

$$\begin{aligned}
 (p \wedge r) \vee [(q \wedge \bar{r}) \vee (\bar{r} \wedge \bar{q})] \wedge p &\equiv^{(1)} (p \wedge r) \vee [(\bar{r} \wedge (q \vee \bar{q})) \wedge p] \\
 &\equiv^{(2)} (p \wedge r) \vee ((\bar{r} \wedge V) \wedge p) \\
 &\equiv (p \wedge r) \vee (\bar{r} \wedge p) \\
 &\equiv^{(3)} p \wedge (r \vee \bar{r}) \\
 &\equiv^{(4)} p \wedge V \\
 &\equiv^{(2)} p
 \end{aligned}$$

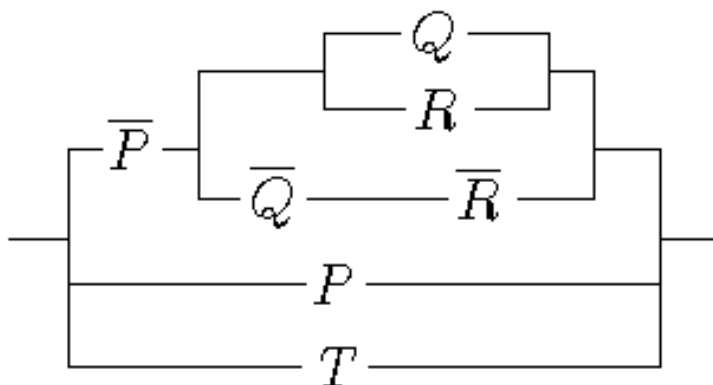
Luego, el circuito queda

$$\text{---} P \text{---} \bar{P} \text{---}$$

Luego, por el circuito NUNCA pasa corriente.

- (1) Distribución mirada de derecha a izquierda, digamos “factorización”.
- (2) : $\bar{r} \wedge V \equiv \bar{r}$
- (3) Factorización de p
- (4) : $r \vee \bar{r} \equiv V$

5. Reduzcamos el circuito siguiente:

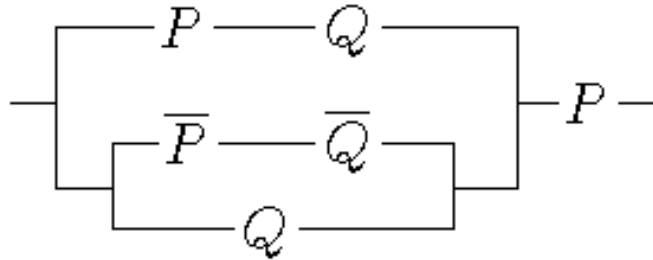


Solución. Comencemos por expresarlo algebraicamente

$$\begin{aligned}
 (\bar{p} \wedge ((q \vee r) \vee (\bar{q} \wedge \bar{r}))) \vee p \vee t &\equiv (\bar{p} \wedge ((q \vee r) \vee (\bar{q} \vee \bar{r}))) \vee p \vee t \\
 &\equiv (\bar{p} \wedge V) \vee p \vee t \\
 &\equiv \bar{p} \vee p \vee t \\
 &\equiv V \vee t \\
 &\equiv V
 \end{aligned}$$

Entonces, por este circuito SIEMPRE pasa corriente, es decir, es equivalente a un circuito sin interruptor.

6. Estudiemos el circuito



Solución. Comencemos por escribir su expresión algebraica

$$\begin{aligned}
 ((p \wedge q) \vee ((\bar{p} \wedge \bar{q}) \vee q)) \wedge p &\equiv (((p \wedge q) \vee q) \vee (\bar{p} \wedge \bar{q})) \wedge p \\
 &\equiv (q \vee (\bar{p} \wedge \bar{q})) \wedge p \\
 &\equiv (p \wedge q) \vee (p \wedge \bar{p} \wedge \bar{q}) \\
 &\equiv (p \wedge q) \vee F \equiv p \wedge q
 \end{aligned}$$

Luego, el circuito queda reducido a



1.9 Teoría de conjuntos

En esta sección veremos sólo algunas definiciones sobre conjuntos. El resto será obtenido como consecuencia de lo estudiado en la sección anterior.

Un conjunto es una colección de objetos los cuales serán llamados elementos.

Si a es un elemento de un conjunto A , decimos " a pertenece a A " y escribiremos $a \in A$. En caso contrario diremos que " a no pertenece a A " y escribiremos " $a \notin A$ ".

Definición 1.9.1 Diremos que dos conjuntos son **iguales** si tienen los mismos elementos.

Ejemplo. $\{1, 1, 2, 2, 2\} = \{2, 1\}$

Definición 1.9.2 El conjunto al cual pertenecen todos los elementos que estamos considerando será llamado **conjunto universal** o **conjunto universo** y lo denotaremos por U .

Nota Es absurdo pensar en un conjunto universal único. Es una paradoja pensar en "el conjunto que contiene a todos los conjuntos"

Ejemplo. Si estamos trabajando solamente con números naturales, entonces, en este caso $U = \mathbb{N}$

Observación. Consideremos las oraciones:

$$(i) \sqrt{2} = n; \quad (ii) x = y + z; \quad (iii) x = y^2 + z^2; \quad (iv) x^2 = -1$$

Estas oraciones al ser consideradas dentro de un conjunto, adquieren un valor de verdad que puede ser verdadero o falso. Estas oraciones serán llamadas **predicados**.

Por ejemplo si pensamos que $U = \mathbb{N}$, el predicado (iii) a veces es verdadero y a veces es falso. ($13 = 2^2 + 3^2$, $5 = 1^2 + 2^2$), sin embargo el 3 no puede ser escrito como suma de dos cuadrados.

El predicado (iv) es falso para todo número real. Sin embargo es verdadero si $x \in \mathbb{C}$ y $x = i$ o $x = -i$

Definición 1.9.3 Un **predicado** es una oración que contiene una o más variables, las cuales se transforman en proposiciones cuando son reemplazadas por objetos del conjunto A considerado.

Nota Cuando un conjunto tiene una cantidad infinita o una gran cantidad de elementos es descrito con el uso de un predicado.

Ejemplo. $A = \{x \in \mathbb{R}; x = y^2 + z^2\}$; $B = \{n \in \mathbb{Z}; -1 \leq n < 50\}$; $C = \{a \in \mathbb{Z}; a^2 > 1\}$

Nota Será conveniente dar una notación para aquel conjunto que no tiene elementos.

Definición 1.9.4 Llamaremos **conjunto vacío**, denotado \emptyset , al conjunto que no tiene elementos.

Ejemplo. Este conjunto puede ser descrito de diferentes maneras, por ejemplo:

1. $\{n \in \mathbb{N}; n + 2 = 0\} = \emptyset$; 3. $\{r \in \mathbb{Q}; r = \sqrt{2}\} = \emptyset$
2. $\{n \in \mathbb{Z}; 2n = 1\} = \emptyset$; 4. $\{x \in \mathbb{R}; x^2 = -1\} = \emptyset$

Definición 1.9.5 Dado un conjunto A se define el **cardinal de A** como el número de elementos de A . Lo denotaremos por $|A|$ o bien por $\#A$.

1.9.1 Cuantificadores

Observación. Sea $U = \mathbb{Z}$. Consideremos los siguientes predicados:

$$(i) \ x = y + z; \quad (ii) \ x = y^2 + z^2$$

Cada vez que nos damos $x \in \mathbb{Z}$, existe $y, z \in \mathbb{Z}$ tal que $x = y + z$. Sin embargo no es verdadero que "cada vez que nos damos $x \in \mathbb{Z}$ ", "exista $y, z \in \mathbb{Z}$ tal que $x = y^2 + z^2$ ". Por ejemplo, para $x = 6$, no existe $y, z \in \mathbb{Z}$ tal que $6 = y^2 + z^2$, es decir el 6 no se puede escribir como suma de dos cuadrados.

Nota Queremos medir, cuantificar, la cantidad de elementos de un conjunto que hacen verdadero o falso un predicado.

Vamos a considerar tres casos: (1) Todo elemento, (2) Existe un elemento o (3) Existe un único elemento. El segundo caso, es en el sentido de "existe al menos un elemento"

Nota Cuando nos interese la cantidad exacta de elementos que satisfacen un predicado, hablaremos del "cardinal del conjunto."

Definición 1.9.6 *Se definen los siguientes cuantificadores:*

1. **Para todo**, denotado por \forall , una A hacia arriba, primera letra de la palabra "any" del inglés que significa para cada o para todo.
2. **Existe**, denotado por \exists , una E hacia la izquierda, primera letra de la palabra inglesa "exists" . *There exists= existe*
3. **Existe un único**, denotado por $\exists!$

Ejemplo.

1. $\forall n \in \mathbb{N}, n \geq 0$. Proposición verdadera.
2. $\forall n \in \mathbb{N}, n > 0$. Proposición falsa pues el 0 no la satisface.
3. $\exists n \in \mathbb{N}, n > 0$. Proposición verdadera.
4. $\exists n \in \mathbb{N}, n > 7$. Proposición verdadera.
5. $\exists! n \in \mathbb{Z}, n + 5 = 8$. Proposición verdadera.

Ejercicio

Sea $U = \{personas\}$. Comparemos las siguientes proposiciones:

1. $p : \forall y, \exists x; x \text{ ama a } y$.
2. $q : \exists y, \forall x; x \text{ ama a } y$.
3. $r : \forall y, \exists x; y \text{ ama a } x$.

4. $s : \exists y, \forall x; y \text{ ama a } x.$

En lenguaje de la vida diaria, tenemos

1. p : Toda persona es por alguien amada.
2. q : Existe una persona que es por todos amada.
3. r : Toda persona tiene a alguien a quien ama.
4. s : Existe una persona que nos ama a todos

1.9.2 Negación de los cuantificadores

La negación de la proposición: $\forall x; p(x)$ es $\exists x; \overline{p(x)}$.

La negación de la proposición: $\exists x; p(x)$ es $\forall x; \overline{p(x)}$

La negación de la proposición: $\exists! x; p(x)$ es

$$(\forall x; \overline{p(x)}) \vee (\exists x, y; p(x) \wedge p(y) \wedge x \neq y)$$

Ejemplo. Veamos la negación de las proposiciones anteriores:

1. $\overline{p} : \exists y, \forall x; x \text{ no ama a } y.$
2. $\overline{q} : \forall y, \exists x; x \text{ no ama a } y.$
3. $\overline{r} : \exists y, \forall x; y \text{ no ama a } x.$
4. $\overline{s} : \forall y, \exists x; y \text{ no ama a } x.$

En lenguaje de la vida diaria tenemos:

1. \overline{p} : Existe una persona que no es por nadie amada.
2. \overline{q} : Toda persona tiene alguien que no la ama.
3. \overline{r} : Existe una persona que no ama a nadie.

4. \bar{s} : Toda persona tiene a alguien a quien no ama.

Ejercicio

Negemos las proposiciones siguientes:

1. p : $\exists n, m, t \in \mathbb{N}$ tal que $n = m^2 + t^2$.
2. q : $\forall n \in \mathbb{Z}, \exists m, t \in \mathbb{Z}$ tal que $n = m + t$.
3. r : $\exists n \in \mathbb{N}, \forall m \in \mathbb{N}$ tal que $n \leq m$.
4. s : $\forall n \in \mathbb{N}, \exists m \in \mathbb{N}$ tal que $n = m + 1$
5. t : $\forall n \in \mathbb{N}, \exists m \in \mathbb{N}$ tal que $n + 1 = m$
6. u : $\exists! n \in \mathbb{Z}$ tal que $3 + n = 5$
7. v : $\exists! x \in \mathbb{R}$ tal que $x^2 = 4$

Sus negaciones son las siguientes:

1. \bar{p} : $\forall n, m, t \in \mathbb{N}, n \neq m^2 + t^2$.
2. \bar{q} : $\exists n \in \mathbb{Z}, \forall m, t \in \mathbb{Z}$ tal que $n \neq m + t$
3. \bar{r} : $\forall n \in \mathbb{N}, \exists m \in \mathbb{N}$ tal que $n > m$
4. \bar{s} : $\exists n \in \mathbb{N}, \forall m \in \mathbb{N}$ tal que $n \neq m + 1$
5. \bar{t} : $\exists n \in \mathbb{N}, \forall m \in \mathbb{N}$ tal que $n + 1 \neq m$
6. \bar{u} : $(\forall n \in \mathbb{Z}; 3 + n \neq 5) \vee (\exists n, m \in \mathbb{Z}; 3 + n = 5, 3 + m = 5 \wedge n \neq m)$
7. \bar{v} : $(\forall x \in \mathbb{R}; x^2 \neq 4) \vee (\exists x, y \in \mathbb{R}; x^2 = 4, y^2 = 4 \wedge x \neq y)$

En lenguaje cotidiano las proposiciones son:

1. p : Existen tres números naturales tales que uno de ellos es la suma de los cuadrados de los otros dos.

2. q : Todo número entero puede ser escrito como suma de otros dos números enteros.
3. r : Existe un número natural que es menor o igual a todo número natural.
4. s : Todo número natural es el sucesor de otro número natural.
5. t : Todo número natural tiene un sucesor.
6. u : Existe un único número entero que satisface la ecuación $3 + n = 5$.
7. v : Existe un único número real cuyo cuadrado es 4.

En lenguaje cotidiano la negación de las proposiciones es:

1. \bar{p} : Cada vez que tengo tres números naturales, uno de ellos no es la suma de los cuadrados de los otros dos.
2. \bar{q} : Existe un número entero que no puede ser escrito como suma de dos enteros.
3. \bar{r} : Para todo número natural, existe un número natural menor que él.
4. \bar{s} : Existe un número natural que no es sucesor de ningún número natural.
5. \bar{t} : Existe un número natural que no tiene sucesor.
6. \bar{u} : Al sumarle tres a cualquier número entero se obtiene siempre un número diferente de cinco o bien existen dos números enteros diferentes tal que al sumar tres a cada uno de ellos, se obtiene cinco como resultado.
7. \bar{v} : El cuadrado de todo número real es diferente de cuatro o bien existen dos números reales distintos cuyo cuadrado es cuatro.

1.9.3 Ejemplos y contraejemplos

Nota Para demostrar la proposición $\forall x; p(x)$, es necesario dar un argumento que demuestre la veracidad de $p(x)$, cualquiera sea el valor de x .

Si uno da varios ejemplos, incluso podrían ser infinitos ejemplos, esto NO es una demostración de la proposición. Es decir puede haber un número infinito de valores que satisfagan una proposición y sin embargo ser esta falsa.

Ejemplo. Sea $p: \forall n \in \mathbb{N}; n^2 \geq 7$. Vemos que hay infinitos números que la satisfacen, sin embargo es una proposición falsa ya que hay números naturales (por ejemplo el 2) cuyo cuadrado no es mayor o igual 7.

Observación. Pensemos en la proposición siguiente: p : Todos los árboles conservan sus hojas durante el invierno. ¿Cómo explicar que esta proposición es falsa? ¿Buscar toda una explicación biológica para explicar la falsedad de esta proposición? Hay una solución ¡trivial! Durante el invierno llevar a esa persona que afirma " p " y ponerla delante de un álamo o ciruelo o cualquier árbol que halla perdido sus hojas. Esto basta para explicar la falsedad de " p ". Diremos que el álamo o el ciruelo son contraejemplos. La idea es trivial, pero a veces es difícil encontrar un contraejemplo.

Definición 1.9.7 *Un contraejemplo de la proposición $\forall x; p(x)$ es un valor de x que no cumple $p(x)$*

Ejemplo. Demostremos que es falsa la proposición:

$$\forall x \in \mathbb{R}; \quad x^2 - 2x + 5 \leq 0$$

Basta considerar el contraejemplo $x = 0$, pues $0^2 - 2 \cdot 0 + 5 > 0$

1.9.4 Operaciones entre conjuntos

Definición 1.9.8 *Si S y T son conjuntos, diremos que S es un subconjunto de T y escribiremos $S \subset T$ o $S \subseteq T$ si todo elemento que*

pertenece a S , pertenece también a T , es decir

$$x \in S \Rightarrow x \in T$$

Ejemplo. Sea $S = \{\text{números pares}\}$, $T = \mathbb{Z}$. Tenemos $S \subset \mathbb{Z}$

Proposición 1.9.1 *Si $S \subset T$ y $T \subset S$ entonces $S = T$*

Demostración. $x \in S \Rightarrow x \in T$ y $x \in T \Rightarrow x \in S$. Luego $x \in S \Leftrightarrow x \in T$. Luego $S = T$

Proposición 1.9.2 *El conjunto vacío es subconjunto de todo conjunto. Es decir*

$$\emptyset \subset S, \quad \forall S \text{ conjunto}$$

Demostración. En efecto, supongamos que existe un $x \in \emptyset$. Esta proposición es falsa luego la implicación es verdadera, es decir, $x \in S$, cualquiera sea S

Proposición 1.9.3 *El conjunto vacío es único.*

Demostración. Supongamos que existen \emptyset y \emptyset' dos conjuntos vacíos. Tenemos: $\emptyset \subset \emptyset'$ y $\emptyset' \subset \emptyset$ y por la proposición anterior tenemos $\emptyset = \emptyset'$.

Definición 1.9.9 *Sea U el conjunto universal que estamos considerando. Si A es un subconjunto de U , su **complemento**, denotado \overline{A} , se define por*

$$\overline{A} = \{x \in U; x \notin A\}$$

Ejemplo. Sea $U = \mathbb{N}$.

1. Sea $A = \{n \in \mathbb{N}; n \text{ es par}\}$. Entonces $\overline{A} = \{n \in \mathbb{N}; n \text{ es impar}\}$.
2. Sea $B = \{n \in \mathbb{N}; n = 3m, \quad m \in \mathbb{N}\}$. Entonces

$$\overline{B} = \{n \in \mathbb{N}; n = 3m + 1 \quad \text{o} \quad n = 3m + 2, m \in \mathbb{N}\}$$

Observación. Se tiene que:

$$\begin{aligned}x \in \overline{A} &\Leftrightarrow \overline{x \in A} \\x \in A &\Leftrightarrow \text{no}(x \in \overline{A}) \Leftrightarrow \overline{x \in \overline{A}}\end{aligned}$$

Proposición 1.9.4 Sean A y B conjuntos, entonces

1. $\overline{\overline{A}} = A$
2. $A \subset B \Rightarrow \overline{B} \subset \overline{A}$

Demostración 1. $x \in \overline{\overline{A}} \Leftrightarrow \overline{x \in \overline{A}} \Leftrightarrow \overline{\overline{x \in A}} \Leftrightarrow x \in A$

Demostración 2. $x \in \overline{B} \Rightarrow \overline{x \in B} \Rightarrow \overline{x \in A} \Leftrightarrow x \in \overline{A}$.

1.9.5 Unión e intersección

En U , consideremos A y B dos conjuntos. La unión e intersección denotadas $A \cup B$ y $A \cap B$ respectivamente, están definidas por:

$$A \cup B = \{x \in U; x \in A \vee x \in B\}; A \cap B = \{x \in U; x \in A \wedge x \in B\}$$

Ejemplo. Sea $A = \{a, b, c, d\}$, $B = \{a, d, e, f\}$. Entonces

$$A \cup B = \{a, b, c, d, e, f\}; A \cap B = \{a, d\}$$

Proposición 1.9.5 Sean A, B conjuntos. Entonces

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Demostración. Es sencilla y se deja como ejercicio.

Nota Para el caso de tres conjuntos se tiene:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

Nota Todas las propiedades de las proposiciones de lógica se pueden utilizar en la teoría de conjuntos. A modo de ejercicio, veamos algunas de ellas.

Ejercicios Resueltos

1. Idempotencia de " \cup " y " \cap ", es decir $A \cup A = A$ y $A \cap A = A$.

Solución. $x \in A \cup A \Leftrightarrow (x \in A) \vee (x \in A) \Leftrightarrow x \in A$

$$x \in A \cap A \Leftrightarrow (x \in A) \wedge (x \in A) \Leftrightarrow x \in A$$

2. Leyes de Morgan

(a) $\overline{A \cap B} = \overline{A} \cup \overline{B}$

(b) $\overline{A \cup B} = \overline{A} \cap \overline{B}$

Solución. $x \in \overline{A \cap B} \Leftrightarrow x \in \overline{A \cap B} \Leftrightarrow \overline{(x \in A) \wedge (x \in B)} \Leftrightarrow$
 $\overline{x \in A \vee x \in B} \Leftrightarrow x \in \overline{A} \vee x \in \overline{B} \Leftrightarrow x \in \overline{A} \cup \overline{B}$

La segunda afirmación se demuestra de manera análoga a la anterior.

Nota De esta manera se demuestran todas las propiedades básicas de teoría de conjunto.

3. Usando las propiedades básicas, demostremos que

$$((A \cap B) \cup ((\overline{A} \cap \overline{B}) \cup B)) \cap A = A \cap B$$

Solución.

$$\begin{aligned} ((A \cap B) \cup ((\overline{A} \cap \overline{B}) \cup B)) \cap A &= \\ (A \cap B \cap A) \cup (((\overline{A} \cap \overline{B}) \cup B) \cap A) &= \\ (A \cap B) \cup (((\overline{A} \cap \overline{B} \cap A) \cup (B \cap A))) &= \\ (A \cap B) \cup (\emptyset \cup (B \cap A)) &= \\ (A \cap B) \cup (A \cap B) &= \\ A \cap B & \end{aligned}$$

4. En U simplifiquemos la expresión: $(A \cap B) \cup C \cup (\overline{A} \cap \overline{C}) \cup (\overline{C} \cap \overline{B})$

Solución.

$$\begin{aligned} (A \cap B) \cup C \cup (\overline{A} \cap \overline{C}) \cup (\overline{C} \cap \overline{B}) &= \\ (A \cap B) \cup C \cup (\overline{C} \cap (\overline{A} \cup \overline{B})) &= \\ (A \cap B) \cup C \cup (\overline{C} \cap (\overline{A \cap B})) &= \\ (A \cap B) \cup C \cup (\overline{C \cap (A \cap B)}) &= \\ U & \end{aligned}$$

5. Demostremos que: $(A \cup B) \cap (\bar{A} \cup \bar{B}) = (A \cap \bar{B}) \cup (\bar{A} \cap B)$

Solución.

$$\begin{aligned}
 (A \cup B) \cap (\bar{A} \cup \bar{B}) &= ((A \cup B) \cap \bar{A}) \cup ((A \cup B) \cap \bar{B}) \\
 &= (A \cap \bar{A}) \cup (B \cap \bar{A}) \cup (A \cap \bar{B}) \cup (B \cap \bar{B}) \\
 &= \emptyset \cup (\bar{A} \cap B) \cup (A \cap \bar{B}) \cup \emptyset \\
 &= (\bar{A} \cap B) \cup (A \cap \bar{B})
 \end{aligned}$$

6. Demostremos que: $A - (B \cup C) = (A - B) - C$

Solución. $A - (B \cup C) = A \cap \overline{(B \cup C)} = A \cap (\bar{B} \cap \bar{C}) =$
 $= (A \cap \bar{B}) \cap \bar{C} = (A - B) - C$

7. Demostremos que: $\overline{\overline{(A \cup B) \cap C} \cup \bar{B}} = B \cap C$

Solución.

$$\begin{aligned}
 \overline{\overline{(A \cup B) \cap C} \cup \bar{B}} &= \overline{\overline{(A \cup B) \cap C} \cap B} \\
 &= ((A \cup B) \cap C) \cap B \\
 &= ((A \cup B) \cap B) \cap C \\
 &= B \cap C
 \end{aligned}$$

Nótese que en la última igualdad utilizamos la ley de absorción.

8. Demostremos que: $((\bar{A} - B) \cup \bar{B}) - \bar{A} \cap (A \cup B) = A$

Solución. Comencemos por simplificar la primera expresión. Tenemos:

$$\overline{(\bar{A} - B)} \cup \bar{B} = \overline{(\bar{A} \cap \bar{B})} \cup \bar{B} = (A \cup B) \cup \bar{B} = A \cup (B \cup \bar{B}) = A \cup U = U.$$

Reemplacemos esta simplificación en la expresión inicial. Tenemos:

$$(U - \bar{A}) \cap (A \cup B) = (U \cap \bar{\bar{A}}) \cap (A \cup B) = A \cap (A \cup B) = A$$

1.9.6 Conjunto Potencia

Observación. Sea $A = \{a, b, c\}$. El conjunto formado por todos los subconjuntos de A , denotado $P(A)$, es el siguiente:

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

Será llamado "conjunto potencia de A ".

Definición 1.9.10 Sea A un conjunto cualquiera. Llamaremos **conjunto potencia** de A , denotado $P(A)$, al conjunto formado por todos los subconjuntos de A .

Teorema 1.9.6 Sea A un conjunto finito, entonces

$$|P(A)| = 2^{|A|}$$

Demostración. Sea A un conjunto y consideremos el conjunto $B = A \cup \{b\}$ con $b \notin A$. Comencemos por estudiar $P(B)$. Tenemos la situación siguiente: $T \subset B$ y $T \not\subset A \Rightarrow b \in T$.

Luego $T = S \cup \{b\}$, con $S \subset A$.

De donde

$$P(B) = \{S; S \subset A\} \cup \{S \cup \{b\}; S \subset A\}$$

Ambos conjuntos tienen el cardinal de $P(A)$. Luego

$$|P(B)| = 2 \cdot |P(A)|$$

Es decir cada vez que agregamos un elemento, se duplica el cardinal de la potencia del conjunto anterior. Luego tenemos que si A posee n elementos entonces $|P(A)| = 2^n$.

Proposición 1.9.7 Si $A \cap B = \emptyset$, entonces $P(A) \cap P(B) = \{\emptyset\}$.

Demostración. La proposición a demostrar es equivalente a demostrar:

$$P(A) \cap P(B) \neq \{\emptyset\} \implies A \cap B \neq \emptyset$$

Sea $P(A) \cap P(B) \neq \{\emptyset\}$, entonces existe $X \neq \emptyset$, $X \in P(A) \cap P(B)$. Luego $X \subset A$ y $X \subset B$. Es decir $X \subset A \cap B$. De donde $A \cap B \neq \emptyset$

Observación. La definición de igualdad de conjuntos dice que "dos conjuntos son iguales si tienen los mismos elementos". Ahora demostraremos que dos conjuntos son iguales si tienen los mismos subconjuntos. Es decir, si coinciden sus conjuntos potencia. Tenemos la proposición siguiente:

Proposición 1.9.8 $P(A) = P(B) \Leftrightarrow A = B$

Demostración. $A = B \Rightarrow P(A) = P(B)$ ¡Obvio!

Sea $P(A) = P(B)$. Por demostrar $A = B$.

$x \in A \Rightarrow \{x\} \subset A \Rightarrow \{x\} \in P(A) = P(B) \Rightarrow \{x\} \in P(B) \Rightarrow \{x\} \subset B \Rightarrow x \in B$. Luego hemos demostrado que $A \subset B$. En forma análoga se demuestra que $B \subset A$.

Proposición 1.9.9 $A \subset B \Leftrightarrow P(A \cup B) \subset P(B)$

Demostración. (i) Por demostrar: $A \subset B \Rightarrow P(A \cup B) \subset P(B)$. $X \in P(A \cup B) \Rightarrow X \subset A \cup B$. Pero $A \cup B = B$. Luego $X \subset B$. De donde $X \in P(B)$

(ii) Por demostrar: $P(A \cup B) \subset P(B) \Rightarrow A \subset B$.

$x \in A \Rightarrow x \in A \cup B \Rightarrow \{x\} \subset A \cup B \Rightarrow \{x\} \in P(A \cup B) \subseteq P(B) \Rightarrow \{x\} \in P(B) \Rightarrow \{x\} \subset B \Rightarrow x \in B$

1.9.7 Conjuntos numéricos

1. $\mathbb{N} = \{0, 1, 2, \dots, n, \dots\}$. El conjunto de los números naturales.
2. $\mathbb{Z} = \{\dots, -n, \dots, -2, -1, 0, 1, 2, \dots, n, \dots\}$. El conjunto de los números enteros.
3. $\mathbb{Q} = \{\frac{p}{q}; p, q \in \mathbb{Z}, q \neq 0\} = \{\text{decimales periódicos}\}$. El conjunto de los números racionales.
4. $\mathbb{R} = \{\text{números reales}\}$

5. $\mathbb{R}^+ = \{x \in \mathbb{R}; x > 0\}$. El conjunto de los reales positivos.
6. $\mathbb{R}^- = \{x \in \mathbb{R}; x < 0\}$. El conjunto de los reales negativos.
7. $\mathbb{R}^* = \mathbb{R} - \{0\}$
8. $I = \mathbb{R} - \mathbb{Q}$. El conjunto de los números irracionales.

Se tiene:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$$

1.9.8 Diferencia simétrica

Sean A y B dos conjuntos. Llamaremos **diferencia simétrica entre** A y B , denotado $A \triangle B$, al conjunto siguiente

$$A \triangle B = (A - B) \cup (B - A)$$

Ejercicio. Demostremos que: $A \triangle B = A \triangle C \implies B = C$

Demostración. Por demostrar

$$(A - B) \cup (B - A) = (A - C) \cup (C - A) \implies B = C$$

Consideremos las proposiciones siguientes:

$$p : x \in A; \quad q : x \in B; \quad r : x \in C$$

Entonces nosotros queremos demostrar la siguiente proposición:

$$(p \wedge \bar{q}) \vee (q \wedge \bar{p}) \equiv (p \wedge \bar{r}) \vee (r \wedge \bar{p}) \Rightarrow (q \Leftrightarrow r)$$

Hemos visto que:

$$(a \wedge b) \vee (\bar{a} \wedge \bar{b}) \equiv (a \Leftrightarrow b)$$

Luego

$$(p \wedge \bar{q}) \vee (q \wedge \bar{p}) \equiv (p \wedge \bar{r}) \vee (r \wedge \bar{p})$$

Es equivalente a

$$(p \Leftrightarrow \bar{q}) \equiv (p \Leftrightarrow \bar{r})$$

Luego $\bar{q} \Leftrightarrow \bar{r}$. De donde $q \Leftrightarrow r$

1.10 Ejercicios Propuestos

1. (a) Traduzca a lenguaje ordinario las proposiciones siguientes:
 - i. $(\forall n \in \mathbb{N})(\exists m \in \mathbb{N}), m > n$
 - ii. $(\exists m \in \mathbb{N})(\forall n \in \mathbb{N}), m > n$
 - iii. $(\forall x, y \in \mathbb{Q})(\exists z \in \mathbb{Q}), x < z < y$
 - iv. $(n \in \mathbb{N} \text{ y } m \in \mathbb{N}) \Rightarrow (n + m \in \mathbb{N} \text{ y } n - m \in \mathbb{N})$
 - v. $(\forall n \in \mathbb{N}) n > 3 \Rightarrow n > 6$
 - vi. $(\forall r \in \mathbb{Q})(\exists m, n \in \mathbb{N}), r = \frac{m}{n}$
 - vii. $(\forall x \in X)(\exists A \in P(X)), x \in A$
 - viii. $(\forall A \in P(X))(\exists x \in X), x \in A$(b) Diga si ellas son verdaderas o falsas. Explique o pruebe si corresponde.
2. Traduzca a lenguaje formal las proposiciones siguientes:
 - (a) La suma y el producto de dos números racionales son números racionales.
 - (b) Todo número real positivo posee una raíz cuadrada.
 - (c) El cuadrado de todo número real es positivo.
 - (d) Todo número racional multiplicado por 1 es igual a él mismo.
 - (e) Un número divisible por 10 es divisible por 5.
 - (f) Todo número par es divisible por 4.
 - (g) El cuadrado de un número par es divisible por 4.
 - (h) El producto de dos números es positivo si y sólo si ellos tienen el mismo signo.
 - (i) Un triángulo es equilátero si y sólo si sus ángulos son iguales.
 - (j) Un cuadrilátero es un cuadrado si y sólo si todos sus ángulos son iguales.
 - (k) 2 y 3 son las únicas raíces de la ecuación $x^2 - 6x + 5 = 0$.

- (l) Para todos los números reales x e y se tiene ya sea x es menor o igual a y , o bien y es menor o igual a x .
 - (m) Existen dos conjuntos A y B tales que ni A está incluido en B , ni B está incluido en A .
- ¿Cuáles de estas proposiciones son ciertas?
3. Pruebe sirviéndose de las tablas de verdad las tautologías siguientes:

- (a) $(p \Rightarrow q) \Leftrightarrow (\bar{q} \Rightarrow \bar{p})$
- (b) $\overline{(p \wedge q)} \Leftrightarrow (\bar{p} \vee \bar{q})$
- (c) $\overline{(p \vee q)} \Leftrightarrow (\bar{p} \wedge \bar{q})$
- (d) $(p \Rightarrow q) \Leftrightarrow (\bar{p} \vee q)$
- (e) $((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$.

Aplique estas tautologías para probar

- (a) Si n^2 es par entonces n es par.
 - (b) Sean A y B subconjuntos de un conjunto X . Pruebe que $A \subset B$ ssi $\bar{A} \cup B = X$
 - (c) Si $A \subset B$ y $B \subset C$ entonces $A \subset C$.
4. Sirviéndose de las reglas

$$\overline{((\exists x)p(x))} \Leftrightarrow (\forall x)(\overline{p(x)})$$

$$\overline{((\forall x)p(x))} \Leftrightarrow (\exists x)(\overline{p(x)})$$

Encuentre las negaciones de las proposiciones siguientes:

- (a) Toda parte de un conjunto finito es finito
- (b) El cuadrado de un número par es divisible por 4
- (c) Todo número primo es impar
- (d) Existe un hombre que no es mortal
- (e) Para todo entero x existe un entero mayor que él

5. Dibuje los circuitos correspondientes a las expresiones simbólicas siguientes:

(a) $(P \wedge Q) \vee \overline{P}$

(b) $(P \wedge \overline{Q}) \vee (\overline{P} \wedge Q)$

(c) $(P \wedge Q) \vee R \vee (\overline{P} \wedge \overline{Q} \wedge \overline{R})$

6. ¿Qué tipo de circuito le corresponde a una tautología ?, dé un ejemplo.

7. Sea $A = \{a, \{a\}, \{a, \{a\}\}\}$. Diga cuáles de las siguientes afirmaciones son verdaderas:

(a) $a \subseteq A$ (b) $a \in A$ (c) $\{a\} \in A$ (d) $\{a\} \subseteq A$

(e) $\{\{a\}\} \subseteq A$ (f) $\{\{a\}, a\} \subseteq A$ (g) $\{\{a\}, a\} \in A$

8. Sea $A = \{a, \emptyset, \{b\}, \{a\}, \{\emptyset\}, \{a, \emptyset\}\}$. Encuentre $P(A)$.

9. ¿Puede dar un ejemplo en que $P(A) = \emptyset$?

10. Diga si es válido el siguiente argumento, utilizando diagrama de Venn.

Todos los productos baratos son baratijas

Todas las baratijas se agotan

Todos los productos baratos se agotan.

11. Use un diagrama de Venn para obtener una conclusión válida para el siguiente argumento.

Algunos comerciales de televisión son inefectivos

Todos los comerciales de televisión son cuidadosamente diseñados

12. Un hotel recibe 60 visitantes, de los cuales 37 permanecen al menos una semana, 43 gastan al menos \$ 30 diarios, 32 están completamente satisfechos del servicio; 30 permanecieron al menos una semana y gastaron al menos \$ 30 diarios; 26 permanecieron al menos una semana y quedaron completamente satisfechos; 27 gastaron al menos \$ 30 diarios y quedaron completamente satisfechos y 24 permanecieron al menos una semana, gastaron al menos \$ 30 diarios y quedaron completamente satisfechos.
- a) ¿Cuántos visitantes permanecieron al menos una semana, gastaron al menos \$ 30 diarios pero no quedaron completamente satisfechos?
- b) ¿Cuántos visitantes quedaron completamente satisfechos pero permanecieron menos de una semana y gastaron menos de \$ 30 diarios?
- c) ¿Cuántos visitantes permanecieron menos de una semana, gastaron menos de \$ 30 diarios y no quedaron completamente satisfechos?
13. Sean A , B subconjuntos de un conjunto X : Pruebe, usando un diagrama de Venn que $(A \cap B^c) \cup (A^c \cap B) = A \cup B \iff A \cap B = \emptyset$
14. Demuestre que
- (a) $A \cap B = \emptyset \Rightarrow P(A) \cap P(B) = \{\emptyset\}$
- (b) $A^c \setminus B^c = B \setminus A$
15. Demuestre que
- (a) $A \cup B = \emptyset \Rightarrow A = \emptyset \wedge B = \emptyset$
- (b) $A \cap (A \cup B) = A$
16. ¿Para cuáles $S \in \{\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ son verdaderas las siguientes afirmaciones?
- (a) $\{x \in S / x^2 = 5\} \neq \emptyset$

- (b) $\{x \in S \mid |x - 1| \leq \frac{1}{2}\} = \{1\}$
 (c) $\{x \in \mathbb{R} \mid x^2 = -1\} = \emptyset$
17. Dé un ejemplo de tres conjuntos A , B y C tales que ellos cumplan $A \cap B \neq \emptyset$, $B \cap C \neq \emptyset$, $A \cap C \neq \emptyset$ pero $A \cap B \cap C = \emptyset$
18. Determine las posibles relaciones de inclusión entre A y B :
- a) $A = \{0, 1, 2, 6\}$, $B = \{ \text{divisores de } 30 \}$
 b) $A = X - (Y - T)$, $B = T$
 c) $A = E - S$, $B = \{x \in S; x \in E - S\}$
 d) $A = P(E - S)$, $B = P(E) - P(S)$
19. Demuestre que
- (a) $\overline{(A \cup (B \cap C) \cup (\overline{B} \cap \overline{C}) \cup C)} = \overline{(A \cup C)} \cap B$
 (b) $A \cup ((A - B) \cap B) \cup \overline{(\overline{A} \cup \overline{B})} = A$
 (c) $(\overline{A} \cup \overline{B}) \cap (\overline{A} \cup B) = \overline{A}$
 (d) $A \cap (B - C) = (A \cap B) - (A \cap C)$
 (e) $A - (B - C) = (A - B) \cup (A \cap C)$
 (f) $(A - B) - C = A - (B \cup C)$
20. Escriba como expresión lógica las expresiones conjuntistas siguientes:
- (a) $(A \subset B \wedge B \subset C) \Rightarrow (A \subset C)$
 (b) $A \subset B \Leftrightarrow A \cap B = A$
21. Demuestre que:
- $$(A - B) \cup (B - A) = (A \cup B) - (A \cap B)$$
22. Demuestre que:
- (a) $(A \cap B) - C = (A - C) \cap (B - C)$

$$(b) \overline{(\overline{A} - \overline{C})} - (\overline{A} - B) = A \cup (B - C)$$

$$(c) A \cup (B - C) = (A \cup B) - (C - A)$$

23. Demuestre las identidades:

$$(a) X - (Y - X) = X$$

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

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

$$(d) P(A) \cup P(B) \subset P(A \cup B)$$

$$(e) P(A) \cup P(B) = P(A \cup B) \Leftrightarrow A \subset B \text{ o } B \subset A$$

24. Resuelva en $P(E)$ las ecuaciones:

$$a) X - A = \emptyset \qquad b) X - (A \cap X) = \emptyset$$

$$c) A - (X - A) = X \quad d) A \cup X = B$$

$$e) A \cap X = B$$

Capítulo 2

Sumatorias y Recurrencia

2.1 Sumatorias

Motivación. Queremos encontrar el valor de sumas tales como:

$$1^3 + 2^3 + 3^3 + \dots + 5.000^3$$

o bien

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \dots + n(n+1)$$

Problema. Comencemos por algo sencillo. Busquemos el valor de la suma de 1 a 50.

Gauss (1.777-1.855) a temprana edad, tuvo el chispazo genial siguiente:

$$\begin{array}{cccccccc} 1 & + & 2 & + & 3 & + & \dots & + & 48 & + & 49 & + & 50 \\ 50 & + & 49 & + & 48 & + & \dots & + & 3 & + & 2 & + & 1 \end{array}$$

Si sumamos hacia abajo tenemos 50 veces 51. Luego

$$2(1 + 2 + 3 \dots + 48 + 49 + 50) = 50 \cdot 51$$

De donde

$$1 + 2 + 3 + \dots + 50 = \frac{50 \cdot 51}{2}$$

Problema. Ahora nos interesa la siguiente suma:

$$1 + 2 + 3 + \cdots + (n - 1) + n$$

Donde n es un número natural cualquiera. Hacemos el mismo cálculo:

$$\begin{array}{ccccccc} 1 & + & 2 & + & \cdots & + & (n - 1) & + & n \\ n & + & (n - 1) & + & \cdots & + & 2 & + & 1 \end{array}$$

Si sumamos en forma vertical tenemos n veces $(n + 1)$. Pero hemos sumado dos veces la suma pedida. Luego:

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

De donde:

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

Nota. Por un método un poco más sofisticado, se puede encontrar el valor de la suma de los cuadrados, de los cubos y otros. Los dos primeros los buscaremos al final de esta sección.

Estos resultados son:

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n + 1)(2n + 1)}{6}$$

$$1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{(n(n + 1))^2}{4}$$

Problema. Ahora trataremos de calcular sumas con n términos que tengan formas tales como:

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots$$

$$1 \cdot 3 + 3 \cdot 5 + 5 \cdot 7 + \cdots$$

$$1 \cdot 11 + 2 \cdot 12 + 3 \cdot 13 + \cdots$$

$$1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + \cdots$$

Para esto será necesario hacer uso del concepto y propiedades de "sumatoria"

Definición 2.1.1 Sumatoria es la suma de n terminos que están *construídos con una cierta regla*.

Observación. Ahora vamos a introducir una notación que es muy útil. Comencemos por verlo en ejemplos.

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

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

Notación. $a_0 + a_1 + a_2 + \cdots + a_n = \sum_{i=0}^n a_i$

De la misma manera puede ser denotado como sigue:

$$\sum_{k=1}^n a_k \quad \text{o bien} \quad \sum_{l=1}^n a_l \quad \text{etc.}$$

Ejercicio. Escribamos en forma de sumatoria, la suma de los n primeros términos de cada una de las expresiones siguientes:

1. $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots$
2. $1 \cdot 11 + 2 \cdot 12 + 3 \cdot 13 + \cdots$
3. $1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + \cdots$
4. $1 \cdot 3 + 2 \cdot 5 + 3 \cdot 7 + \cdots$
5. $1 \cdot 3 + 3 \cdot 5 + 5 \cdot 7 + \cdots$
6. $9 + 11 + 13 + 15 + \cdots$

Solución.

1. El término general es de la forma: $k(k+1)$. Luego la suma pedida tiene la forma

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

2. El término general es de la forma: $k(k + 10)$. Luego la suma pedida es

$$\sum_{k=1}^n k(k + 10)$$

3. El término general es $k(k + 2)$. Luego la suma pedida es

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

4. Los segundos números son impares. Todo número impar es de la forma $2k + 1$. Necesitamos que para $k = 1$ el impar sea 3. Luego el término general es de la forma $k(2k + 1)$. La suma pedida se escribe

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

5. Ahora tenemos dos impares seguidos. Pero queremos empezar por $k = 1$, el término general tendrá la forma: $(2k - 1)(2k + 1)$. La suma pedida es

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

6. Se va sumando 2 (progresión aritmética). Luego escribiremos $9 = 2 \cdot 1 + 7$; $11 = 2 \cdot 2 + 7$; $13 = 2 \cdot 3 + 7$. Luego el término general es de la forma $2 \cdot k + 7$. Se nos pide

$$\sum_{k=1}^n (2k + 7)$$

2.1.1 Propiedades de la sumatoria

Observación. $(1^2 + 1) + (2^2 + 2) + (3^2 + 3) = (1^2 + 2^2 + 3^2) + (1 + 2 + 3)$.
Es decir:

$$\sum_{k=1}^3 (k^2 + k) = \sum_{k=1}^3 k^2 + \sum_{k=1}^3 k$$

Observación.

$$(1^2 + 1) + (2^2 + 2) + \cdots + (n^2 + n) = (1^2 + 2^2 + \cdots + n^2) + (1 + 2 + \cdots + n)$$

Es decir:

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

En general, tenemos la propiedad siguiente:

$$\sum_{k=1}^n (a_k + b_k) = \sum_{k=1}^n a_k + \sum_{k=1}^n b_k$$

Observación. $5 \cdot 1^2 + 5 \cdot 2^2 + \cdots + 5 \cdot n^2 = 5 \cdot (1^2 + 2^2 + \cdots + n^2)$.

Luego

$$\sum_{k=1}^n 5k^2 = 5 \sum_{k=1}^n k^2$$

Es decir factorizar por 5 equivale a sacar el 5 fuera de la sumatoria.

En general se tiene:

$$\sum_{k=1}^n (a \cdot a_k) = a \cdot \sum_{k=1}^n a_k$$

Ahora estamos en condiciones de poder calcular las sumatorias escritas anteriormente.

Ejercicios Resueltos

1. Busquemos el valor de la suma de los n primeros términos de la sumatoria que comienza por:

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots$$

Solución. Vimos que el término general es de la forma: $k \cdot (k+1)$

Tenemos:

$$\begin{aligned}
 \sum_{k=1}^n k(k+1) &= \sum_{k=1}^n k^2 + \sum_{k=1}^n k \\
 &= \frac{n(n+1)(2n+1)}{6} + \frac{n(n+1)}{2} \\
 &= \frac{n(n+1)(2n+1) + 3n(n+1)}{6} \\
 &= \frac{n(n+1)(2n+1+3)}{6} \\
 &= \frac{n(n+1)(n+2)}{3}
 \end{aligned}$$

Pregunta: ¿Por qué la cantidad $\frac{n(n+1)(n+2)}{3}$ es un número natural?

2. Busquemos el valor de la suma de los n primeros términos de la sumatoria que comienza por:

$$1 \cdot 11 + 2 \cdot 12 + 3 \cdot 13 + \dots$$

Solución. Entonces tenemos

$$\begin{aligned}
 1 \cdot 11 + 2 \cdot 12 + \dots + n(n+10) &= \sum_{k=1}^n k(k+10) \\
 &= \sum_{k=1}^n (k^2 + 10k) \\
 &= \sum_{k=1}^n k^2 + 10 \sum_{k=1}^n k \\
 &= \frac{n(n+1)(2n+1)}{6} + \frac{10n(n+1)}{2} \\
 &= \frac{n(n+1)(2n+1+30)}{6} \\
 &= \frac{n(n+1)(2n+31)}{6}
 \end{aligned}$$

3. Idem ejercicio anterior para:

$$1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + \dots$$

Solución.

$$\begin{aligned}
 1 \cdot 3 + \cdots + n(n+2) &= \sum_{k=1}^n k(k+2) \\
 &= \sum_{k=1}^n (k^2 + 2k) \\
 &= \sum_{k=1}^n k^2 + 2 \sum_{k=1}^n k \\
 &= \frac{n(n+1)(2n+1)}{6} + \frac{2n(n+1)}{2} \\
 &= \frac{n(n+1)(2n+1+6)}{6} \\
 &= \frac{n(n+1)(2n+7)}{6}
 \end{aligned}$$

4. Al igual que el ejercicio anterior para la sumatoria que comienza por:

$$1 \cdot 3 + 3 \cdot 5 + 5 \cdot 7 + \cdots$$

Solución.

$$\begin{aligned}
 1 \cdot 3 + \cdots + (2n-1) \cdot (2n+1) &= \sum_{k=1}^n (2k-1)(2k+1) \\
 &= \sum_{k=1}^n (4k^2 - 1) \\
 &= 4 \left(\sum_{k=1}^n k^2 \right) - n \\
 &= \frac{4n(n+1)(2n+1)}{6} - n \\
 &= \frac{n((2n+2)(2n+1) - 3)}{3} \\
 &= \frac{n(4n^2 + 6n - 1)}{3}
 \end{aligned}$$

Nota. En el capítulo dedicado a la aritmética veremos que 3 divide a $n(4n^2 + 6n - 1)$

5. Idem al ejercicio anterior

$$7 \cdot 1 + 9 \cdot 2 + 11 \cdot 3 + \cdots$$

Solución. Tenemos $7, 9, 11, \dots$. Estos números van uno por medio, luego tenemos $2k$. Para $n = 1$, se tiene $7 = 2 \cdot 1 + 5$. Luego el término general es de la forma: $2k + 5$ Entonces

$$\begin{aligned} \sum_{k=1}^n (2k + 5)k &= \sum_{k=1}^n (2k^2 + 5k) \\ &= 2 \sum_{k=1}^n k^2 + 5 \sum_{k=1}^n k \\ &= \frac{2n(n+1)(2n+1)}{6} + \frac{5n(n+1)}{2} \\ &= \frac{n(n+1)(4n+2+15)}{6} \\ &= \frac{n(n+1)(4n+17)}{6} \end{aligned}$$

Nota. En la sección de Aritmética veremos que $\frac{n(n+1)(4n+17)}{6}$ es un número natural.

6. Expresemos como un producto de números naturales $\sum_{k=1}^{48} k^2$.

Solución. $\sum_{k=1}^{48} k^2 = \frac{48 \cdot 49 \cdot (2 \cdot 48 + 1)}{6}$. Es decir $8 \cdot 49 \cdot 97$

7. Calculemos: $5^2 + 6^2 + 7^2 + \dots + 50^2$.

Solución.

$$\begin{aligned} \sum_{k=5}^{50} k^2 &= \sum_{k=1}^{50} k^2 - \sum_{k=1}^4 k^2 \\ &= \frac{50 \cdot 51 \cdot 101}{6} - \frac{4 \cdot 5 \cdot 9}{6} \\ &= 25 \cdot 17 \cdot 101 - 30 \end{aligned}$$

Curiosidad. En ambos casos las fracciones se simplificaron hasta obtener 1 en el denominador. Luego obtuvimos un número entero. ¡Corresponde! pues al lado izquierdo se tiene un número entero.

8. Encontremos el valor de la sumatoria: $\sum_{k=5}^{10} (2k - 1)^2$

Solución.

$$\begin{aligned}
\sum_{k=5}^{10} (2k-1)^2 &= \sum_{k=1}^{10} (2k-1)^2 - \sum_{k=1}^4 (2k-1)^2 \\
&= \sum_{k=1}^{10} (4k^2 - 4k + 1) - \sum_{k=1}^4 (4k^2 - 4k + 1) \\
&= \frac{4 \cdot 10 \cdot 11 \cdot 21}{6} - \frac{4 \cdot 10 \cdot 11}{2} + 10 - \left(\frac{4 \cdot 4 \cdot 5 \cdot 9}{6} - \frac{4 \cdot 4 \cdot 5}{2} + 4 \right) \\
&= 1246
\end{aligned}$$

9. Calculemos:

$$\sum_{k=10}^{100} k^2$$

Solución.

$$\begin{aligned}
\sum_{k=10}^{100} k^2 &= \sum_{k=1}^{100} k^2 - \sum_{k=1}^9 k^2 \\
&= \frac{100 \cdot 101 \cdot 201}{6} - \frac{9 \cdot 10 \cdot 19}{6} \\
&= 50 \cdot 101 \cdot 67 - 15 \cdot 19
\end{aligned}$$

10. Encontremos el valor de la sumatoria: $\sum_{k=8}^{200} (2k-1)(3k+1)$ **Solución.**

$$\begin{aligned}
\sum_{k=8}^{200} (2k-1)(3k+1) &= \sum_{k=8}^{200} (6k^2 - k - 1) \\
&= \sum_{k=1}^{200} (6k^2 - k - 1) - \sum_{k=1}^7 (6k^2 - k - 1) \\
&= 6 \sum_{k=1}^{200} k^2 - \sum_{k=1}^{200} k - 200 - 6 \sum_{k=1}^7 k^2 + \sum_{k=1}^7 k + 7 \\
&= \frac{6 \cdot 200 \cdot 201 \cdot 401}{6} - \frac{200 \cdot 201}{2} - 193 - \frac{6 \cdot 7 \cdot 8 \cdot 15}{6} + \frac{7 \cdot 8}{2} \\
&= 200 \cdot 201 \cdot 401 - 20 \cdot 100 - 193 - 7 \cdot 8 \cdot 15 + 28
\end{aligned}$$

11. Sabiendo que:

$$\begin{aligned}
1 + 2 + 3 + \dots + n &= \frac{n(n+1)}{2} \\
1^2 + 2^2 + 3^2 + \dots + n^2 &= \frac{n(n+1)(2n+1)}{6}
\end{aligned}$$

Encontremos

$$\begin{array}{lll} (1) \sum_{k=1}^{n+3} k & (2) \sum_{k=1}^{n+2} k^2 & (3) \sum_{k=1}^{n-1} k \\ (4) \sum_{k=1}^{n-1} k^2 & (5) \sum_{k=1}^{n-3} k & (6) \sum_{k=1}^{n-4} k^2 \end{array}$$

Solución

$$\begin{array}{ll} (1) \sum_{k=1}^{n+3} k = \frac{(n+3)(n+4)}{2} & (2) \sum_{k=1}^{n+2} k^2 = \frac{(n+2)(n+3)(2n+5)}{6} \\ (3) \sum_{k=1}^{n-1} k = \frac{(n-1)n}{2} & (4) \sum_{k=1}^{n-1} k^2 = \frac{(n-1)n(2n-1)}{6} \\ (5) \sum_{k=1}^{n-3} k = \frac{(n-3)(n-2)}{2} & (6) \sum_{k=1}^{n-4} k^2 = \frac{(n-4)(n-3)(2n-7)}{6} \end{array}$$

12. Sabiendo que

$$\frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \cdots + \frac{1}{(2n-1) \cdot (2n+1)} = \frac{n}{2n+1}$$

Encontremos el valor de:

$$\begin{array}{l} (1) \frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \cdots + \frac{1}{15 \cdot 17} \\ (2) \frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \cdots + \frac{1}{(2n+9) \cdot (2n+11)} \end{array}$$

Solución (1) Escribimos 17 de la forma: $17 = 16 + 1 = 2 \cdot 8 + 1$.

Luego

$$\frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \cdots + \frac{1}{15 \cdot 17} = \frac{8}{17}$$

Solución (2) Tenemos que $2n+11 = (2n+10)+1 = 2(n+5)+1$.

Además $2n+11$ es mayor que $2n+9$. Luego

$$\frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \cdots + \frac{1}{(2n+9) \cdot (2n+11)} = \frac{n+5}{2n+11}$$

13. Busquemos el valor de la suma de los n primeros términos de la sumatoria:

$$1 \cdot 3 + 2 \cdot 5 + 3 \cdot 7 + \dots$$

Solución. El término general es de la forma $k(2k+1)$. Luego se tiene la sumatoria

$$\begin{aligned} \sum_{k=1}^n k(2k+1) &= \sum_{k=1}^n (2k^2 + k) \\ &= 2 \sum_{k=1}^n k^2 + \sum_{k=1}^n k \\ &= \frac{2n(n+1)(2n+1)}{6} + \frac{n(n+1)}{2} \\ &= \frac{n(n+1)(4n+2+3)}{6} \\ &= \frac{n(n+1)(4n+5)}{6} \end{aligned}$$

14. Encontremos la suma de los n primeros términos de la sumatoria:

$$1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + 3 \cdot 4 \cdot 5 + \dots$$

Solución. El término general es de la forma $k(k+1)(k+2)$. Luego se tiene la sumatoria

$$\begin{aligned} \sum_{k=1}^n k(k+1)(k+2) &= \sum_{k=1}^n (k^3 + k^2 + 2k) \\ &= \sum_{k=1}^n (k^3 + 3k^2 + 2k) \\ &= \sum_{k=1}^n k^3 + 3 \sum_{k=1}^n k^2 + 2 \sum_{k=1}^n k \\ &= \frac{n^2(n+1)^2}{4} + \frac{3n(n+1)(2n+1)}{6} + n(n+1) \\ &= \frac{n(n+1)(3n(n+1) + 6(2n+1) + 12)}{12} \\ &= \frac{n(n+1)(3n^2 + 15n + 18)}{12} \\ &= \frac{n(n+1)(n^2 + 5n + 6)}{4} \\ &= \frac{n(n+1)(n+2)(n+3)}{4} \end{aligned}$$

15. Encuentre la suma de los n primeros términos de la sumatoria:

$$(6 + 5 \cdot 1) + (6 + 5 \cdot 2) + (6 + 5 \cdot 3) + \cdots$$

Solución. El n -ésimo término de la sumatoria es de la forma $6 + 5 \cdot n$. Luego tenemos:

$$\begin{aligned} \sum_{k=1}^n (6 + 5 \cdot k) &= 6n + 5 \sum_{k=1}^n k \\ &= 6n + \frac{5n(n+1)}{2} \\ &= \frac{n(17 + 5n)}{2} \end{aligned}$$

2.1.2 Progresiones aritméticas

Definición 2.1.2 Una **progresión aritmética**, es una sucesión de la forma:

$$a, a + d, a + 2d, \cdots, a + (n - 1)d$$

Donde d es llamada la *diferencia de la progresión*.

Observe que el segundo término de la progresión es $a + d$, el tercero es $a + 2d$. El n -ésimo término es $a + (n - 1)d$.

Sea s_n la suma de los n primeros términos. Entonces

$$s_n = a + (a + d) + (a + 2d) + \cdots + (a + (n - 1)d)$$

$$s_n = na + (1 + 2 + \cdots + (n - 1))d$$

$$s_n = na + \frac{(n - 1) \cdot n \cdot d}{2}$$

$$s_n = \frac{n(2a + (n - 1)d)}{2}$$

O bien, puesto que el n -ésimo término es $a_n = a + (n - 1)d$, entonces la suma se puede escribir como sigue:

$$s_n = \frac{a_1 + a_n}{2}$$

Donde $a_1 = a$

Ejercicio

Encontremos la suma de los n primeros términos de la progresión aritmética siguiente:

$$5 + 8 + 11 + 14 + \dots$$

Solución.

Se tiene que $a_1 = 5$ y $d = 3$. Luego

$$s_n = \frac{n(5 + (n - 1) \cdot 3)}{2} = \frac{n(3n + 2)}{2}$$

Ejercicio

En una progresión aritmética, el primer término es 4, el último 37 y la suma es 246. Encuentre el número de términos y la diferencia.

Solución

$$s_n = \frac{n(4 + 37)}{2} = 246. \text{ Luego } n = 12.$$

Por otra parte: $37 = 4 + 11d$. Luego $d = 3$.

Ejercicio El primer término de una progresión aritmética es 2. Si amplifcamos el primer término por 2, el segundo por 3 y le sumamos 26 unidades al tercer término, se tiene nuevamente una progresión aritmética. Encuentre ambas progresiones.

Ejercicio

1^{era} progresión: $2, 2 + d, 2 + 2d$

2^a progresión: $4, 6 + 3d, 2 + 2d + 26$ Por ser la segunda progresión aritmética, se tiene la igualdad siguiente:

$$6 + 3d - 4 = 2 + 2d + 26 - (6 + 3d)$$

De donde $d = 5$

Luego las dos progresiones buscadas son: 2, 7, 12 y 4, 21, 38

2.1.3 Progresiones Geométricas

Ejemplos de progresiones geométricas

$$3 + 3 \cdot 2 + 3 \cdot 2^2 + \dots + 3 \cdot 2^{n-1}$$

$$5 + 5 \cdot 4 + 5 \cdot 4^2 + \dots + 5 \cdot 4^{n-1}$$

Definición 2.1.3 Una **progresión geométrica**, es una sucesión del tipo:

$$a, a \cdot r, a \cdot r^2, a \cdot r^3, \dots a \cdot r^{n-1}$$

donde r es llamada la razón de la progresión. Nuestro problema es calcular la suma de los n primeros términos de la progresión geométrica.

Observación. Veamos un procedimiento similar al que usamos para sumar los n primeros términos de la sumatoria $1 + 2 + 3 + \dots + n$. Busquemos el valor de la sumatoria siguiente:

$$3 + 3 \cdot 2 + 3 \cdot 2^2 + \dots + 3 \cdot 2^{n-1}$$

Sea

$$s_n = 3 + 3 \cdot 2 + 3 \cdot 2^2 + \dots + 3 \cdot 2^{n-1}$$

Multipliquemos ambos lados de la igualdad por -2 . Se tiene:

$$\begin{aligned} s_n &= 3 + 3 \cdot 2 + 3 \cdot 2^2 + \dots + 3 \cdot 2^{n-1} \\ -2s_n &= -3 \cdot 2 - 3 \cdot 2^2 - 3 \cdot 2^3 - \dots - 3 \cdot 2^{n-2} - 3 \cdot 2^n \end{aligned}$$

Tenemos :

$$s_n - 2s_n = 3 - 3 \cdot 2^n$$

De donde

$$(1 - 2)s_n = 3(1 - 2^n)$$

Luego

$$s_n = \frac{3(1 - 2^n)}{1 - 2}$$

Caso general

Dada la progresión geométrica

$$a, a \cdot r, a \cdot r^2, a \cdot r^3, \dots, a \cdot r^{n-1}, \dots \text{ con } r \neq 1$$

La suma de los n primeros terminos es:

$$s_n = a + a \cdot r + a \cdot r^2 + a \cdot r^3 + \dots + a \cdot r^{n-1}$$

Calculemos esta suma. En efecto, consideremos

$$s_n = a + a \cdot r + a \cdot r^2 + a \cdot r^3 + \dots + a \cdot r^{n-1} \text{ y}$$

$$-rs_n = -a \cdot r - a \cdot r^2 - a \cdot r^3 - \dots - a \cdot r^n$$

Sumando ambas igualdades se obtiene

$$s_n - r \cdot s_n = a - a \cdot r^n$$

Factorizando queda:

$$(1 - r)s_n = a(1 - r^n)$$

De donde

$$s_n = \frac{a(1 - r^n)}{1 - r}$$

Donde a es el primer término de la progresión y r es la razón de la progresión.

Ejemplo

$$\begin{aligned} 7 + 7 \cdot \frac{1}{3} + 7 \cdot \left(\frac{1}{3}\right)^2 + \dots + 7 \cdot \left(\frac{1}{3}\right)^{n-1} &= \frac{7(1 - (\frac{1}{3})^n)}{1 - \frac{1}{3}} \\ &= \frac{7(1 - (\frac{1}{3})^n)}{\frac{2}{3}} \end{aligned}$$

Ejercicio

Inserte 5 términos en una progresión geométrica que tiene por extremos 3 y 192

Solución

La progresión geométrica buscada es:

$$3, 3 \cdot r, 3 \cdot r^2, 3 \cdot r^3, 3 \cdot r^4, 3 \cdot r^5, 192$$

Luego $3 \cdot r^6 = 192$. De donde $r = 2$

Tenemos entonces que la progresión buscada es :

$$3, 6, 12, 24, 48, 96, 192$$

Ejercicio

Sume los $2n$ primeros términos de la progresión geométrica que comienza por: $3, -4, \frac{16}{3}$

Solución

$$r = \frac{-4}{3} = \frac{16}{3(-4)} \quad \text{Luego} \quad r = -\frac{4}{3}$$

$$s_{2n} = \frac{3\left(\left(-\frac{4}{3}\right)^{2n} - 1\right)}{-\frac{4}{3} - 1} = -\frac{9\left(\left(\frac{4}{3}\right)^{2n} - 1\right)}{7}$$

2.1.4 Sumas de cuadrados

Buscamos el valor de:

$$1^2 + 2^2 + 3^2 + \cdots + n^2$$

En efecto, sean

$$S_n(2) = \sum_{i=1}^n i^2 = 0^2 + 1^2 + 2^2 + \cdots + n^2$$

$$S_n(3) = \sum_{i=1}^n i^3 = 0^3 + 1^3 + 2^3 + \cdots + n^3$$

Se tiene

$$0^3 + 1^3 + 2^3 + \cdots + n^3 + (n+1)^3 = \sum_{i=0}^n (i+1)^3$$

Es decir

$$S_n(3) + (n+1)^3 = \sum_{i=0}^n (i+1)^3 \quad *$$

Pero

$$\begin{aligned} \sum_{i=0}^n (i+1)^3 &= \sum_{i=0}^n (i^3 + 3i^2 + 3i + 1) \\ &= \sum_{i=0}^n i^3 + \sum_{i=0}^n i^2 + \left(\sum_{i=0}^n i\right) + n + 1 \end{aligned}$$

Reemplazando en * se tiene:

$$S_n(3) + (n+1)^3 = S_n(3) + 3S_n(2) + \frac{3n(n+1)}{2} + n + 1$$

Luego

$$\begin{aligned} 3S_n(2) &= (n+1)^3 - \frac{3n(n+1)}{2} - n - 1 \\ S_n(2) &= \frac{2n^3 + 3n^2 + n}{6} \end{aligned}$$

De donde

$$S_n(2) = \frac{n(n+1)(2n+1)}{6}$$

2.2 Inducción o recurrencia

2.2.1 Los números naturales

Construcción según Peano

Existe un conjunto no vacío \mathbb{N} , cuyos elementos se llaman números naturales y a cada elemento m se le asocia un número $s(m)$, llamado el siguiente o el sucesor de m , sometidos a las siguientes condiciones, llamadas postulados de Peano, que son:

P.1. A cada número natural le corresponde un único número siguiente y cada número natural es a lo más el siguiente de un número natural.

P.2. Hay un número que no es el siguiente de ningún número, llamado primer elemento.

P.3. Sea $A \subset \mathbb{N}$ tal que:

- i) Hay $n_0 \in A$ con n_0 un número natural.
- ii) Todo elemento en A tiene su número siguiente en A

Entonces $A = \mathbb{N}$

El postulado 3 dice si un conjunto tiene un primer elemento y contiene todos los siguientes elementos dicho conjunto es \mathbb{N} . Este postulado es conocido como "Axioma de Inducción". Entonces vemos que este axioma está en la esencia de los números naturales.

El segundo postulado también lo cumple solamente el conjunto de los números naturales. Sin embargo el conjunto de los números enteros cumple el primer postulado.

Ejercicios Resueltos

1. (Suma de los cuadrados) Demostremos por inducción que:

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}; \forall n \in \mathbb{N}$$

Solución.

- (a) Para $n = 2$, tenemos:

Lado izquierdo: $1^2 + 2^2 = 5$

Lado derecho: $\frac{2 \cdot 3 \cdot 5}{6} = 5$

Luego cumple para $n = 2$

- (b) Supongamos que esta propiedad es válida para un cierto n , es decir, supongamos que

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

- (c) Por demostrar que esta propiedad es válida para el número siguiente, es decir para $n+1$. Queremos entonces demostrar que

$$1^2 + 2^2 + \cdots + n^2 + (n+1)^2 = \frac{(n+1)(n+2)(2n+3)}{6}$$

Demostración.

$$\begin{aligned} 1^2 + 2^2 + \cdots + (n+1)^2 &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ &= \frac{n(n+1)(2n+1) + 6(n+1)^2}{6} \\ &= \frac{(n+1)(2n^2 + n + 6n + 6)}{6} \\ &= \frac{(n+1)(n+2)(2n+3)}{6} \end{aligned}$$

Por (a), (b) y (c) esta propiedad es válida para todo número natural.

2. (Suma de los cubos) Demostremos por inducción que:

$$1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2; \forall n \in \mathbb{N}$$

Solución.

- (a) La comprobación para $n = 1$ es evidente.
 (b) Supongamosla válida para un cierto n . Es decir, supongamos que:

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

- (c) Por demostrar para el número siguiente, es decir, por demostrar que:

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

Demostración.

$$\begin{aligned}
 1^3 + \cdots + n^3 + (n+1)^3 &= (1+2+\cdots+n)^2 + (n+1)^3 \\
 &= \left(\frac{n(n+1)}{2}\right)^2 + (n+1)^3 \\
 &= \frac{(n+1)^2}{4}(n^2+4(n+1)) \\
 &= \frac{(n+1)^2}{4}(n+2)^2 \\
 &= \left(\frac{(n+1)(n+2)}{2}\right)^2 \\
 &= (1+2+\cdots+n+(n+1))^2
 \end{aligned}$$

3. (Suma de los números pares) Demostremos por inducción que:

$$2 + 4 + 6 + \cdots + 2n = n(n+1); \forall n \in \mathbb{N}$$

Solución.

- (a) Para $n = 1$ se verifica la igualdad.
 (b) Hipótesis de inducción:

$$2 + 4 + 6 + \cdots + 2n = n(n+1)$$

- (c) Por demostrar para $n+1$, es decir, por demostrar que :

$$2 + 4 + 6 + \cdots + 2n + 2(n+1) = (n+1)(n+2)$$

Demostración.

$$\begin{aligned}
 2 + 4 + 6 + \cdots + 2n + 2(n+1) &= n(n+1) + 2(n+1) \\
 &= (n+1)(n+2)
 \end{aligned}$$

Por (a), (b) y (c) se tiene que esta fórmula es verdadera para todo número natural n .

4. (Suma de los números impares) Demostremos por inducción que:

$$1 + 3 + 5 + \cdots + (2n-1) = n^2; \forall n \in \mathbb{N}$$

Solución.

- (a) Trivialmente se verifica la proposición para $n = 1$.
 (b) Hipótesis de inducción. Supongamos que es verdadera para un cierto n , es decir, supongamos que:

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2$$

- (c) Por demostrar que es válida para $n + 1$, es decir:

$$1 + 3 + 5 + \cdots + (2n - 1) + (2n + 1) = (n + 1)^2$$

Demostración.

$$\begin{aligned} 1 + 3 + 5 + \cdots + (2n - 1) + (2n + 1) &= n^2 + (2n + 1) \\ &= n^2 + 2n + 1 \\ &= (n + 1)^2 \end{aligned}$$

Por (a), (b) y (c) esta propiedad es verdadera para todo $n \in \mathbb{N}$.

5. (Suma de los múltiplos de 4) Demostremos por inducción que:

$$4 + 8 + 12 + \cdots + 4n = (2n)(n + 1); \forall n \in \mathbb{N}$$

Solución.

- (a) Demostremos que esta proposición es verdadera para $n = 2$
 Lado izquierdo: $4 + 8 = 12$. Lado derecho: $(2 \cdot 2)(3) = 12$.
 Luego es válido para $n = 2$
 (b) Hipótesis de inducción. Supongamos que es verdadera para un cierto n , es decir, supongamos que:

$$4 + 8 + 12 + \cdots + 4n = (2n)(n + 1)$$

- (c) Por demostrar que es verdadera para $n + 1$, es decir,

$$4 + 8 + 12 + \cdots + 4n + 4(n + 1) = 2(n + 1)(n + 2)$$

Demostración.

$$\begin{aligned} 4 + 8 + 12 + \cdots + 4n + 4(n + 1) &= 2n(n + 1) + 4(n + 1) \\ &= (n + 1) \cdot 2 \cdot (n + 2) \\ &= 2(n + 1)(n + 2) \end{aligned}$$

Por (a), (b) y (c) esta propiedad es verdadera para todo número natural.

6. Demostremos por inducción que:

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + n(n+1) = \frac{n(n+1)(n+2)}{3}; \forall n \in \mathbb{N}$$

Solución.

(a) Es claro que la proposición es verdadera para $n = 1$.

(b) Hipótesis de inducción. Supongamos que es verdadera para un cierto n , es decir, supongamos que:

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + n(n+1) = \frac{n(n+1)(n+2)}{3}$$

(c) Por demostrar que es verdadera para $n + 1$, es decir,

$$1 \cdot 2 + 2 \cdot 3 + \cdots + n(n+1) + (n+1)(n+2) = \frac{(n+1)(n+2)(n+3)}{3}$$

Demostración.

$$\begin{aligned} 1 \cdot 2 + \cdots + (n+1)(n+2) &= \frac{n(n+1)(n+2)}{3} + (n+1)(n+2) \\ &= \frac{n(n+1)(n+2) + 3(n+1)(n+2)}{3} \\ &= \frac{(n+1)(n+2)(n+3)}{3} \end{aligned}$$

Por (a), (b) y (c) esta proposición es válida para todo número natural

7. Demostremos por inducción que:

$$1 \cdot 3^1 + 2 \cdot 3^2 + 3 \cdot 3^3 + \cdots + n \cdot 3^n = \frac{(2n-1)3^{n+1} + 3}{4}; \forall n \in \mathbb{N}$$

Solución.

- (a) Demostremos que esta proposición es verdadera para $n = 2$

Lado izquierdo: $1 \cdot 3^1 + 2 \cdot 3^2 = 21$

Lado derecho: $\frac{(2 \cdot 2 - 1) \cdot 3^{2+1} + 3}{4} = 21$

Luego es válido para $n = 2$

- (b) Hipótesis de inducción. Supongamos que es verdadera para un cierto n , es decir, supongamos que:

$$1 \cdot 3^1 + 2 \cdot 3^2 + 3 \cdot 3^3 + \cdots + n \cdot 3^n = \frac{(2n - 1)3^{n+1} + 3}{4}$$

- (c) Por demostrar que esta proposición es verdadera para $n+1$, es decir, por demostrar que:

$$1 \cdot 3^1 + 2 \cdot 3^2 + 3 \cdot 3^3 + \cdots + n \cdot 3^n + (n+1) \cdot 3^{n+1} = \frac{(2n+1)3^{n+2} + 3}{4}$$

Demostración.

$$\begin{aligned} 1 \cdot 3^1 + \cdots + (n+1) \cdot 3^{n+1} &= \frac{(2n-1)3^{n+1} + 3}{4} + (n+1)3^{n+1} \\ &= \frac{3^{n+1}((2n-1) + 4(n+1)) + 3}{4} \\ &= \frac{3^{n+1}(6n+3) + 3}{4} \\ &= \frac{3^{n+1} \cdot 3(2n+1) + 3}{4} \\ &= \frac{3^{n+2}(2n+1) + 3}{4} \end{aligned}$$

Por (a), (b) y (c) se tiene que esta propiedad es verdadera para todo número natural n .

8. (Suma de las potencias de $\frac{1}{2}$.) Demostremos por inducción que:

$$\frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots + \frac{1}{2^n} = 1 - \frac{1}{2^n}; \forall n \in \mathbb{N}$$

Solución.

(a) Demostremos que esta proposición es verdadera para $n = 3$

$$\text{Lado izquierdo: } \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} = \frac{7}{8},$$

$$\text{Lado derecho: } 1 - \frac{1}{2^3} = \frac{7}{8}.$$

Luego es válido para $n = 3$

(b) Hipótesis de inducción. Supongamos que es verdadera para un cierto n , es decir, supongamos que:

$$\frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots + \frac{1}{2^n} = 1 - \frac{1}{2^n}$$

(c) Por demostrar que es verdadero para $n + 1$, es decir, por demostrar que:

$$\frac{1}{2} + \frac{1}{2^2} + \cdots + \frac{1}{2^n} + \frac{1}{2^{n+1}} = 1 - \frac{1}{2^{n+1}}$$

Demostración.

$$\begin{aligned} \frac{1}{2} + \cdots + \frac{1}{2^n} + \frac{1}{2^{n+1}} &= \left(1 - \frac{1}{2^n}\right) + \frac{1}{2^{n+1}} \\ &= 1 + \frac{-2 + 1}{2^{n+1}} \\ &= 1 - \frac{1}{2^{n+1}} \end{aligned}$$

Por (a), (b) y (c), se tiene que esta propiedad es verdadera para todo número natural n .

9. Demostremos por inducción que:

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}; \forall n \in \mathbb{N}$$

Solución.

(a) Para $n = 2$ es fácil ver que la proposición es verdadera.

(b) Hipótesis de inducción. Supongamos que es verdadera para un cierto n , es decir, supongamos que:

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$$

- (c) Por demostrar que es verdadero para $n + 1$, es decir, por demostrar que:

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{n(n+1)} + \frac{1}{(n+1)(n+2)} = \frac{n+1}{n+2}$$

Demostración.

$$\begin{aligned} \frac{1}{1 \cdot 2} + \cdots + \frac{1}{n(n+1)} + \frac{1}{(n+1)(n+2)} &= \frac{n}{n+1} + \frac{1}{(n+1)(n+2)} \\ &= \frac{n(n+2) + 1}{(n+1)(n+2)} \\ &= \frac{n^2 + 2n + 1}{(n+1)(n+2)} \\ &= \frac{n+1}{n+2} \end{aligned}$$

Por (a), (b) y (c) se tiene que esta propiedad es verdadera para todo número natural n .

10. Demostremos por inducción que:

$$\frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \cdots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}; \forall n \in \mathbb{N}$$

Solución.

- (a) Demostremos que esta proposición es verdadera para $n = 2$

Lado izquierdo: $\frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} = \frac{2}{5},$

Lado derecho: $\frac{2}{5}.$

Luego es válido para $n = 2$

- (b) Hipótesis de inducción. Supongamos que es verdadera para un cierto n , es decir, supongamos que:

$$\frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \cdots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}$$

- (c) Por demostrar que es verdadero para $n + 1$, es decir, por demostrar que:

$$\frac{1}{1 \cdot 3} + \cdots + \frac{1}{(2n-1)(2n+1)} + \frac{1}{(2n+1)(2n+3)} = \frac{n+1}{2n+3}$$

Demostración.

$$\begin{aligned} \frac{1}{1 \cdot 3} + \cdots + \frac{1}{(2n-1)(2n+1)} + \frac{1}{(2n+1)(2n+3)} &= \frac{n}{2n+1} + \frac{1}{(2n+1)(2n+3)} \\ &= \frac{2n^2+3n+1}{(2n+1)(2n+3)} \\ &= \frac{(2n+1)(n+1)}{(2n+1)(2n+3)} \\ &= \frac{n+1}{2n+3} \end{aligned}$$

Por (a), (b) y (c) se tiene que esta propiedad es verdadera para todo número natural n .

2.3 Ejercicios Propuestos

1. Pruebe por recurrencia para todo $n \in \mathbb{N}$.

$$1^4 + 2^4 + 3^4 + \cdots + n^4 = \frac{1}{30}n(n+1)(2n+1)(3n^2+3n-1)$$

2. Pruebe por recurrencia para todo $n \in \mathbb{N}$.

$$(a) \sum_{k=1}^n (2k-1)^2 = \frac{1}{3}n(4n^2-1)$$

$$(b) \sum_{k=1}^n k \cdot k! = (n+1)! - 1$$

(Comience por escribir las sumas del lado izquierdo de las igualdades como las expresiones del ejercicio 1.)

3. Muestre que no es cierto que

$$\left(\sum_{k=1}^n a_k \right) \cdot \left(\sum_{k=1}^n b_k \right) = \sum_{k=1}^n a_k \cdot b_k$$

(basta dar un contraejemplo)

4. Calcule las siguientes sumas (utilice las propiedades conocidas):

(a) $\sum_{k=1}^n (6k - 5)$

(b) $\sum_{k=1}^n k(k + 1)$

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

Pruebe por recurrencia las fórmulas que usted encontró.

5. Pruebe por recurrencia las proposiciones siguientes.

(a) La suma de los ángulos en un polígono convexo de n lados es $(n - 2)\pi$.

(b) Un polígono convexo de n lados posee $\frac{n(n-3)}{2}$ diagonales.

6. (a) Encuentre $k \in \mathbb{N}$ tal que $n^3 > 3n^2 + 3n + 1$, para todo $n \geq k$.

(b) Encuentre $k \in \mathbb{N}$ tal que $2^n > n^3$, para todo $n \geq k$.

7. Demuestre por recurrencia que en un conjunto de n elementos ($n \geq 3$) hay

(a) $\frac{n(n-1)}{2!}$ sub-conjuntos de 2 elementos.

(b) $\frac{n(n-1)(n-2)}{3!}$ sub-conjuntos de 3 elementos.

(c) 2^n sub-conjuntos arbitrarios.

8. Demuestre por recurrencia.

(a) $1 + q + q^2 + \cdots + q^n = \frac{1 - q^{n+1}}{1 - q}$

(b) $a^n + a^{n-1}b + a^{n-2}b^2 + \cdots + ab^{n-1} + b^n = \frac{a^{n+1} - b^{n+1}}{a - b}$

Nota: Se puede deducir (b) de (a) poniendo $q = \frac{b}{a}$.

9. (a) Considere la sucesión (a_n) dada por

$$a_0 = 2, \ a_1 = 5, \ a_{n+2} = 5a_{n+1} - 6a_n$$

Pruebe que para todo n se tiene $a_n = 2^n + 3^n$.

- (b) Considere la sucesión (a_n) dada por

$$a_0 = 2, \ a_1 = 3, \ a_{n+1} = 3a_n - 2a_{n-1}$$

Pruebe que para todo n se tiene $a_n = 2^n + 1$.

Capítulo 3

Binomio de Newton

El objetivo de este capítulo es llegar a conocer la ley del desarrollo de binomios tales como $(a + b)^{10}$, $(a^3 - \frac{2b}{5a})^{35}$, $(a + b)^n$, donde n es un número natural.

3.1 Factorial

En este capítulo será muy común tener que multiplicar cantidades como $1 \cdot 2 \cdot 3 \cdot 4$ o bien $7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12$. Entonces se inventó una abreviación para tales operaciones. Así, $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$, será abreviado $5!$ y diremos "5 factorial"

la abreviación $7!$, denotará $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7$.

Tenemos entonces la definición siguiente:

Definición 3.1.1 Si $n \in \mathbb{N}$, $n \geq 1$, se define el **factorial de n** por

$$n! = 1 \cdot 2 \cdot 3 \cdots n$$

y diremos n **factorial**.

Observación. De acuerdo a la definición anterior, $0!$ no tiene sentido, sin embargo, para que otras definiciones que veremos más adelante,

se puedan extender al caso del 0, las cuales sí tienen sentido, será necesario definir $0!$.

Definición 3.1.2 $0! = 1$

Ejemplos.

$$\begin{aligned}\frac{6!}{5!} &= \frac{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5} = 6 \\ \frac{5!}{3!} &= \frac{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5}{1 \cdot 2 \cdot 3} = 4 \cdot 5 \\ \frac{10!}{6!} &= \frac{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6} = 7 \cdot 8 \cdot 9 \cdot 10 \\ \frac{(n+1)!}{n!} &= \frac{1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n \cdot (n+1)}{1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n} = n+1 \\ \frac{(n+2)!}{n!} &= (n+1)(n+2) \\ \frac{n!}{(n-3)!} &= (n-2)(n-1) \cdot n \\ \frac{(n+2)!}{(n-2)!} &= (n-1) \cdot n \cdot (n+1) \cdot (n+2) \\ \frac{(n-k)!}{(n-k-1)!} &= n-k\end{aligned}$$

Ejercicio. Expresemos con factoriales la suma de fracciones siguiente:

$$\begin{aligned}1) \quad \frac{5!}{2! \cdot 3!} + \frac{5!}{1! \cdot 4!} &= \frac{5! \cdot 4 + 5! \cdot 2}{\frac{2! \cdot 4!}{5! \cdot (4+2)}} \\ &= \frac{2! \cdot 4!}{6!} \\ &= \frac{2! \cdot 4!}{8! \cdot 4 + 8! \cdot 5} \\ 2) \quad \frac{8!}{5! \cdot 3!} + \frac{8!}{4! \cdot 4!} &= \frac{8! \cdot \frac{5! \cdot 4!}{8! \cdot (4+5)}}{\frac{5! \cdot 4!}{9d!}} \\ &= \frac{5! \cdot 4!}{5! \cdot 4!}\end{aligned}$$

3.2 Número combinatorio

En esta sección estaremos preocupados de problemas tales como:

”En un teatro hay sólo tres asientos libres, desde los cuales la visión es completamente diferente. Estamos interesados en saber de cuántas maneras se pueden sentar 3 personas, tomadas de un grupo de 7 personas que quieren ocupar estos asientos”.

Otro problema:

”Hay 7 personas y solamente 3 de ellas podrán ir a un paseo. ¿Cuántas formas diferentes de grupos de 3 personas se pueden formar a partir de estas 7 personas?”

Problema. Sea X un conjunto formado por 7 personas. Hay 3 asientos en un teatro en los cuales hay una visión muy diferentes en cada uno de ellos. Denotemos estos asientos por:

$$A \quad B \quad C$$

¿Cuántas son las formas posibles de ocupar estos 3 asientos, tomadas de un grupo de 7 personas?

Solución. Para el asiento A hay 7 posibilidades. Cada vez que hay una persona en el asiento A , quedan 6 posibilidades para el asiento B . Luego si tenemos el asiento A y B , hay $7 \cdot 6$ posibilidades para ocuparlos.

Cada vez que hay una persona en el asiento A y una en el asiento B , hay 5 posibilidades para el asiento C . Luego si tenemos los asientos A , B y C hay

$$7 \cdot 6 \cdot 5$$

posibilidades para ocuparlos, tomados de un grupo de 7 personas.

Problema. ¿Cuántas maneras diferentes tienen para sentarse 3 personas, en 3 asientos en un teatro?

Solución. Consideremos 3 asientos:

$$A \quad B \quad C$$

Para el asiento A hay 3 posibilidades. Cada vez que hay una persona en el asiento A , hay 2 posibilidades para el asiento B .

Si hay una persona sentada en el asiento A y otra en el asiento B , hay sólo una posibilidad para el asiento C . Luego hay

$$3 \cdot 2 \cdot 1 = 3!$$

formas diferentes de sentarse 3 personas en 3 asientos diferentes.

Problema. En un teatro hay 7 personas. Queremos saber cuántos grupos diferentes, formados de 3 personas, se pueden formar, para que se paseen por el escenario.

Solución. Primero pensemos que hay 3 asientos, luego hay $7 \cdot 6 \cdot 5$ maneras de ocuparlos. Si ahora hacemos pasear esas personas en el escenario, ocurre que cada vez que consideramos 3 personas, éstas han estado sentadas de $3!$ maneras diferentes. Luego si hay 7 personas hay:

$$\frac{7 \cdot 6 \cdot 5}{3!}$$

maneras diferentes que se pasee un grupo de 3 de ellas en el escenario. Esta es la respuesta.

Ahora queremos escribir de manera más elegante este resultado:

$$\frac{7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{(4 \cdot 3 \cdot 2 \cdot 1) \cdot 3!} = \frac{7!}{4! \cdot 3!} =: \binom{7}{3}$$

Nota. No dice: $\left(\frac{7}{3}\right)$, ni tampoco $\frac{7}{3}$.

$\binom{7}{3}$ es llamado el número combinatorio de 7 sobre 3. Es usado para denotar todas las combinaciones que se pueden hacer de 3 elementos tomados de un grupo formado por 7 elementos.

Problema. Tenemos un conjunto X formado por n elementos. Queremos saber cuántos subconjuntos de X , de k ($k \leq n$) elementos podemos formar.

Solución. Si estos k elementos los ponemos en un cierto orden y respetamos los lugares, entonces hay:

$$n \cdot (n-1) \cdots ((n-k)+1)$$

de ponerlos respetando los lugares.

Puesto que son subconjuntos formados por k elementos, debemos entonces dividir por $k!$, los k elementos estaban de $k!$ maneras diferentes puestos en estos lugares. Luego hay

$$\frac{n \cdot (n-1) \cdots ((n-k)+1)}{k!}$$

subconjuntos de k elementos tomados de un conjunto de n elementos.

Si queremos escribirlo de un manera más elegante tenemos:

$$\frac{n \cdot (n-1) \cdots ((n-k)+1) \cdot (n-k) \cdots 2 \cdot 1}{((n-k) \cdots 2 \cdot 1) \cdot k!} = \frac{n!}{(n-k)! \cdot k!}$$

Nota. $\binom{n}{k}$ denotará el número de combinaciones posibles de k elementos, tomados de un conjunto de n elementos. Diremos que $\binom{n}{k}$ es el número combinatorio de n sobre k .

Proposición 3.2.1 Sean $n, k \in \mathbb{N}, n \geq k$, entonces se tiene

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

Esto ha sido demostrado anteriormente.

Nota. Queremos que sepas que este número tiene propiedades muy hermosas que iremos descubriendo a partir de ejercicios. Es por esto que te invitamos a no saltarte ejercicios. Como te explicamos, nos ayudarán a descubrir leyes que ellos cumplen.

Ejercicio.

$$\begin{aligned} \binom{3}{0} &= \frac{3!}{3! \cdot 0!} = 1 & ; & \quad \binom{3}{1} = \frac{3!}{2! \cdot 1!} = 3 & ; & \quad \binom{3}{2} = \frac{3!}{1! \cdot 2!} = 3 \\ \binom{3}{3} &= \frac{3!}{0! \cdot 3!} = 1 & ; & \quad \binom{2}{0} = \frac{2!}{2! \cdot 0!} = 1 & ; & \quad \binom{2}{1} = \frac{2!}{1! \cdot 1!} = 2 \\ \binom{2}{2} &= \frac{2!}{0! \cdot 2!} = 1 & ; & \quad \binom{1}{0} = \frac{1!}{1! \cdot 0!} = 1 & ; & \quad \binom{1}{1} = \frac{1!}{0! \cdot 1!} = 1 \end{aligned}$$

Además

$$\binom{0}{0} = \frac{0!}{0! \cdot 0!} = 1$$

Nota. Famoso es el triángulo de Pascal el cual lleva el nombre del matemático y filósofo Blaise Pascal(1.623-1.662)

3.2.1 Triángulo de Pascal

$$\begin{array}{ccccccc}
 n = 0 & & & & \binom{0}{0} & & \\
 n = 1 & & & \binom{1}{0} & & \binom{1}{1} & \\
 n = 2 & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} \\
 n = 3 & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & \binom{3}{3}
 \end{array}$$

Haciendo los cálculos, éstos números son los siguientes:

$$\begin{array}{ccccccc}
 & & & & 1 & & & & \\
 & & & & 1 & & 1 & & \\
 & & & 1 & & 2 & & 1 & \\
 & & 1 & & 3 & & 3 & & 1 \\
 & 1 & & 4 & & 6 & & 4 & & 1 \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
 & 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 \\
 1 & & 1 & & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & & 1
 \end{array}$$

Al mirar estos números, uno descubre leyes muy curiosas, admirables. Realmente fue un chispazo genial el de Pascal el ordenar en esta forma éstos números.

Propiedades del triángulo de Pascal

La primera propiedad que salta a la vista, es que en los bordes tenemos solamente 1. Esto se expresa como sigue:

Propiedad 1. $\binom{n}{0} = 1$; $\binom{n}{n} = 1$

Demostración. $\binom{n}{0} = \frac{n!}{n! \cdot 0!} = 1$; $\binom{n}{n} = \frac{n!}{0! \cdot n!} = 1$ ¡Trivial! ¿cierto?

Observación. Observa que este triángulo es simétrico. Por ejemplo la fila de $n = 6$ es:

$$1 \quad 6 \quad 15 \quad 20 \quad 15 \quad 6 \quad 1$$

Algo así como "los números se devuelven"

Para la fila de $n = 7$, tenemos

$$1 \quad 7 \quad 21 \quad 35 \quad \text{y luego} \quad 35 \quad 21 \quad 7 \quad 1$$

Ahora es necesario escribir esto mediante una expresión algebraica.

Con respecto a las filas de $n = 6$ y $n = 7$, tenemos:

$$\begin{aligned} \binom{6}{0} &= \binom{6}{6}; & \binom{6}{1} &= \binom{6}{5}; & \binom{6}{2} &= \binom{6}{4}; \\ \binom{7}{0} &= \binom{7}{7}; & \binom{7}{1} &= \binom{7}{6}; & \binom{7}{2} &= \binom{7}{5}; & \binom{7}{3} &= \binom{7}{4} \end{aligned}$$

¿Cuál es entonces la ley que cumplen?

Propiedad 2. Sean $n, k \in \mathbb{N}, n \geq k$, entonces se tiene

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

Demostración.

$$\begin{aligned} \binom{n}{n-k} &= \frac{n!}{(n-(n-k))!(n-k)!} \\ &= \frac{n!}{k!(n-k)!} \\ &= \frac{n!}{(n-k)!k!} \\ &= \binom{n}{k} \end{aligned}$$

Observación. Observa que en una misma fila, la suma de 2 números seguidos tiene su resultado en la fila siguiente, justo al medio de los dos números dados.

Por ejemplo:

$$\begin{array}{ccccc} 6 & 4 & \text{es decir} & \binom{4}{2} & \binom{4}{3} \\ & & & & \binom{5}{3} \\ & 10 & & & \end{array}$$

Veamos que esto ocurre efectivamente:

$$\begin{aligned}
 \binom{4}{2} + \binom{4}{3} &= \frac{4!}{2! \cdot 2!} + \frac{4!}{1! \cdot 3!} \\
 &= \frac{4! \cdot 3 + 4! \cdot 2}{4! \cdot 3 + 4! \cdot 2} \\
 &= \frac{2!3!}{4! \cdot (3+2)} \\
 &= \frac{2! \cdot 3!}{5!} \\
 &= \frac{2! \cdot 3!}{5!} \\
 &= \binom{5}{3}
 \end{aligned}$$

Pero esto que nos "parece" verdadero, obviamente debemos demostrarlo. Entonces:

Propiedad 3. Sean $n, k \in \mathbb{N}, n \geq k$, entonces se tiene

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

Demostración.

$$\begin{aligned}
 \binom{n}{k} + \binom{n}{k-1} &= \frac{n!}{(n-k)!k!} + \frac{n!}{(n-(k-1))!(k-1)!} \\
 &= \frac{n!(n-k+1) + n!k}{n!(n-k+1) + n!k} \\
 &= \frac{(n-k+1)!k!}{n!(n-k+1+k)} \\
 &= \frac{(n+1-k)!k!}{n!(n+1)} \\
 &= \frac{((n+1)-k)!k!}{(n+1)!} \\
 &= \frac{((n+1)-k)!k!}{((n+1)-k)!k!} \\
 &= \binom{n+1}{k}
 \end{aligned}$$

Observación. La suma de dos elementos seguidos de una fila, da un elemento de la fila siguiente. Tenemos por ejemplo:

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

o bien:

$$\binom{n+1}{\cdot} + \binom{n+1}{\cdot} = \binom{n+2}{\cdot}$$

o bien:

$$\binom{n-2}{\cdot} + \binom{n-2}{\cdot} = \binom{n-1}{\cdot}$$

etc.

Observación. El número obtenido de la suma de dos números combinatorios consecutivos de una fila, corresponde al número combinatorio ubicado en la siguiente fila entre ambos números dados. Luego, el número de abajo en el número combinatorio obtenido de la suma, corresponde al mayor de los dos números dados. Tenemos:

$$\binom{\cdot}{k} + \binom{\cdot}{k+1} = \binom{\cdot}{k+1}$$

o bien

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

Observación. Esta propiedad se puede escribir de infinitas maneras. Como por ejemplo

$$\binom{n-1}{k-3} + \binom{n-1}{k-2} = \binom{n}{k-2}, \quad \text{con } k-3 \leq n-1$$

$$\binom{n-3}{k+5} + \binom{n-3}{k+6} = \binom{n-2}{k+6} \quad \text{con } k+5 \leq n-3$$

Estas son las tres propiedades más conocidas del triángulo de Pascal.

Ejemplo.

$$\binom{25}{4} + \binom{25}{5} = \binom{26}{5}$$

Observación. En el triángulo de Pascal, si dejamos fijo $k = 2$ y hacemos variar $n = 2, 3, 4, 5, 6$ y sumamos, tenemos:

$$\binom{2}{2} + \binom{3}{2} + \binom{4}{2} + \binom{5}{2} + \binom{6}{2} = \binom{7}{3}$$

Es decir,

$$\sum_{i=2}^6 \binom{i}{2} = \binom{7}{3}$$

Observe que esto corresponde a la suma de los elementos de una parte de la diagonal para $k = 2$. Tenemos la siguiente propiedad a modo de ejercicio.

Ejercicio. Dado $n \in \mathbb{N}$, entonces se tiene

$$\sum_{i=2}^n \binom{i}{2} = \binom{n+1}{3}$$

En efecto, la demostración la haremos por inducción sobre n .

1. Para $n = 1$ tenemos: Lado izquierdo: 1; Lado derecho: 1. Luego es válido para $n = 1$.
2. Hipótesis de inducción. Supongamos que esta propiedad es verdadera para n .
3. Por demostrar que es verdadera para $n + 1$, es decir, por demostrar que:

$$\sum_{i=2}^{n+1} \binom{i}{2} = \binom{n+2}{3}$$

En efecto

$$\begin{aligned} \sum_{i=2}^{n+1} \binom{i}{2} &= \sum_{i=2}^n \binom{i}{2} + \binom{n+1}{2} \\ &= \binom{n+1}{3} + \binom{n+1}{2} \\ &= \binom{n+2}{3} \end{aligned}$$

Por (1), (2) y (3) esta propiedad es verdadera para todo número natural $n \in \mathbb{N}$.

Otras propiedades

$$\sum_{i=3}^n \binom{i}{3} = \binom{n+1}{4}$$

O bien

$$\sum_{i=4}^n \binom{i}{4} = \binom{n+1}{5}$$

En general tenemos la proposición siguiente a modo de ejercicio.

Ejercicio. Demuestre que para $n \in \mathbb{N}$ se tiene

$$\sum_{i=k}^n \binom{i}{k} = \binom{n+1}{k+1}$$

Observación. Veamos de qué manera en una fila podemos obtener el número siguiente hacia la derecha.

Por ejemplo: como pasar del 6 al 4, o del 10 al 5, o del 20 al 15.

Ejemplo. Como pasar del 6 al 4.

$$\binom{4}{2} \cdot \frac{2}{3} = \binom{4}{3}$$

Ejemplo. Como pasar del 10 al 5.

$$\binom{5}{3} \cdot \frac{2}{4} = \binom{5}{4}$$

Ejemplo. Como pasar del 20 al 15.

$$\binom{6}{3} \cdot \frac{3}{4} = \binom{6}{4}$$

Ejercicio Resueltos.

1. Demostremos que:

$$\binom{m}{n} \cdot \frac{m-n}{n+1} = \binom{m}{n+1}$$

(Cómo avanzar un lugar hacia la derecha en una fila cualquiera.)

Solución.

$$\begin{aligned}
 \binom{m}{n} \cdot \frac{m-n}{n+1} &= \frac{m-n}{n+1} \cdot \frac{m!}{(m-n)!n!} \\
 &= \frac{m-n}{n+1} \cdot \frac{m!}{(m-n-1)! \cdot (m-n) \cdot n!} \\
 &= \frac{m!}{(n+1) \cdot n! (m-(n+1))!} \\
 &= \frac{m!}{(n+1)! (m-(n+1))!} \\
 &= \binom{m}{n+1}
 \end{aligned}$$

2. Determinemos n tal que:

$$3 \cdot \binom{n}{4} = 5 \cdot \binom{n-1}{5}$$

Solución.

$$3 \cdot \frac{n!}{(n-4)!4!} = 5 \cdot \frac{(n-1)!}{(n-1-5)!5!}$$

Luego, se tiene:

$$\frac{3(n-3)(n-2)(n-1)n}{1 \cdot 2 \cdot 3 \cdot 4} = \frac{(n-5)(n-4)(n-3)(n-2)(n-1)}{4!}$$

De donde

$$3n = (n-5)(n-4)$$

Luego $n^2 - 12n + 20 = 0$. Luego $(n-2)(n-10) = 0$.

Las soluciones son entonces: $n = 2$ y $n = 10$. Pero $n = 2$ no tiene sentido. Luego hay una sola solución y esta es $n = 10$

3. Demostremos que

$$\binom{6}{4} + 2 \binom{6}{3} + \binom{6}{2} = \binom{8}{4}$$

Solución.

$$\begin{aligned}\binom{6}{4} + 2\binom{6}{3} + \binom{6}{2} &= (\binom{6}{4} + \binom{6}{3}) + (\binom{6}{3} + \binom{6}{2}) \\ &= \binom{7}{4} + \binom{7}{3} \\ &= \binom{8}{4}\end{aligned}$$

4. Simplifiquemos la expresión

$$\frac{n! - (n-1)!}{(n-1)!}$$

Solución.

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

5. Simplifiquemos

$$\frac{n! - (n+1)! + (n-2)!}{(n-2)!}$$

Solución.

$$\begin{aligned}\frac{n! - (n+1)! + (n-2)!}{(n-2)!} &= (n-1) \cdot n - (n-1) \cdot n \cdot (n+1) + 1 \\ &= n^2 - n - (n^3 - n) + 1 \\ &= -n^3 + n^2 + 1\end{aligned}$$

6. Calculemos el valor de n en las siguientes relaciones

$$\begin{aligned}(1) \quad \binom{n}{3} &= \binom{n}{4} \\ (2) \quad \binom{n+1}{3} &= 2\binom{n}{2}\end{aligned}$$

Solución de (1) Se tiene: $n - 4 = 3$, luego $n = 7$

Solución de (2)

$$\frac{(n+1)!}{(n+1-3)!3!} = 2 \cdot \frac{n!}{(n-2)!2!}$$

Luego

$$\frac{n!(n+1)}{(n-2)!3!} = \frac{n!}{(n-2)!}$$

De donde $n+1=6$, es decir $n=5$

7. Demostremos que:

$$\binom{n}{k} \cdot \frac{n+1}{k+1} = \binom{n+1}{k+1}$$

Solución.

$$\begin{aligned} \binom{n}{k} \cdot \frac{n+1}{k+1} &= \frac{n!}{(n-k)!k!} \cdot \frac{n+1}{k+1} \\ &= \frac{(n+1)!}{(n+1-(k+1))!(k+1)!} \\ &= \binom{n+1}{k+1} \end{aligned}$$

3.3 Desarrollo del binomio

Nota. Ahora tenemos los elementos necesarios para calcular binomios de la forma:

$$(x+y)^n$$

donde n es un número natural.

Problema. Desarrollemos el binomio

$$(x+y)^7$$

Solución.

$$(x+y)^7 = (x+y)(x+y)(x+y)(x+y)(x+y)(x+y)(x+y)$$

El primer término del desarrollo es x^7 .

El segundo término queremos que tenga la forma x^6y . ¿Cuántos x^6y hay? y ¿Por qué?. De las 7 y que hay, queremos saber todas las posibilidades de tomar una sola.

1. Del primer binomio tomamos "y" y de los 6 restantes tomamos "x".
2. Del segundo binomio tomamos "y" y de los 6 restantes tomamos "x", etc.

Tenemos $\binom{7}{1}$ combinaciones posibles. Luego el segundo sumando es $\binom{7}{1} x^6 y$.

El tercer término queremos que tenga la expresión " $x^5 y^2$ ". El tercer sumando tiene la forma $\binom{7}{2} x^5 y^2$, etc.

Luego el desarrollo del binomio es:

$$\begin{aligned} (x+y)^7 = & \binom{7}{0} x^7 y^0 + \binom{7}{1} x^6 y^1 + \binom{7}{2} x^5 y^2 + \binom{7}{3} x^4 y^3 + \binom{7}{4} x^3 y^4 \\ & + \binom{7}{5} x^2 y^5 + \binom{7}{6} x^1 y^6 + \binom{7}{7} x^0 y^7 \end{aligned}$$

Este genial descubrimiento fue hecho por el físico y matemático Isaac Newton (1642-1727)

Teorema 3.3.1 (Binomio de Newton) Sean $x, y \in \mathbb{R}$ y $n \in \mathbb{N}$, entonces se tiene:

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

Demostración. Por inducción sobre n.

1. Para $n = 2$ tenemos:

$$\begin{aligned} (x+y)^2 &= (x+y) \cdot (x+y) \\ &= x^2 + xy + xy + y^2 \\ &= x^2 + 2xy + y^2 \\ &= \binom{2}{0} x^2 y^0 + \binom{2}{1} xy + \binom{2}{2} x^0 y^2 \end{aligned}$$

2. Hipótesis de inducción. Supongamos que:

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

3. Por demostrar que:

$$(x + y)^{n+1} = \binom{n+1}{0} x^{n+1} y^0 + \binom{n+1}{1} x^n y^1 + \cdots + \binom{n+1}{n+1} x^0 y^{n+1}$$

Demostración. (Las explicaciones están al final)

$$\begin{aligned} (x + y)^{n+1} &= (x + y)^n (x + y) \\ &= \binom{n}{0} x^{n+1} y^0 + \binom{n}{1} x^n y^1 + \cdots + \binom{n}{n} x^1 y^n + \\ &\quad + \binom{n}{0} x^n y^1 + \binom{n}{1} x^{n-1} y^2 + \cdots + \binom{n}{n} x^0 y^{n+1} \\ &= \binom{n}{0} x^{n+1} y^0 + \left(\binom{n}{1} + \binom{n}{0} \right) x^n y^1 + \cdots + \\ &\quad + \left(\binom{n}{n} + \binom{n}{n-1} \right) x^1 y^n + \binom{n}{n} x^0 y^{n+1} \\ &= \binom{n+1}{0} x^{n+1} y^0 + \binom{n+1}{1} x^n y^1 + \cdots + \\ &\quad + \binom{n+1}{n} x^1 y^n + \binom{n+1}{n+1} x^0 y^{n+1} \end{aligned}$$

Nota. En la segunda igualdad, multiplicamos la expresión $(x + y)^n$ por x y le sumamos la expresión $(x + y)^n$, multiplicada por y .

En la tercera igualdad factorizamos $x^n y^1$, luego $x^{n-1} y^2, \dots, x^1 y^n$, es decir sumamos los términos semejantes.

En la cuarta igualdad usamos las tres propiedades más importantes del Triángulo de Pascal.

Por (1), (2) y (3), esta propiedad es verdadera para todo número natural.

Notación

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

Ejemplo de notación

$$\begin{aligned}
 \left(\frac{2}{3}a^4 - \frac{1}{5}ab^7\right)^{30} &= \left(\frac{2}{3}a^4 + (-1)\frac{1}{5}ab^7\right)^{30} \\
 &= \sum_{k=0}^{30} \binom{30}{k} \left(\frac{2}{3}a^4\right)^{30-k} \cdot \left((-1)\frac{1}{5}ab^7\right)^k
 \end{aligned}$$

Corolario 3.3.2 Sea $n \in \mathbb{N}$, entonces $\sum_{k=0}^n \binom{n}{k} = 2^n$

Demostración. Tomemos $x = y = 1$. Entonces

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

Corolario 3.3.3 Sea $n \in \mathbb{N}$, entonces $\sum_{k=0}^n (-1)^k \binom{n}{k} = 0$

Demostración. En el teorema tomemos $x = 1$, $y = -1$. Entonces:

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

Observación. En el Triángulo de Pascal, observemos, en la línea correspondiente a $n = 5$, que la suma para los impares, coincide con la suma de los k pares. Así $5 + 10 + 1 = 1 + 10 + 5$.

Para $n = 6$, la suma de los k impares es $6 + 20 + 6$ y la suma de los k pares es: $1 + 15 + 15 + 1$.

Entonces uno se pregunta si esto es una coincidencia o si bien ocurre para todo n . Esta hipótesis tiene su respuesta en la propiedad siguiente:

Propiedad del Triángulo de Pascal Sea $n \in \mathbb{N}$, entonces

$$\sum_{j, \text{par}}^n \binom{n}{j} = \sum_{j, \text{impar}}^n \binom{n}{j}$$

Demostración.

$$\begin{aligned}
\sum_{j, \text{par}}^n \binom{n}{j} - \sum_{j, \text{impar}}^n \binom{n}{j} &= \sum_{j, \text{par}}^n \binom{n}{j} (1)^{n-j} (-1)^j \\
&+ \sum_{j, \text{impar}}^n \binom{n}{j} (1)^{n-j} (-1)^j \\
&= \sum_{j=0}^n \binom{n}{j} (1)^{n-j} (-1)^j \\
&= (1 + (-1))^n \\
&= 0
\end{aligned}$$

Nota Hemos utilizado el Teorema del Binomio de Newton, el cual es válido para todo número natural, luego éste corolario es válido para todo n , número natural.

Ejercicios Resueltos

1. Escribamos el desarrollo del binomio

$$(x^{\frac{2}{3}} - y^{\frac{2}{3}})^6$$

Solución.

$$\begin{aligned}
(x^{\frac{2}{3}} - y^{\frac{2}{3}})^6 &= \binom{6}{0} (x^{\frac{2}{3}})^{6-0} (-y^{\frac{2}{3}})^0 + \binom{6}{1} (x^{\frac{2}{3}})^{6-1} (-y^{\frac{2}{3}})^1 \\
&+ \binom{6}{2} (x^{\frac{2}{3}})^{6-2} (-y^{\frac{2}{3}})^2 + \binom{6}{3} (x^{\frac{2}{3}})^{6-3} (-y^{\frac{2}{3}})^3 \\
&+ \binom{6}{4} (x^{\frac{2}{3}})^{6-4} (-y^{\frac{2}{3}})^4 + \binom{6}{5} (x^{\frac{2}{3}})^{6-5} (-y^{\frac{2}{3}})^5 \\
&+ \binom{6}{6} (x^{\frac{2}{3}})^{6-6} (-y^{\frac{2}{3}})^6 \\
&= 1 \cdot x^{\frac{12}{3}} - 6 \cdot x^{\frac{10}{3}} \cdot y^{\frac{2}{3}} + 3 \cdot 5 \cdot x^{\frac{8}{3}} y^{\frac{4}{3}} - 4 \cdot 5 x^{\frac{6}{3}} y^{\frac{6}{3}} \\
&+ 15 x^{\frac{4}{3}} y^{\frac{8}{3}} - 6 x^{\frac{2}{3}} y^{\frac{10}{3}} + y^{\frac{12}{3}} \\
&= x^4 - 6 x^{\frac{10}{3}} y^{\frac{2}{3}} + 15 x^{\frac{8}{3}} y^{\frac{4}{3}} - 20 x^2 y^2 + 15 x^{\frac{4}{3}} y^{\frac{8}{3}} \\
&- 6 x^{\frac{2}{3}} y^{\frac{10}{3}} + y^4
\end{aligned}$$

2. Hagamos el desarrollo del binomio

$$(2a - 3y)^5$$

Solución.

$$\begin{aligned}
 (2a - 3y)^5 &= \binom{5}{0} (2a)^{5-0} (-3y)^0 + \binom{5}{1} (2a)^{5-1} (-3y)^1 \\
 &\quad + \binom{5}{2} (2a)^{5-2} (-3y)^2 + \binom{5}{3} (2a)^{5-3} (-3y)^3 \\
 &\quad + \binom{5}{4} (2a)^{5-4} (-3y)^4 + \binom{5}{5} (2a)^{5-5} (-3y)^5 \\
 &= \frac{5!}{5!0!} 2^5 a^5 - \frac{5!}{4!1!} 2^4 a^4 3y \\
 &\quad + \frac{5!}{3!2!} 2^3 a^3 3^2 y^2 - \frac{5!}{2!3!} 2^2 a^2 3^3 y^3 \\
 &\quad + \frac{5!}{1!4!} 2a 3^4 y^4 - \frac{5!}{0!5!} 3^5 y^5 \\
 &= 2^5 \cdot a^5 - 5 \cdot 2^4 \cdot 3 \cdot a^4 \cdot y + 10 \cdot 2^3 \cdot 3^2 \cdot a^3 \cdot y^2 \\
 &\quad - 10 \cdot 2^2 \cdot 3^3 \cdot a^2 \cdot y^3 + 5 \cdot 2 \cdot a \cdot 3^4 \cdot y^4 - 3^5 \cdot y^5
 \end{aligned}$$

Nota Observemos que el primer término corresponde a $k = 0$. Luego el n -ésimo término corresponde a $k = n - 1$

3. Dado el binomio

$$(6 - 5a)^{19}$$

Busquemos el décimo término y el coeficiente de a^{14}

Solución. El décimo término corresponde a $k = 9$. Este término es el siguiente:

$$\begin{aligned}
 \binom{19}{9} (2 \cdot 3)^{19-9} \cdot 5^9 \cdot a^9 &= -\frac{19!}{10! \cdot 9!} \cdot 2^{10} \cdot 3^{10} \cdot 5^9 \cdot a^9 \\
 &= -2^{11} \cdot 3^{10} \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 5^9 \cdot a^9
 \end{aligned}$$

El coeficiente de a^{14} , corresponde a $k = 14$. Este es:

$$\binom{19}{14} \cdot (2 \cdot 3)^5 (-5)^{14} = 2^7 \cdot 3^7 \cdot 17 \cdot 19 \cdot 5^{14}$$

4. En el binomio

$$\left(2x^2 - \frac{1}{x}\right)^9$$

Busquemos el término independiente de x .

Solución. El término general es

$$\binom{9}{k} (2x^2)^{9-k} \left(-\frac{1}{x}\right)^k$$

Si ponemos la atención solamente en las "x" para obtener el valor de k , tenemos:

$$(x^2)^{9-k} \cdot \left(\frac{1}{x}\right)^k = x^{18-2k-k} = x^{18-3k}$$

Luego $18 - 3k = 0$. Entonces $k = 6$.

El término independiente de x es entonces

$$\binom{9}{6} \cdot 2^{9-6} \cdot (-1)^6 = \frac{9!}{3!6!} 2^3 = 2^5 \cdot 3 \cdot 7$$

5. Busquemos el término central del desarrollo del binomio

$$\left(\frac{2}{x} + \frac{x}{2}\right)^8$$

Solución. El término central corresponde a $k = 4$. Es decir

$$\binom{8}{4} \left(\frac{2}{x}\right)^{8-4} \left(\frac{x}{2}\right)^4 = 2 \cdot 5 \cdot 7$$

Nótese que en este caso, el término central, también corresponde al término independiente de x .

6. Busquemos el quinto término del binomio siguiente:

$$\left(\frac{\sqrt{x^3}}{\sqrt{a}} + \frac{\sqrt{y^5}}{\sqrt{b^3}}\right)^8$$

Solución. El quinto término corresponde a $k = 4$. Tenemos

$$\begin{aligned} \binom{8}{4} \left(\frac{x^{\frac{3}{2}}}{a^{\frac{1}{2}}}\right)^{8-4} \left(-\frac{y^{\frac{5}{2}}}{b^{\frac{3}{2}}}\right)^4 &= \frac{8!}{4!4!} \cdot \frac{x^{\frac{3}{2} \cdot 4}}{a^{\frac{1}{2} \cdot 4}} \cdot \frac{y^{\frac{5}{2} \cdot 4}}{b^{\frac{3}{2} \cdot 4}} \\ &= 2 \cdot 5 \cdot 7 \cdot \frac{x^6 \cdot y^{10}}{a^2 \cdot b^6} \end{aligned}$$

7. Dado el binomio

$$\left(\frac{2x}{25y} - \frac{5y^2}{4x^3}\right)^{27}$$

Busquemos el último término y el coeficiente de $\frac{y^{51}}{x^{77}}$

Solución. El último término se obtiene para $k = 27$ y éste es :

$$\binom{27}{27} \left(\frac{2x}{5^2y}\right)^{27-27} \left(-\frac{5y^2}{2^2x^3}\right)^{27} = -\frac{5^{27}y^{54}}{2^{54}x^{81}}$$

El término general tiene la forma siguiente:

$$\binom{27}{k} \left(\frac{2x}{5^2y}\right)^{27-k} \left(-\frac{5y^2}{2^2x^3}\right)^k$$

Consideremos solamente $\frac{y}{x}$

$$\frac{x^{27-k}}{y^{27-k}} \cdot \frac{y^{2k}}{x^{3k}} = \frac{y^{2k+k-27}}{x^{3k+k-27}} = \frac{y^{3k-27}}{x^{4k-27}}$$

De donde $3k - 27 = 51$, es decir $k = 26$, o bien, consideremos $4k - 27 = 77$, luego $k = 26$. El coeficiente pedido es

$$\binom{27}{26} \left(\frac{2}{5^2}\right)^{27-26} \left(\frac{5}{2^2}\right)^{26} = \frac{27!}{26!1!} \frac{2}{5^2} \frac{5^{26}}{2^{52}} = \frac{5^{24}27}{2^{51}}$$

Luego el coeficiente de $\frac{y^{51}}{x^{77}}$ es $\frac{5^{24}27}{2^{51}}$

8. En el desarrollo del binomio $(1+x)^{43}$, el coeficiente del $(2r+1)$ -ésimo término y del $(r+2)$ -ésimo término son iguales. Encontramos r .

Solución.

$$\binom{43}{2r} = \binom{43}{r+1}$$

Luego $2r = 43 - (r+1)$, de donde $r = 14$

9. En el binomio $(a + b)^6$, busquemos el valor de a y b , sabiendo que el segundo y tercer término de su desarrollo son 576 y 2.160

Solución. Tenemos el sistema de ecuaciones siguientes:

$$\begin{array}{l} (1) \quad \binom{6}{1} a^5 b^1 = 576 \\ (2) \quad \binom{6}{2} a^4 b^2 = 2.160 \end{array} \quad \Rightarrow \quad \begin{array}{l} (1) \quad 6a^5 b = 576 \\ (2) \quad 15a^4 b^2 = 2.160 \end{array}$$

$$\Rightarrow \begin{array}{l} (1) \quad a^5 b = 96 \\ (2) \quad a^4 b^2 = 144 \end{array}$$

$a \cdot (2) : a^5 b^2 = 144a$, luego $a^5 b \cdot b = 144a$, de donde $96b = 144a$. Es decir $b = \frac{3}{2}a$. Reemplazando el valor de b en la ecuación (1), tenemos $a^5 \cdot \frac{3}{2}a = 96$, es decir $a^6 = 64$. Luego $a = \pm 2$ y $b = \pm 3$.

El binomio que buscábamos es $(2 + 3)^6$, o bien, $(-2 + -3)^6$

10. En el binomio $(x + y)^n$, busquemos los valores de x, y, n , sabiendo que el segundo, tercer y cuarto término del desarrollo son 240, 720 y 1080 respectivamente.

Solución. Tenemos:

$$\begin{array}{l} (1) \quad \binom{n}{1} x^{n-1} y^1 = 240 \\ (2) \quad \binom{n}{2} x^{n-2} y^2 = 720 \\ (3) \quad \binom{n}{3} x^{n-3} y^3 = 1080 \end{array}$$

Luego

$$\begin{array}{l} (1) \quad \frac{n!}{(n-1)!1!} x^{n-1} y = 240 \\ (2) \quad \frac{n!}{(n-2)!2!} x^{n-2} y^2 = 720 \\ (3) \quad \frac{n!}{(n-3)!3!} x^{n-3} y^3 = 1080 \end{array}$$

Haciendo todas las simplificaciones posibles, nos queda:

$$\begin{array}{l} (1) \quad nx^{n-1}y^1 = 240 \\ (2) \quad (n-1)nx^{n-2}y^2 = 720 \cdot 2 \\ (3) \quad (n-2)(n-1)nx^{n-3}y^3 = 1080 \cdot 6 \end{array}$$

Tomamos

$$x \cdot (2) : (n-1)nx^{n-1}y \cdot y = 720 \cdot 2 \cdot x$$

Reemplazando la ecuación (1) en esta ecuación, nos queda:

$$(n-1) \cdot 240y = 720 \cdot 2 \cdot x$$

Simplificando, tenemos:

$$(a) : (n-1)y = 6x$$

Luego

$$y = \frac{6x}{n-1}$$

Ahora multipliquemos por x la tercera ecuación

$$x \cdot (3) : (n-2) \cdot (n-1)nx^{n-2}y^2 \cdot y = 1080 \cdot 6x$$

Reemplazando (2) en esta ecuación, queda:

$$(n-2) \cdot 720 \cdot 2 \cdot y = 1080 \cdot 6x$$

De donde obtenemos la ecuación siguiente:

$$(b) : (n-2)2y = 9x$$

Ahora consideremos la ecuación (a) en (b):

$$(n-2)2 \cdot \frac{6x}{n-1} = 9x$$

Luego $4(n-2) = 3(n-1)$. De donde $n = 5$

Consideremos (a) y $n = 5$ en (1):

$$5x^4 \frac{6x}{4} = 240$$

Luego $x^5 = 2^5$, es decir, $x = 2$

Reemplazando $x = 2$ en (a): $y = \frac{6 \cdot 2}{4}$, luego $y = 3$.

Entonces el binomio que cumple estas condiciones es $(2+3)^5$

3.4 Ejercicios Propuestos

1. Escriba como un número combinatorio, la suma:

$$\binom{8}{5} + \binom{8}{6} + \binom{8}{6} + \binom{8}{7}$$

2. Demuestre que

$$\binom{24}{3} \cdot \frac{21}{4} = \binom{24}{4}$$

3. Demuestre por inducción que

(a)

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

(b)

$$\sum_{k=i}^n \binom{k}{i} = \binom{n+1}{i+1}$$

4. Encuentre el termino independiente de a en el desarrollo del binomio siguiente

$$\left(\frac{2b}{3a^6} - \frac{9a^2}{4b^2} \right)^8$$

5. Dado el binomio $\left(\frac{2x}{5y} - \frac{5y}{2x} \right)^{12}$ Encuentre:

(a) El termino central

(b) El coeficiente de $\frac{x^6}{y^6}$

(c) Encuentre, si existe, el termino independiente de x

6. Dado el binomio $\left(x^{\frac{1}{2}} - \frac{1}{3x^{\frac{3}{2}}} \right)^6$. Encuentre:

(a) El coeficiente de $\frac{1}{x}$ (b) El termino central

7. En el binomio $(a + b)^7$, encuentre el valor de a y b sabiendo que el tercer y cuarto termino del desarrollo del binomio son: $\frac{7 \cdot 2^3}{3^4}$
y $\frac{-2 \cdot 5 \cdot 7}{3^4}$

Capítulo 4

Relaciones Binarias

4.1 Producto Cartesiano

Comencemos a estudiar lo que es un "par ordenado". Un ejemplo de par ordenado, es nuestros apellidos, en los cuales hay que respetar el orden en que están. Un par ordenado es denotado en la forma (x, y) .

Observación. $(1, 2) \neq (2, 1)$, $(1, 2) \neq (1, 4)$.

Definición 4.1.1 Diremos que el par (x, y) es **igual** al par (z, t) , denotado $(x, y) = (z, t)$ si y solamente si $x = z$ e $y = t$.

Observación. La definición de par ordenado puede ser dada a partir de la teoría de conjuntos. Es la siguiente:

$$(x, y) = \{\{x\}, \{x, y\}\}$$

Ejemplo. $(1, 2) = \{\{1, 2, 2\}, \{1\}\} = \{\{1\}, \{1, 1, 1, 2, 2, 2, \}\}$

$(3, 1) = \{\{3\}, \{1, 3\}\} = \{\{3, 1\}, \{3\}\} = \{\{1, 3\}, \{3\}, \{3\}, \{3\}\}$

Observación. Sea $A = \{1, 2\}$, $B = \{a, b, c\}$. Queremos escribir el conjunto formado por todos los pares que tienen un elemento de A al lado izquierdo y un elemento de B al lado derecho. Este conjunto lo denotaremos por $A \times B$ y es el siguiente:

$$A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$$

Diremos que este es el producto cartesiano entre A y B . Tenemos la definición siguiente:

Definición 4.1.2 Sean A y B dos conjuntos. Definimos el **producto cartesiano** entre A y B , denotado $A \times B$, de la manera siguiente: $A \times B = \{(a, b); a \in A, b \in B\}$

Ejemplos.

1. Sea $A = \{1, 2, 3\}$ y $B = \{4\}$. Entonces $A \times B = \{(1, 4), (2, 4), (3, 4)\}$
2. Sea $A = \{a, b, c\}$. Entonces

$$A \times A = \{(a, a), (a, b), (a, c), (b, a), (b, b), (b, c), (c, a), (c, b), (c, c)\}$$

Proposición 4.1.1 Sean A, B, C, D conjuntos. Si $A \subset C$ y $B \subset D$, entonces $A \times B \subset C \times D$

Demostración. $(a, b) \in A \times B \Rightarrow (a \in A \wedge b \in B) \Rightarrow (a \in C \wedge b \in D) \Rightarrow (a, b) \in C \times D$

Proposición 4.1.2 Sean A, B conjuntos, entonces $A \times B = \emptyset$ ssi $(A = \emptyset \text{ o } B = \emptyset)$

Demostración. Haremos demostraciones indirectas.

1. Por demostrar $A \times B = \emptyset \Rightarrow (A = \emptyset \text{ o } B = \emptyset)$
 Supongamos no $(A = \emptyset \text{ o } B = \emptyset)$, es decir, $(A \neq \emptyset \wedge B \neq \emptyset)$.
 Luego existe al menos un $a \in A$ y al menos un $b \in B$.
 Luego tenemos $(a, b) \in A \times B$, es decir $A \times B \neq \emptyset$.
 En consecuencia tenemos no $(A \times B = \emptyset)$
2. Por demostrar $(A = \emptyset \text{ o } B = \emptyset) \Rightarrow A \times B = \emptyset$
 Supongamos no $(A \times B = \emptyset)$. Equivalentemente, $A \times B \neq \emptyset$, es decir, existe $(a, b) \in A \times B$, ciertos $a \in A$, $b \in B$. Luego existe $a \in A$ y $b \in B$. Esto quiere decir que $A \neq \emptyset$ y $B \neq \emptyset$. Luego no $(A = \emptyset \text{ o } B = \emptyset)$

Proposición 4.1.3 Sean A, B, C tres conjuntos cualesquiera. Entonces

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

Demostración.

$$\begin{aligned} (a, t) \in A \times (B \cup C) &\Leftrightarrow (a \in A \wedge t \in B \cup C) \\ &\Leftrightarrow (a \in A \wedge (t \in B \vee t \in C)) \\ &\Leftrightarrow ((a \in A \wedge t \in B) \vee (a \in A \wedge t \in C)) \\ &\Leftrightarrow ((a, t) \in A \times B \vee (a, t) \in A \times C) \\ &\Leftrightarrow (a, t) \in (A \times B) \cup (A \times C) \end{aligned}$$

Proposición 4.1.4 Sean A, B, C tres conjuntos cualesquiera. Entonces

$$A \times (B \cap C) = (A \times B) \cap (A \times C)$$

Demostración. Te dejamos la alegría de hacer esta demostración

4.2 Conceptos básicos

Estamos interesados en estudiar relaciones entre dos conjuntos dados y algunas propiedades que ellas puedan cumplir. Comencemos por formalizar el concepto de relación. Primero veámoslo en un ejemplo.

Observación. Sea $A = \{1, 4, 5, 6\}$ y $B = \{2, 6, 8, 12\}$. Consideremos el siguiente subconjunto de $A \times B$:

$$R = \{(1, 2), (1, 6), (1, 8), (1, 12), (4, 8), (4, 12), (6, 6), (6, 12)\}$$

Al mirar detenidamente R , observamos que la primera componente divide a la segunda. Es decir, al considerar un subconjunto de $A \times B$, hemos obtenido una relación entre A y B .

Podemos escribir R por comprensión de la manera siguiente:

$$R = \{(n, m); \quad n \text{ divide a } m\}.$$

Parece natural entonces la definición siguiente:

Definición 4.2.1 Diremos que R es una **relación** entre A y B si R es un subconjunto de $A \times B$. Es decir, todo subconjunto de $A \times B$ es llamado una relación entre A y B

Ejemplo. Sea $X = \{2, 3, 5, 6, 8, 10\}$, $Y = \{1, 2, 3, 4, 5\}$

Sea $R = \{(2, 1), (6, 3), (8, 4), (10, 5)\}$.

Entonces R es una relación entre X e Y .

Nosotros diremos $(2, 1) \in R$ o $(6, 3) \in R$. De ahora en adelante escribiremos $2R1$ o $6R3$. y diremos "2 está relacionado con 1" y "6 está relacionado con 3"

Notación. Si $(x, y) \in R$, escribiremos xRy y diremos "x está relacionado con y". En caso contrario escribiremos $x \not R y$ y diremos que "x no está relacionado con y"

Ejemplo. El ejemplo anterior lo podemos escribir de la manera siguiente:

$$aRb \text{ ssi } a = 2b$$

Observación. Sean $A = \{1, 2, 3, 4\}$ y $R \subset A \times A$ una relación, definida por

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

En este caso $1R3$ y $3R1$, también $1R4$ y $4R1$. Mientras que $2R1$ y $1 \not R 2$, análogamente $3R2$ y $2 \not R 3$.

Observemos también que $2 \not R 4$ y $4 \not R 2$.

Conclusiones.

1. xRy no implica necesariamente yRx .

2. No necesariamente todos los elementos de un conjunto están relacionados, es decir, puede que no tengamos xRy y tampoco tengamos yRx .

Ejemplo. Sea $R \subset \mathbb{N} \times \mathbb{N}$ definida por:

$$aRb \text{ ssi } a + b \text{ es un número par.}$$

En este caso, todo número par está relacionado con todo número par, pues la suma de dos números pares es un número par.

En efecto, a, b pares $\Rightarrow a = 2k, b = 2t$, ciertos $k, t \in \mathbb{N} \Rightarrow a + b = 2k + 2t = 2(k + t)$, ciertos $k, t \in \mathbb{N}$. Es decir, $a + b$ es par.

Además todo número impar está relacionado con todo número impar.

En efecto, a, b impares $\Rightarrow a = 2k + 1, b = 2t + 1$, ciertos $k, t \in \mathbb{N} \Rightarrow a + b = 2k + 1 + 2t + 1 = 2(k + t + 1)$. Es decir, $a + b$ es par.

Sin embargo un número par no está relacionado con ningún número impar ni recíprocamente. En efecto a par, b impar $\Rightarrow a = 2k, b = 2t + 1$, ciertos $k, t \in \mathbb{N} \Rightarrow a + b = 2k + 2t + 1 = 2(k + t) + 1$, es decir $a + b$ es impar.

Ahora estamos interesados en definir nuevos conceptos. Veámoslos primero en la siguiente observación.

Observación. Sean $A = \{1, 2, 3, 4\}$, $B = \{a, b, c\}$ y

$R = \{(1, b), (1, c), (2, c), (4, c)\}$. Diremos que el Dominio de R , denotado $Dom(R)$, es $Dom(R) = \{1, 2, 4\}$.

Diremos que la imagen de R , denotada $Im(R)$ es $Im(R) = \{b, c\}$

B es llamado codominio de R .

Tenemos las siguientes definiciones

Definición 4.2.2 Llamaremos **Dominio** de la relación R , denotado $Dom(R)$, al conjunto formado por todas las primeras componentes de los pares ordenados que forman R . De manera simbólica, escribimos: $Dom(R) = \{a \in A / \exists b \in B; (a, b) \in R\}$

Definición 4.2.3 Llamaremos **Imagen** de la relación R , denotado $Im(R)$, al conjunto formado por todas las segundas componentes de los pares ordenados que forman R . De manera simbólica, escribimos: $Im(R) = \{b \in B / \exists a \in A; (a, b) \in R\}$.

Definición 4.2.4 Si $R \subset A \times B$, entonces B es llamado el **Codomínio** de R

Ejemplos

1. Sea $R \subset \mathbb{N} \times \mathbb{N}$, definida por

$$aRb \text{ ssi } a = b^2.$$

Vemos que la primera componente debe ser un cuadrado perfecto, luego $Dom(R) = \{b^2; b \in \mathbb{N}\} \neq \mathbb{N}$. Sin embargo la segunda componente no tiene ninguna exigencia, luego $Im(R) = \mathbb{N} = Codom(R)$.

2. Sea $R \subset \mathbb{N} \times \mathbb{N}$, definida por

$$aRb \text{ ssi } b = a^2. \text{ En este caso } b \text{ es un cuadrado perfecto.}$$

En este caso $Dom(R) = \mathbb{N}$, $Im(R) = \{a^2; a \in \mathbb{N}\}$. $Im(R) \neq \mathbb{N}$. $Codom(R) = \mathbb{N}$

3. Sea $R \subset \mathbb{N} \times \mathbb{N}$, definida por

$$aRb \text{ ssi } a + b \text{ es par}$$

$Dom(R) = \mathbb{N}$, pues si a es par, todo b par cumple $a + b$ par. Por otra parte si a es impar, todo b impar cumple $a + b$ par, luego $Im(R) = \mathbb{N}$.

Si tomamos b par en $Codom(R)$, existe a par en $Dom(R)$ que cumple $a + b$ par. Si tomamos b impar en $Codom(R)$, existe a impar en $Dom(R)$ que cumple $a + b$ par, es decir se tiene:

$$R = \{(2k, 2t), (2r + 1, 2s + 1); k, t, r, s \in \mathbb{N}\}.$$

4. Sean $A = \{z \in \mathbb{Z}; -10 \leq z \leq 20\}$ y $R \subset A \times A$ definida por:

$$aRb \text{ ssi } a = |b|.$$

Entonces

$$R = \{(0, 0), (1, 1), \dots, (20, 20), (1, -1), \dots, (10, -10)\}$$

Entonces $Dom(R) = \{0, 1, 2, \dots, 20\}$, $Im(R) = A = Codom(R)$

5. Sea $R \subset \mathbb{Z} \times \mathbb{Z}$ definida por

$$aRb \text{ ssi } a + b = 3.$$

Si $a \in \mathbb{Z}$, siempre existe $b \in \mathbb{Z}$ tal que $a + b = 3$. Luego $Dom(R) = \mathbb{Z}$.

De la misma manera, dado $b \in \mathbb{Z}$, siempre existe $a \in \mathbb{Z}$ tal que $a + b = 3$. Luego $Im(R) = \mathbb{Z}$

6. Sea $B = \{2, 3, 4, 6, 8, 9\}$. Sea $R \subset B \times B$ definida por

$$aRb \text{ ssi } (a, b) = 1.$$

Donde (a, b) denota el máximo común divisor entre a y b .

Tenemos entonces que:

$$2R3, 2R9, 3R4, 3R8, 4R9, 8R9, 3R2, 9R2, 4R3, 8R3, 9R4, 9R8.$$

Luego $Dom(R) = \{2, 3, 4, 8, 9\} = Im(R)$. Además $Codom(R) = B$

7. Sean $A = \{2, 3, 5, 7\}$ y $R \subset A \times A$ definida por:

$$aRb \text{ ssi } a < b.$$

Tenemos $2R3$, $2R5$, $2R7$, $3R5$, $3R7$, $5R7$. Luego $Dom(R) = \{2, 3, 5\}$. $Im(R) = \{3, 5, 7\}$. $Codom(R) = A$.

8. Sea $R \subset \mathbb{N} \times \mathbb{N}$ definida por:

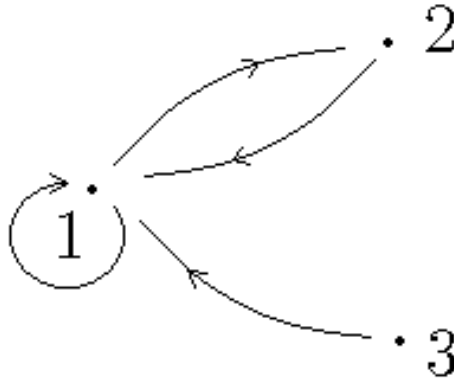
$$aRb \text{ ssi } a^b = 1.$$

Dado $0 \in \mathbb{N}$, $\nexists b \in \mathbb{N}$ tal que $0^b = 1$. Luego $0 \notin Dom(R)$. Sin embargo, $\forall a \in \mathbb{N}$, $a \neq 0$, $a^0 = 1$. Luego $Dom(R) = \mathbb{N}^* = \mathbb{N} - \{0\}$, $Im(R) = \{0, 1\}$.

4.3 Grafos

En esta sección veremos una representación de relaciones en un conjunto A finito. Es decir, $R \subset A \times A$, con A finito.

Observación. Sean $A = \{1, 2, 3\}$ y $R \subset A \times A$, definida por: $R = \{(1, 1), (1, 2), (2, 1), (3, 1)\}$. Su grafo es:

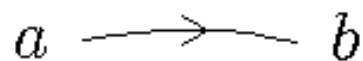


El bucle en el 1 significa $1R1$. La flecha desde 1 hacia 2, significa $1R2$. La flecha desde 2 hacia 1, significa $2R1$ y la flecha desde 3 hacia 1, significa $3R1$.

Nota. Sea $R \subset A \times A$ con A finito. La expresión aRa la representaremos por un bucle en a :



La expresión aRb , la representaremos por una flecha desde a hacia b :

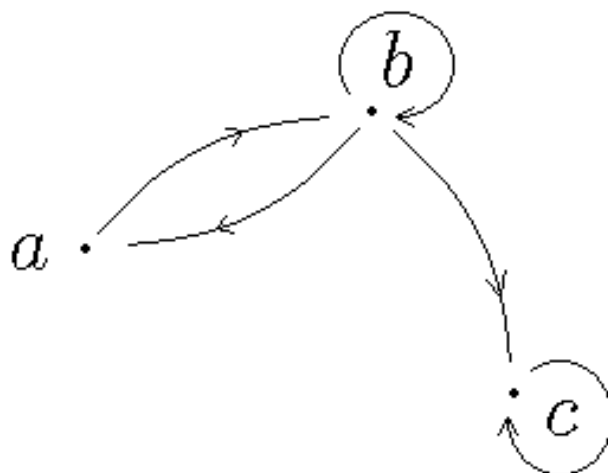


Ejemplos.

- Sean $A = \{a, b, c\}$ y $R \subset A \times A$, definida por:

$$R = \{(a, b), (b, a), (b, b), (b, c), (c, c)\}.$$

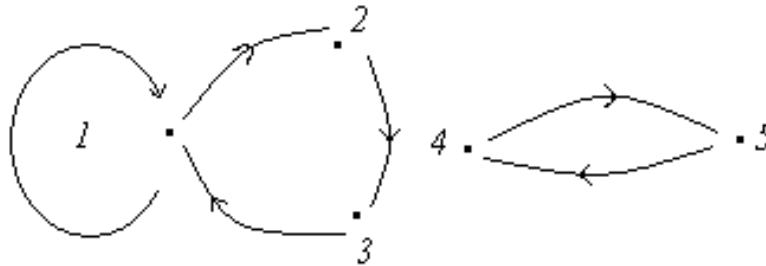
Entonces su grafo es:



- Sean $A = \{1, 2, 3, 4, 5\}$ y $R \subset A \times A$, definida por:

$$R = \{(1, 1), (1, 2), (2, 3), (3, 1), (4, 5), (5, 4)\}.$$

Su grafo es el siguiente:



4.4 Propiedades de las relaciones binarias

De ahora en adelante, estudiaremos una relación R , $R \subset A \times A$ o excepcionalmente $R \subset A \times B$, donde A y B difieren en una cantidad finita de elementos. (Por ejemplo, $R \subset \mathbb{N} \times \mathbb{N}^*$)

En esta sección estudiaremos las propiedades que son necesarias para tener los conceptos de relaciones de equivalencia y las relaciones de orden.

Comenzaremos por aquellas que nos parecen más fáciles de comprender (reflexividad, simetría y transitividad) y luego de tener estos conceptos bien dominados estudiaremos la antisimetría. ¡Verás que es fácil!

4.4.1 Reflexividad

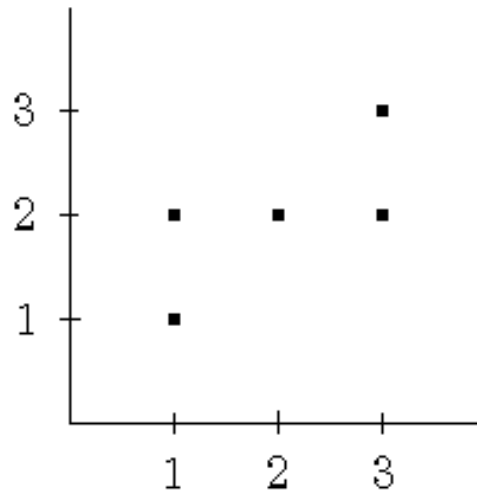
Definición 4.4.1 Sea $R \subset A \times A$. Diremos que R es **refleja** si xRx , $\forall x \in A$.

Ejemplos.

1. Sean $A = \{1, 2, 3\}$ y $R \subset A \times A$, definida por:

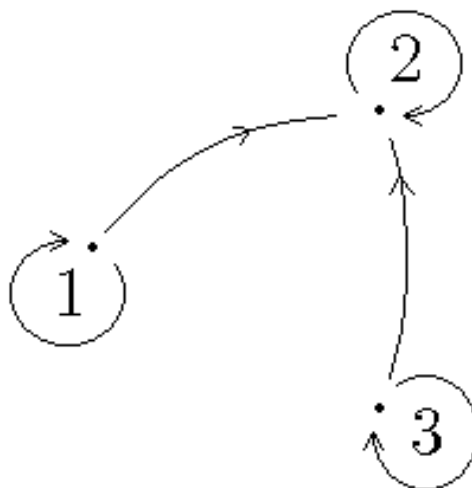
$$R = \{(1, 1), (1, 2), (2, 2), (3, 3), (3, 2)\}$$

Su representación cartesiana es:



Que sea refleja se observa en que están todos los elementos de la diagonal.

Su grafo es:



R es refleja. Esto se observa en que todo elemento tiene un bucle.

2. Sean $A = \{2, 3, 5\}$ y $R \subset A \times A$ definida por:

$$R = \{(2, 2), (3, 3), (5, 5)\}.$$

Tenemos que R es refleja. Esta relación es llamada la **identidad** en A

3. Sea $R \subset \mathbb{Z} \times \mathbb{Z}$ definida por:

$$aRb \text{ ssi } a - b = 3n, \text{ cierto } n \in \mathbb{Z}$$

Demostremos que R es refleja. En efecto $a - a = 0 = 3 \cdot 0$. Luego $aRa, \forall a \in \mathbb{Z}$.

4. Sea $T \subset \mathbb{N} \times \mathbb{N}$ definida por:

$$aRb \text{ ssi } a + b \text{ es par.}$$

T es refleja pues: $a + a = 2a \Rightarrow a + a \text{ es par} \Rightarrow aRa, \forall a \in \mathbb{N}$

5. Sea $S \subset \mathbb{N} \times \mathbb{N}$ definida por:

$$aSb \text{ ssi } a^2 + b^2 \geq 1.$$

S no es refleja pues $0^2 + 0^2 = 0 < 1$. Es decir, el 0 no está relacionado con el 0. Luego $\exists a \in \mathbb{N}$ tal que $a \not R a$.

6. Sea $R \subset \mathbb{Z} \times \mathbb{Z}$ definida por

$$aRb \text{ ssi } \exists r \in \mathbb{Z} \text{ tal que } a \cdot r = b.$$

T es refleja pues: $a \cdot 1 = a, \forall a \in \mathbb{Z}$, luego $aRa, \forall a \in \mathbb{Z}$

7. Sea $R \subset \mathbb{Z} \times \mathbb{Z}$ definida por

$$aRb \text{ ssi } a + b = 3n, \text{ cierto } n \in \mathbb{Z}.$$

R no es refleja. Contraejemplo: 1 no está relacionado con 1, pues $1 + 1 \neq 3n$, $\forall n \in \mathbb{Z}$. Es decir, $\nexists n \in \mathbb{Z}$ tal que $1 + 1 = 3n$.

8. Sea $R \subset \mathbb{Z} \times \mathbb{Z}$ definida por:

$$aRb \text{ ssi } a \leq b.$$

R es refleja pues $a \leq a \forall a \in \mathbb{Z}$, es decir aRa , $\forall a \in \mathbb{Z}$

9. Sea $R \subset \mathbb{Z} \times \mathbb{Z}$ definida por:

$$aRb \text{ ssi } a < b.$$

R no es refleja pues es falso que $a < a$.

10. Sea $R \subset \mathbb{N} \times \mathbb{N}$ definida por:

$$aRb \text{ ssi } (a, b) = 1.$$

El único número natural tal que $(a, a) = 1$ es $a = 1$. Luego aRa sólo para $a = 1$. Luego R no es refleja.

4.4.2 Simetría

Definición 4.4.2 Sea $R \subset A \times A$. Diremos que R es **simétrica** si

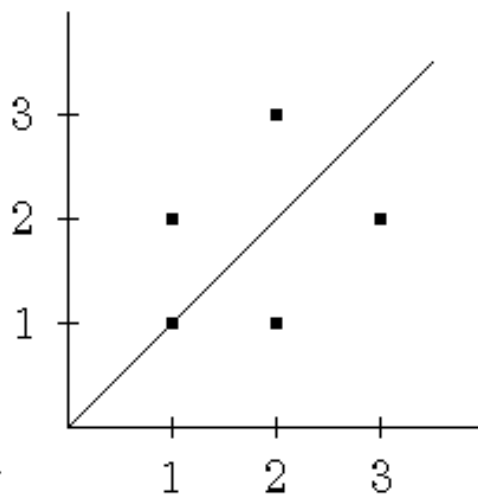
$$aRb \Rightarrow bRa$$

Es decir cada vez que tenemos aRb , debemos tener también bRa . Diremos que el **elemento simétrico** a (a, b) es (b, a) . Llamaremos **eje de simetría** al subconjunto de $A \times A$ siguiente: $\{(a, a); a \in A\}$

Ejemplos.

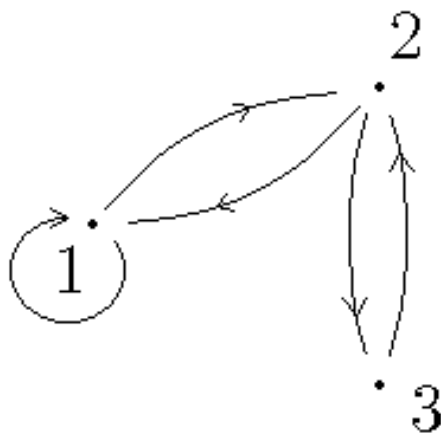
1. Sean $A = \{1, 2, 3\}$ y $R = \{(1, 1), (1, 2), (2, 1), (2, 3), (3, 2)\}$

Gráficamente se tiene



Es claro que esta relación es simétrica. La diagonal es el eje de simetría. La recta que une (a, b) con (b, a) es perpendicular a la diagonal y ambos puntos están a la misma distancia, es decir, son simétricos entre sí.

En un grafo se tiene:

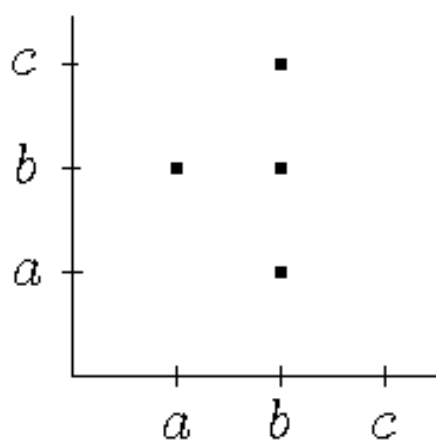


Cuando hay un camino de ida, entonces también está el camino de regreso.

2. Sean $A = \{a, b, c\}$ y $R \subset A \times A$, definida por:

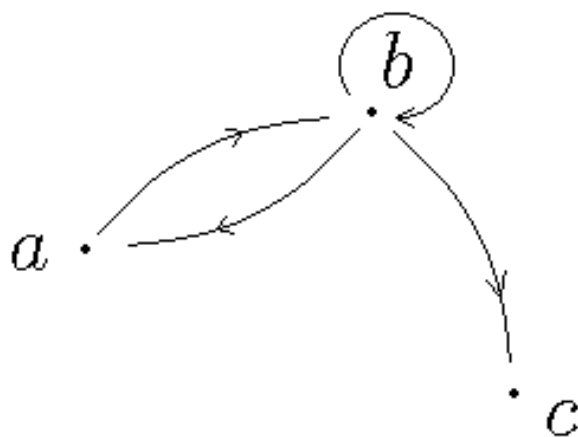
$$R = \{(a, b), (b, a), (b, b), (b, c)\}.$$

Su gráfico es



No está el punto simétrico a (b, c) , que es (c, b) . Luego R no es simétrica.

Su grafo es:



El camino desde b hacia c , no tiene camino de regreso. Luego R no es simétrica.

3. Sea $R \subset \mathbb{N} \times \mathbb{N}$ definida por:

$$aRb \text{ ssi } a + b \text{ es par.}$$

Si aRb entonces $a + b = 2n$, cierto $n \in \mathbb{N}$, luego $b + a = 2n$, $n \in \mathbb{N}$, luego $b + a$ es par. Es decir bRa . Luego R es simétrica.

4. Sea $R \subset \mathbb{Z} \times \mathbb{Z}$ definida por:

$$aRb \text{ ssi } a \leq b.$$

R no es simétrica. Contraejemplo: $1R3$ pero $3 \not R 1$.

5. Sea $R \subset \mathbb{Z} \times \mathbb{Z}$ definida por:

$$aRb \text{ ssi } a - b \text{ es un múltiplo de 3.}$$

Tenemos que R es simétrica. En efecto, $aRb \Rightarrow a - b = 3n$, cierto $n \in \mathbb{Z} \Rightarrow b - a = -3n$, $n \in \mathbb{Z} \Rightarrow b - a = 3(-n)$, $(-n) \in \mathbb{Z} \Rightarrow bRa$

Nota. Si en el caso anterior, hubiésemos tomado \mathbb{N} en vez de \mathbb{Z} , no sería simétrica, pues si $a - b \in \mathbb{N}$, ocurre que $b - a$ no tiene sentido en \mathbb{N} , salvo para $a = b = 0$

6. Sea $R \subset \mathbb{Z} \times \mathbb{Z}$ definida por:

$$aRb \text{ ssi } a + b = 3.$$

Tenemos que R es simétrica.

En efecto, $aRb \Rightarrow a + b = 3 \Rightarrow b + a = 3 \Rightarrow bRa$.

7. Sea $R \subset \mathbb{Z} \times \mathbb{Z}$ definida por:

$$aRb \text{ ssi } a + 2b = 10.$$

Tenemos que $4R3$, pues $4 + 2 \cdot 3 = 10$, sin embargo 3 no está relacionado con 4 , pues $4 + 2 \cdot 4 = 11$ Filosóficamente hablando, si usted cambia a con b , no obtiene la misma expresión. Luego no es una "expresión simétrica"

4.4.3 Transitividad

Definición 4.4.3 Sea $R \subset A \times A$. Diremos que R es **transitiva** si "cada vez que tengamos aRb y también tengamos bRc , entonces obligadamente debemos tener aRc ".

En lenguaje simbólico:

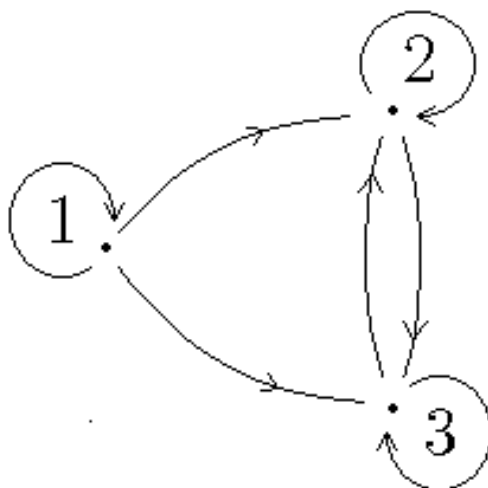
$$aRb \text{ y } bRc \Rightarrow aRc$$

Ejemplos.

1. Sean $A = \{1, 2, 3\}$ y R la relación definida por:

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

En un grafo:



Tenemos el camino del 1 hacia el 2, el camino del 2 hacia el 3 y el camino más corto: del 1 hacia el 3.

Tenemos el camino del 1 hacia el 3, el camino del 3 hacia el 2 y el camino más corto: del 1 hacia el 2.

Son triviales las situaciones siguientes:

$1R1 \wedge 1R3 \Rightarrow 1R3$; $3R2 \wedge 2R2 \Rightarrow 3R2$; $3R3 \wedge 3R2 \Rightarrow 3R2$.
Luego R es transitiva.

2. Sea $R \subset \mathbb{Z} \times \mathbb{Z}$ definida por:

$$aRb \text{ ssi } 2a + b = 7.$$

R no es transitiva. Contraejemplo: $2R3 \wedge 3R1 \wedge \neg 2R1$.

3. Sea $R \subset \mathbb{Z} \times \mathbb{Z}$ definida por

$$aRb \text{ ssi } a - b = 3n, \text{ cierto } n \in \mathbb{Z}.$$

Efectivamente R es transitiva pues: aRb y $bRc \Rightarrow a - b = 3n$,
 $b - c = 3m$, ciertos $n, m \in \mathbb{Z} \Rightarrow (a - b) + (b - c) = 3n + 3m$,
 $n, m \in \mathbb{Z} \Rightarrow a - c = 3(n + m)$, $n + m \in \mathbb{Z}$

Nota. En el ejemplo anterior si aRb , entonces $a - b$ es un múltiplo de 3, lo escribiremos $3n$, $n \in \mathbb{Z}$. Por otra parte, bRc significa que $b - c$ es un múltiplo de 3, pero no tiene por qué ser el mismo múltiplo de 3, luego $b - c = 3m$, $m \in \mathbb{Z}$. No podemos usar la misma letra n , pues no son necesariamente iguales.

4. Sea $R \subset \mathbb{Z} \times \mathbb{Z}$ definida por:

$$xRy \text{ ssi } x \leq y$$

es una relación transitiva.

En efecto, $xRy \wedge yRz \Rightarrow x \leq y \wedge y \leq z \Rightarrow x \leq z \Rightarrow xRz$

4.4.4 Antisimetría

Definición 4.4.4 Sea $R \subset A \times A$. Diremos que R es **antisimétrica** si los únicos elementos que pueden tener su simétrico son aquellos que pertenecen al eje de simetría.

Es decir:

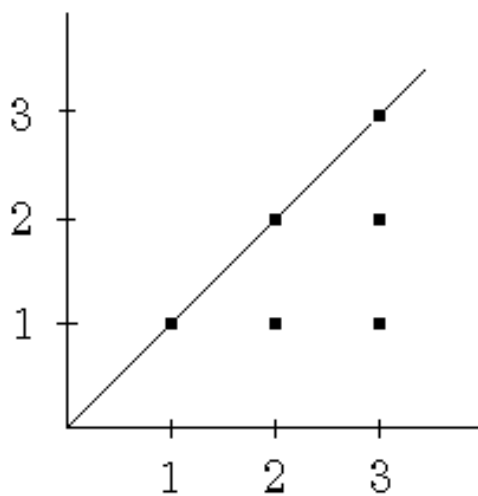
$$R \text{ es antisimétrica ssi } (aRb \wedge bRa \Rightarrow a = b).$$

Ejemplos.

- Sean $A = \{1, 2, 3\}$ y $R \subset A \times A$ definida por:

$$xRy \text{ ssi } x \geq y$$

Esta relación es antisimétrica, su gráfico es:



- Sean $A = \{1, 2, 3\}$ y $R \subset A \times A$ definida por:

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

R no es antisimétrica, pues hay un par, el par $(2, 3)$, que tiene su simétrico y no está en la diagonal. Nótese que esta relación no es simétrica pues el par $(1, 3)$ no tiene su simétrico.

- Sean $A = \{1, 2, 3\}$ y $R \subset A \times A$ definida por:

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

Es antisimétrica. También es simétrica, refleja y transitiva.

¿Puede, en un conjunto cualquiera, haber una relación diferente de la identidad, que cumpla las 4 propiedades estudiadas?

Ejercicios Resueltos.

1. En \mathbb{Z} consideremos, el subconjunto $A = \{1, 2, 3, 4\}$. Estudiemos las propiedades de la relación R definida en A por:

$$aRb \text{ ssi } 2^a \leq a \cdot b$$

Solución

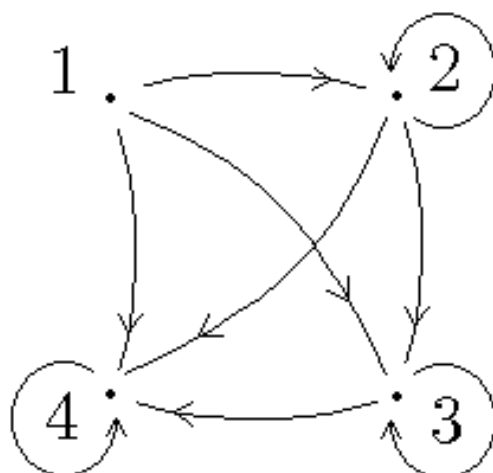
Comencemos por encontrar los pares que están en la relación. Tenemos: $1R2$, $1R3$, $1R4$, $2R2$, $2R3$, $2R4$, $3R3$, $3R4$, $4R4$. Es decir,

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

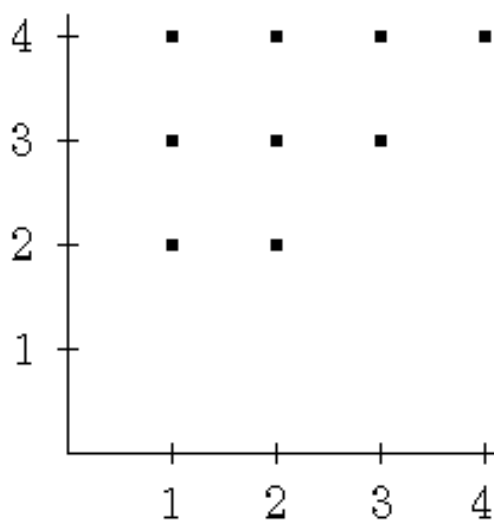
R no es refleja, pues falta el par $(1, 1)$. R no es simétrica, pues está $(1, 2)$ y no está $(2, 1)$. Además hay varios pares que no tienen su simétrico. R es antisimétrica, pues los únicos pares que tienen su simétrico $(3, 3)$, $(2, 2)$, $(4, 4)$.

R es transitiva (te lo dejamos como ejercicio).

En un grafo tenemos:



Su representación cartesiana es:



2. Sean $A \subset \mathbb{Z}$, $A = \{1, 2, 3, 4\}$ y $R \subset A \times A$, definida por:

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

Solución. Tenemos que

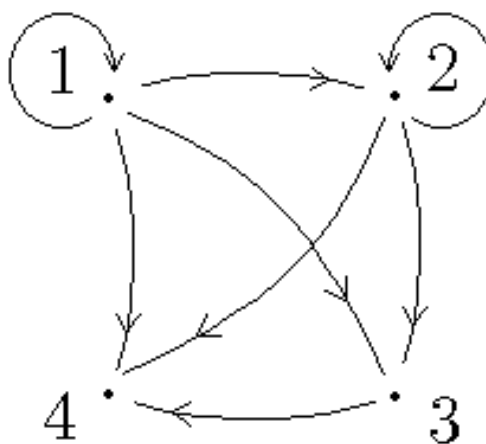
R no es refleja ya que $3 \not R 3$.

No es simétrica pues $1 R 2$ y $2 \not R 1$.

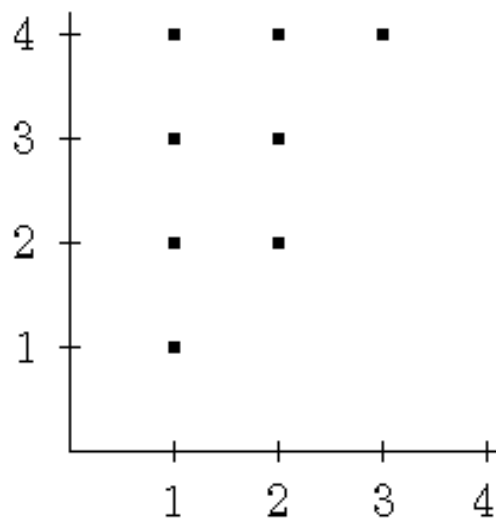
Es antisimétrica, pues los únicos pares que tienen su simétrico son $(1, 1)$ y $(2, 2)$.

Es transitiva, pues $2 R 3 \wedge 3 R 4 \wedge 2 R 4$, $1 R 3 \wedge 3 R 4 \wedge 1 R 4$, $2 R 3 \wedge 3 R 4 \wedge 2 R 4$ y también $1 R 2 \wedge 2 R 4 \wedge 1 R 4$.

Su grafo es:



Su representación cartesiana es:

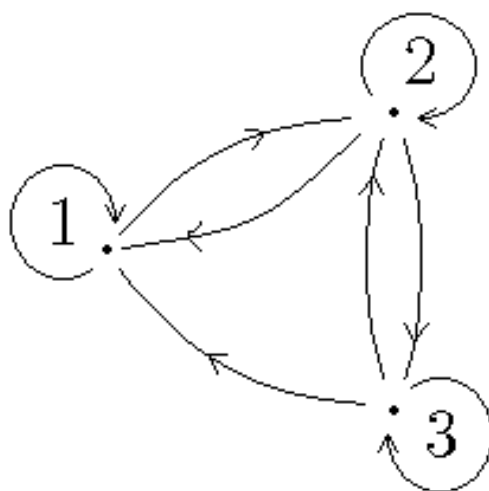


3. Sean $A = \{1, 2, 3\}$ y $R \subset A \times A$, definida por:

$$aRb \text{ ssi } a^2 + 1 \geq b$$

Solución. Los elementos que están relacionados son: $1R1, 1R2, 2R1, 2R2, 2R3, 3R3, 3R2, 3R1$.

Su grafo es:



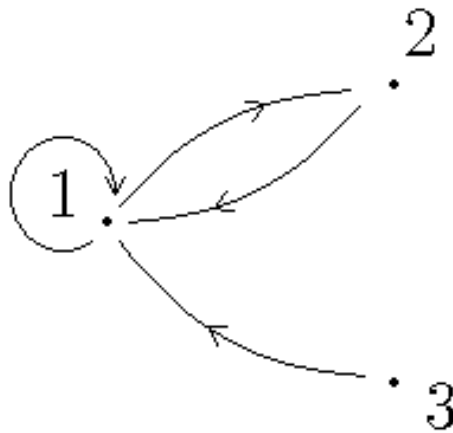
Observamos que R es refleja, pues tenemos $1R1$, $2R2$, $3R3$. R no es simétrica pues $1R2$ y $2 \not R 1$. R no es antisimétrica pues $2R3 \wedge 3R2 \wedge 2 \neq 3$. R no es transitiva pues $1R2 \wedge 2R3$ sin embargo $1 \not R 3$.

4. Sean $A = \{1, 2, 3\}$ y $R \subset A \times A$, definida por:

$$aRb \text{ ssi } a \cdot b \leq a + 1$$

Estudiemos las propiedades de R

Solución. Tenemos $1R1$, $1R2$, $2R1$, $3R1$ Su grafo es:



R no es refleja pues $2 \not R 2$. R no es simétrica pues $3R1$ y $1 \not R 3$. R no es antisimétrica pues $1R2$ y $2R1$ y $1 \neq 2$. R no es transitiva pues $2R1$ y $1R2$ y $2 \not R 2$.

5. Sean $A = \{1, 2, 3\}$ y $R \subset A \times A$, definida por:

$$aRb \text{ ssi } a^3 = b^2 - 1$$

Estudiemos las propiedades de R .

Solución. Tenemos solamente $2R3$.

R no es refleja pues $1 \not R 1$. R no es simétrica pues $2R3$ y $3 \not R 2$. R es antisimétrica y transitiva.

6. Sobre \mathbb{Z} se define la relación R siguiente:

$$aRb \text{ ssi } a - b \text{ es un número impar}$$

Estudiemos las propiedades de R .

Solución.

- (a) R no es refleja. Contraejemplo: 2 no está relacionado consigo mismo, pues $2 - 2 = 0$ y el 0 es par.
- (b) R es simétrica pues $aRb \Rightarrow a - b = 2n + 1$, cierto $n \in \mathbb{Z} \Rightarrow b - a = -(2n + 1)$, cierto $n \in \mathbb{Z} \Rightarrow b - a = 2(-n) - 1 \Rightarrow bRa$.
- (c) R no es transitiva. Contraejemplo: $7R4$ y $4R3$ y $7 \not R 3$. Más aún se puede demostrar que no es transitiva: $aRb \wedge bRc \Rightarrow a - b = 2n + 1, b - c = 2m + 1 \Rightarrow (a - b) + (b - c) = (2n + 1) + (2m + 1) \Rightarrow a - c = 2(n + m + 1) \Rightarrow a \not R c$.
- (d) R no es antisimétrica. Contraejemplo: $5R2 \wedge 2R5 \wedge 2 \neq 5$

7. Sobre \mathbb{Z} se define la relación R siguiente:

$$aRb \text{ ssi } a - b \text{ es un número primo}$$

Estudiemos las propiedades de R .

Solución. Recordemos que un número entero se dice **primo** si tiene exactamente 4 divisores. Ejemplo el 5 es primo, pues sus divisores son: 1, -1, 5, -5.

- (a) R no es refleja. Contraejemplo $5 \not R 5$ pues $5 - 5 = 0$ y el 0 no es primo.

(b) R es simétrica, en efecto:

$$aRb \Rightarrow a - b = p \Rightarrow b - a = -p \Rightarrow bRa$$

Observe que los divisores de p coinciden con los divisores de $-p$

(c) R no es transitiva. Para demostrar que no es transitiva basta que demos un contraejemplo:

$8R5$ y $5R2$ y $8 \not R 2$, pues $8 - 5 = 3$ y $5 - 2 = 3$ y 3 es primo. Sin embargo $8 - 2 = 6$ y 6 no es primo.

(d) R no es antisimétrica. Contraejemplo: $7R5$ y $5R7$ y $5 \neq 7$

8. Sobre \mathbb{Z} se define la relación R siguiente:

$$aRb \text{ ssi } a \cdot b \geq 0$$

Estudiemos las propiedades de R .

Solución.

(a) R es refleja. En efecto:

$$aRa \text{ ssi } a \cdot a \geq 0 \text{ ssi } a^2 \geq 0, \text{ lo cual es verdadero } \forall a \in \mathbb{Z}.$$

(b) R es simétrica. En efecto:

$$aRb \Rightarrow a \cdot b \geq 0 \Rightarrow b \cdot a \geq 0 \Rightarrow bRa$$

(c) R no es transitiva, pues

$$1R0 \wedge 0R-2 \text{ pero } 1 \not R -2$$

(d) R no es antisimétrica. Tenemos el siguiente contraejemplo:

$$1R2 \text{ pues } 1 \cdot 2 \geq 0 \text{ y } 2R1, \text{ pues } 2 \cdot 1 \geq 0 \text{ pero } 1 \neq 2$$

9. Sobre \mathbb{R}^2 se define la relación R siguiente:

$$(a, b)R(c, d) \text{ ssi } a \cdot c \leq b \cdot d$$

Estudiemos las propiedades de R

Solución.

- (a) R no es refleja. Contraejemplo: $(4, 3)$ no está relacionado con $(4, 3)$, pues $4^2 > 3^2$. Sin embargo $(a, a)R(a, a) \forall a \in \mathbb{R}$
 - (b) R es simétrica pues: $(a, b)R(c, d) \Rightarrow a \cdot c \leq b \cdot d \Rightarrow c \cdot a \leq d \cdot b \Rightarrow (c, d)R(a, b)$.
 - (c) R no es antisimétrica. Contraejemplo: $(4, 5)R(3, 7)$ y $(3, 7)R(4, 5)$ y $(3, 7) \neq (4, 5)$
 - (d) R no es transitiva. Contraejemplo: $(2, 3)R(2, 5)$ y $(2, 5)R(7, 3)$ y $(2, 3) \not R(7, 3)$
10. Sea $R \subset A^2$ una relación en A . ¿Qué podemos decir de la relación \overline{R} (el complemento de R) si
- (a) R es refleja
 - (b) R es simétrica (Argumentemos la respuesta)

Solución.

- (a) R refleja $\Rightarrow (x, x) \in R, \forall x \in A \Rightarrow (x, x) \notin \overline{R} \forall x \in A \Rightarrow \overline{R}$ no es refleja.
 - (b) Sea R simétrica. Tenemos:
 $x\overline{R}y \Rightarrow (x, y) \in \overline{R} \Rightarrow \text{no } (x, y) \in R \Rightarrow \text{no } (y, x) \in R \Rightarrow (y, x) \in \overline{R} \Rightarrow y\overline{R}x$. Luego \overline{R} es simétrica.
11. Sea R en \mathbb{R}^2 definida por

$$(a, b)R(c, d) \text{ ssi } a + b < c + d$$

Estudie las propiedades de R

Solución.

- (a) R no es refleja $(a, b)R(a, b)$ ssi $a + b < a + b$. Lo cual es Falso.

- (b) R no es simétrica. Contraejemplo: $(1, 2)R(3, 4)$ sin embargo $(3, 4) \not R(1, 2)$
- (c) R es transitiva.

$$\begin{aligned}(a, b)R(c, d) \wedge (c, d)R(e, f) &\Rightarrow a + b < c + d \wedge c + d < e + f \\ &\Rightarrow a + b < e + f \\ &\Rightarrow (a, b)R(e, f)\end{aligned}$$

4.5 Relaciones de equivalencia

4.5.1 Introducción y definición

El concepto de "Relación de equivalencia", es un concepto que está inmerso en la vida diaria. Es un concepto que se utiliza diariamente.

...el tiempo ha ido transcurriendo...

... los años, los siglos, los milenios

... los segundos, los minutos, las horas.

Los años, los siglos, los milenios, han sido denotados por números naturales, aunque escondidamente son números enteros. Por ejemplo el s.II A.C. podría ser denotado s.-II.

Para las horas, minutos, segundos, aparentemente usamos los números naturales, pero, en este caso, la apariencia engaña.

En el caso de la hora, solamente usamos los números naturales desde el 0 hasta el 23, o bien desde el 0 hasta el 11.

Si tú observas más detenidamente, éstos números no se suman de la misma manera que los números naturales, sólo a veces coincide la manera de sumar.

Imagina que son las 20 hrs y que en 5 horas más te vas a desconectar de internet. Decimos: $20 + 5 = 1$. La respuesta es a la 1 : 00 hrs te desconectarás de internet.

¿Cuál fué el razonamiento que hemos usado?

Observe que para nosotros, el 25 y el 1 son "como si fuera lo mismo". En lenguaje matemático: "Hemos hecho una identificación".

¿Qué hay detrás de todo esto?

Hay una relación R , $R \subset \mathbb{Z} \times \mathbb{Z}$

La relación R que se define al estar pensando en la hora, es la siguiente:

$$aRb \text{ ssi } a - b \text{ es un múltiplo de } 24.$$

Así tenemos por ejemplo: $26R2$, $30R6$, etc.

Observamos que esta relación es:

refleja, simétrica y transitiva

Esta idea ha sido generalizada de la manera siguiente:

Definición 4.5.1 Sea A un conjunto y R una relación en A . Diremos que R es una **Relación de equivalencia** si R es refleja, simétrica y transitiva. Los elementos que están relacionados entre sí son llamados *equivalentes*.

Su nombre se debe a que los elementos que están relacionados entre sí, son muy parecidos, se comportan de la misma manera, es por esto que son llamados equivalentes y la relación es llamada de equivalencia.

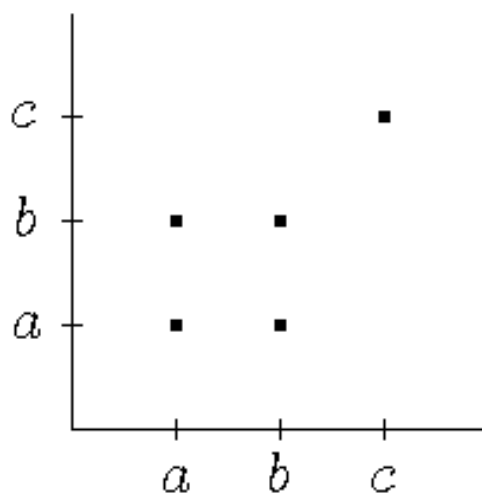
Ejemplos.

1. Sea $A = \{a, b, c\}$ y $R \subset A \times A$, definida por:

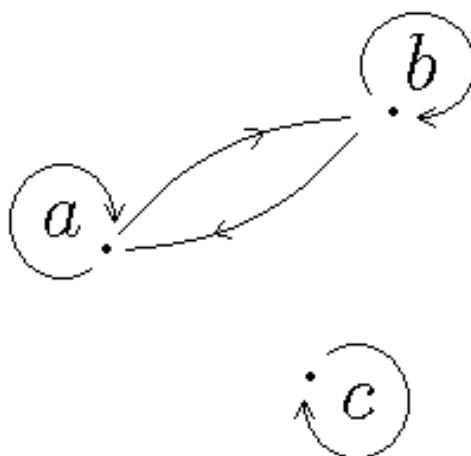
$$R = \{(a, a), (a, b), (b, a), (b, b), (c, c)\}$$

Ocurre que R es una relación de equivalencia.

Su gráfico es:



Su grafo es:



En su grafo se observa fácilmente que es una relación de equivalencia.

2. Sea R una relación en \mathbb{Z} definida por:

$$aRb \text{ ssi } a - b \text{ es un múltiplo de } 3$$

Entonces R es una relación de equivalencia.

En la sección anterior demostramos que R es refleja, simétrica y transitiva.

Observemos que:

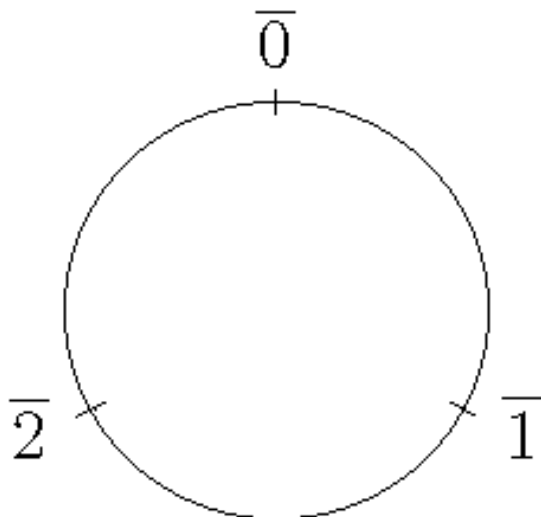
Todos los múltiplos de 3, están relacionados entre sí.

Todos los múltiplos de 3 más 1, están relacionados entre sí.

Todos los múltiplos de 3 más 2, están relacionados entre sí.

Denotemos por $\bar{0}$ el conjunto formado por los múltiplos de 3, por $\bar{1}$ el conjunto formado por los múltiplos de 3 más 1 y por $\bar{2}$ el conjunto formado por los múltiplos de 3 más 2.

Y los ponemos en un reloj.



3. Sea $A = \{a, b, c, d, e, f\}$ y $R \subset A \times A$, definida por:

$$R = \{(a, a), (a, b), (b, a), (b, b), (c, c), (e, f), (f, e), (e, e), (f, f)\}$$

Tenemos que R es una relación de equivalencia.

4. Sea $P = \{\text{personas}\}$ y $R \subset P \times P$, definida por:

aRb ssi tienen el mismo grupo sanguíneo.

Ocurre que R es una relación de equivalencia. Observamos que hay 8 grupos sanguíneo, a saber: $A^+, B^+, 0^+, AB^+, 0^-, A^-, B^-, AB^-$

5. Sobre $\mathbb{Z} \times \mathbb{Z}^*$, definimos la relación siguiente:

$$(a, b)R(c, d) \text{ ssi } a \cdot d = b \cdot c$$

Demostremos que es de equivalencia. En efecto

- (a) R es refleja:

$(a, b)R(a, b)$ ssi $a \cdot b = b \cdot a$, lo cual es verdadero $\forall a \in \mathbb{Z}$ y $\forall b \in \mathbb{Z}^*$.

- (b) R es simétrica:

$$(a, b)R(c, d) \Leftrightarrow a \cdot d = b \cdot c \Leftrightarrow b \cdot c = a \cdot d \Leftrightarrow c \cdot b = d \cdot a \Leftrightarrow (c, d)R(a, b)$$

- (c) R es transitiva:

Esta demostración es más elaborada, pero no es para desanimarse pues es muy interesante:

$$(a, b)R(c, d) \text{ y } (c, d)R(e, f) \Rightarrow ad = bc \text{ y } cf = de \Rightarrow adcf = bcde$$

Puesto que $d \in \mathbb{Z}^*$, podemos cancelar d , luego $acf = bce$.

Para c , tenemos dos posibilidades:

- i. $c \neq 0$, en este caso, cancelamos c y tenemos $af = be$, luego $(a, b)R(e, f)$ y se tiene que R es transitiva.
- ii. $c = 0$, luego $ad = 0$ y $de = 0$. Como $d \neq 0$, se tiene $a = 0$ y $e = 0$, luego $0 \cdot f = b \cdot 0$, es decir, $af = be$, entonces $(a, b)R(e, f)$.

Por (a), (b) y (c) R es una relación de equivalencia.

Es curioso que esta relación no es transitiva sobre $\mathbb{Z} \times \mathbb{Z}$. Contraejemplo: $(1, 9)R(0, 0)$ y $(0, 0)R(2, 5)$ y $(1, 9) \not R(2, 5)$

6. Sea $L = \{\text{rectas sobre el plano}\}$.

Sobre L se define la siguiente relación

$$lRl' \text{ ssi } l \text{ es paralela a } l'$$

Recordemos que una recta l es **paralela** a una recta l' ssi tienen la misma pendiente.

- (a) R es refleja. lRl porque l tiene la misma pendiente que l
- (b) R es simétrica. ¡Trivial!
- (c) R es transitiva. Sea l de pendiente m . Si lRl' y $l'Rl''$, entonces l' tiene pendiente m y l'' tiene pendiente m , luego lRl'' .

Por (a), (b) y (c) tenemos que R es una relación de equivalencia.

7. Sea A un conjunto y R una relación refleja y simétrica en A .

Se define en A la relación R' siguiente:

$$aR'b \text{ ssi } \exists a_1, a_2, \dots, a_n \in A \text{ tq. } a_1 = a, a_n = b \text{ y } a_i R a_{i+1}, \\ i = 1, n-1.$$

Demostremos que R' es una relación de equivalencia.

Demostración.

- (a) R' es refleja ya que R es refleja, luego se tiene $aRa \forall a \in A$. Luego $a_1 = a, a_n = a$ y aRa . Luego $aR'a$.
- (b) R' es simétrica. $aR'b \Rightarrow \exists a_1, \dots, a_n \in A$ tal que $a_1 = a, a_n = b$ y $a_i R a_{i+1} \Rightarrow \exists a_1, \dots, a_n \in A$ talque $a_1 = a, a_n = b$ y $a_{i+1} R a_i$. Sea $b = b_1 = a_n, b_2 = a_{n-1}, \dots, b_i = a_{n-(i-1)}, \dots, b_n = a_1 = a$ y $b_i R b_{i+1}$. Luego $bR'a$
- (c) R' es transitiva.

$$\begin{aligned} aR'b \wedge bR'c &\Rightarrow (\exists a_1, \dots, a_n; a_1 = a, a_n = b \wedge a_i R a_{i+1}) \wedge \\ &\quad (\exists b_1, \dots, b_m; b_1 = b, b_m = c \wedge b_j R b_{j+1}) \\ &\Rightarrow \exists a_1, \dots, a_n = b_1, \dots, b_m; a_i R a_{i+1} \wedge b_j R b_{j+1} \\ &\Rightarrow aR'c \end{aligned}$$

8. Sea R una relación refleja y transitiva en un conjunto A . En A se define:

$$aR'b \text{ ssi } aRb \text{ y } bRa$$

Demostremos que R' es una relación de equivalencia.

- (a) R' es refleja. En efecto, $aRa, \forall a \in A \Rightarrow aRa \wedge aRa \Rightarrow aR'a, \forall a \in A$.
- (b) R' es simétrica. $aR'b \Rightarrow aRb \wedge bRa \Rightarrow bRa \wedge aRb \Rightarrow bR'a$.
- (c) R' es transitiva. $aR'b \wedge bR'c \Rightarrow aRb \wedge bRa \wedge bRc \wedge cRb \Rightarrow (aRb \wedge bRc) \wedge (cRb \wedge bRa) \Rightarrow aRc \wedge cRa \Rightarrow aR'c$

Por (a), (b) y (c) tenemos que R' es una relación de equivalencia.

4.5.2 Clases de Equivalencia y conjunto cuociente

Nuevamente quiero que sepas que el concepto de "clases de equivalencia" es utilizado en la vida diaria. Imaginemos que sobre una mesa extendemos una masa. Uno se aleja, mira y dice: "es una masa". ¡Olvídate! Ahora, con un cuchillo cortamos la masa en líneas rectas paralelas, cercanas una de otra.

Definamos la relación: "Dos elementos están relacionados si están en el mismo pedazo de masa". Es trivial que es una relación de equivalencia.

Si ahora uno mira la mesa, dice: "son tallarines". Ocurre que cada tallarín es una "clase de equivalencia". Todos los elementos que están en un tallarín, están relacionados entre sí y no están relacionados con los elementos que están en otro tallarín.

Bueno, filosóficamente hablando, tenemos que cambió la esencia de la masa que teníamos sobre la mesa, es por esto que nos vimos invitados a cambiarle el nombre.

Esto es exactamente lo que ocurre con una relación de equivalencia, "parte" el conjunto en clases de equivalencia y si ahora miramos el conjunto obtenido, ha cambiado su esencia. Hablaremos de "conjunto cuociente", para designar la unión de todas las clases. Le llamaremos

cuociente, pues todos los pedazos de masa que están en el mismo tallarín los identificaremos con "un solo tallarín". Hay intrínsecamente un concepto de división.

Mas, no queda nuestra alma tranquila con este ejemplo culinario. Queremos demostrarte que utilizas los conceptos de "clase de equivalencia" y "conjunto cuociente" en un ejemplo matemático. Comencemos por ver las definiciones:

Definición 4.5.2 Sean A un conjunto no vacío y $R \subset A \times A$ una relación de equivalencia. Se llama **clase de equivalencia módulo R de un elemento a** , $a \in A$, al conjunto formado por todos los elementos $x \in A$ que están relacionados con a , por la relación R , denotada $C(a)$ o $cl(a)$ o \bar{a} y se lee: clase de a . Es decir

$$cl(a) = \{x \in A; xRa\}$$

La clase de a es un subconjunto de A , luego $cl(a) \in P(A)$. Cada elemento de la clase de a puede ser considerado un representante de su clase.

Definición 4.5.3 Se llama **conjunto cuociente de A por R** , al conjunto formado por todas las clases de equivalencia de A según R , se denota A/R . Es decir,

$$A/R = \{cl(a); a \in A\}$$

Veamos ahora el ejemplo matemático de la vida diaria:

Observación Sobre $\mathbb{Z} \times \mathbb{Z}^*$ consideremos la relación de equivalencia antes definida, a saber

$$(a, b)R(c, d) \text{ ssi } a \cdot d = b \cdot c$$

La clase del elemento (a, b) , denotada $cl(a, b)$, consiste en el conjunto formado por todos los elementos relacionados con (a, b) , es decir,

$$cl(a, b) = \{(c, d); (a, b)R(c, d)\}$$

Por ejemplo veamos la clase del elemento $(1, 2)$. Tenemos: $(a, b)R(1, 2)$ ssi $a \cdot 2 = b \cdot 1$ ssi $b = 2a, b \neq 0$. Luego

$$cl(1, 2) = \{(a, 2a); a \in \mathbb{Z}^*\}$$

Observemos por ejemplo: $(1, 2)R(2, 4); (1, 2)R(3, 6); (1, 2)R(4, 8)$, etc., luego podemos escribir: $cl(1, 2) = cl(3, 6) = cl(4, 8)$.

En este ejemplo, en particular, usaremos otra notación. La clase del elemento (a, b) , será denotada $\frac{a}{b}$. Luego $\frac{1}{2} = \frac{2}{4} = \frac{3}{6} = \frac{a}{2a}, a \neq 0$

¡Aparecieron las fracciones! Estamos, entonces de acuerdo que uno tiene incorporado el concepto de clase de equivalencia en la vida diaria ¿cierto? ¡seguro!

Nuevamente, hemos cambiado la esencia de los entes, luego estamos filosóficamente invitados a cambiarles el nombre. Cada clase será llamada un número racional. Ahora bien, el conjunto formado por todas las clases de equivalencia, llamado "conjunto cociente", es llamado, conjunto de los números racionales, denotado \mathbb{Q} . Escribiremos $(\mathbb{Z} \times \mathbb{Z}^*)/R = \mathbb{Q}$.

Recordemos que al comienzo del ejemplo vimos que esta relación no es de equivalencia sobre $\mathbb{Z} \times \mathbb{Z}$. Esta es una explicación de por qué no puede haber 0 en el denominador de una fracción.

Ejemplo. Sea $R \subset \mathbb{Z} \times \mathbb{Z}$ definida por:

$$aRb \text{ ssi } a - b = 3n, \text{ cierto } n \in \mathbb{Z}.$$

Recordemos que ya analizamos esta relación, por lo que podemos escribir directamente las clases de equivalencia, a saber:

$$cl(0) = \{3n; n \in \mathbb{Z}\}$$

$$cl(1) = \{3n + 1; n \in \mathbb{Z}\}$$

$$cl(2) = \{3n + 2; n \in \mathbb{Z}\}$$

El conjunto cuociente es: $\mathbb{Z}/R = \{cl(0), cl(1), cl(2)\}$

Ejemplo. Sean $A = \{a, b, c\}$, $R \subset A \times A$ definida por :

$$R = \{(a, a), (a, b), (b, a), (b, b), (c, c)\}$$

$$cl(a) = \{a, b\} = cl(b); cl(c) = \{c\}$$

Observación. El conjunto de personas se puede dividir en ocho grupos, de acuerdo a su grupo sanguíneo. Son ocho grupos disjuntos de dos en dos, es decir, no hay una persona que pertenezca a dos grupos. La unión de los ocho grupos es exactamente el conjunto H formado por todas las personas, es decir,

$$cl(0^+) \cup cl(A^+) \cup cl(B^+) \cup cl(AB^+) \cup cl(0^-) \cup cl(A^-) \cup cl(B^-) \cup cl(AB^-)$$

Tenemos $H = \text{Humanidad}$, "partido" en ocho subconjuntos, luego:

$$\{cl(0^+), cl(A^+), cl(B^+), cl(AB^+), cl(0^-), cl(A^-), cl(B^-), cl(AB^-)\}$$

es una "partición" de H . Esto nos invita a la definición siguiente:

Definición 4.5.4 Sean A un conjunto y $P_1, P_2, \dots, P_t \in P(A)$. Diremos que el conjunto $\{P_1, P_2, \dots, P_t\}$ es una **partición de A** si:

1. $P_i \neq \emptyset, \forall i = 1, \dots, t$
2. $P_1 \cup P_2 \cup \dots \cup P_t = A$
3. $P_i \cap P_j = \emptyset, \forall i \neq j$

Teorema 4.5.1 (Teo. Fundamental sobre rel. de equivalencia)

A toda relación de equivalencia R , en un conjunto A , le corresponde una descomposición de A en clases de equivalencia disjuntas dos a dos y cuya unión es A . Es decir, el conjunto A/R es una partición de A .

Demostración. Comenzaremos por demostrar que :

$$aRb \implies cl(a) = cl(b)$$

En efecto, si $x \in cl(a)$ entonces xRa y puesto que aRb entonces se tiene xRb es decir $x \in cl(b)$, luego $cl(a) \subset cl(b)$. Análogamente se prueba que $cl(b) \subset cl(a)$, luego $cl(a) = cl(b)$.

Ahora demostraremos que si dos elementos no están relacionados entonces sus clases de equivalencia son disjuntas, es decir:

$$a \not R b \implies cl(a) \cap cl(b) = \emptyset$$

En efecto, sea $x \in cl(a) \cap cl(b) \implies x \in cl(a)$ y $x \in cl(b) \implies xRa$ y $xRb \implies aRx$ y $xRb \implies aRb \implies \Leftarrow$, luego $cl(a) \cap cl(b) = \emptyset$

De lo anterior se desprende que A es la unión disjunta de todas las clases de equivalencia.

Teorema 4.5.2 (Teorema recíproco) *A toda partición de un conjunto A , le corresponde una relación de equivalencia R de A , cuyas clases de equivalencia son los elementos de la partición.*

Demostración. Se define la relación de equivalencia:

$$aRb \text{ ssi } a \text{ y } b \text{ están en el mismo elemento de la partición.}$$

Ejemplos.

1. Sobre \mathbb{Z} definamos la relación de equivalencia siguiente:

$$aRb \text{ ssi } a - b = 12n, n \in \mathbb{Z}$$

Denotemos por \bar{a} la clase del elemento a . Tenemos $\bar{0} = \{12n; n \in \mathbb{Z}\}$; $\bar{1} = \{12n + 1; n \in \mathbb{Z}\}, \dots, \bar{11} = \{12n + 11; n \in \mathbb{Z}\}$.

Cada elemento de la partición es una clase de equivalencia y la unión de todas las clases es el conjunto \mathbb{Z} . Es decir

$$\mathbb{Z}/R = \bar{0} \dot{\cup} \bar{1} \dot{\cup} \dots \dot{\cup} \bar{11}$$

En este caso se denota $\mathbb{Z}/R = \mathbb{Z}_{12}$

2. Sea $R \subset \mathbb{Z} \times \mathbb{Z}$ definida por

$$aRb \text{ ssi } a + b = 2n, \text{ cierto } n \in \mathbb{Z}$$

Ya vimos que R es una relación de equivalencia. Recordemos que la suma de dos números es par si y sólo si ambos números son pares o ambos impares. Luego tenemos dos clases de equivalencia: la clase de los números pares y la clase de los números impares. Es decir, $\mathbb{Z}/R = \{2n; n \in \mathbb{Z}\} \dot{\cup} \{2n+1; n \in \mathbb{Z}\}$

3. Sea L el conjunto de todas las rectas en el plano euclidiano. Sea R la relación de equivalencia definida por:

$$lRl' \text{ ssi } l \text{ es paralela a } l'$$

Vimos que R es una relación de equivalencia en L . Esta relación de equivalencia en L , permite clasificar todas las rectas del plano euclidiano como sigue:

- (a) Dos rectas paralelas pertenecen a la misma clase.
- (b) Dos rectas que no son paralelas, pertenecen a clases distintas.

Así todas las rectas están clasificadas. Cada clase se llama una "dirección". Toda recta puede ser escogida como representante de una dirección.

4.5.3 Congruencias en \mathbb{Z}

Nosotros vimos que la relación R en \mathbb{Z} definida por:

$$aRb \text{ ssi } a - b \text{ es un múltiplo de } n.$$

es una relación de equivalencia. A propósito de esta relación tenemos la definición siguiente:

Definición 4.5.5 Dos enteros a y b se dicen **congruentes módulo n** , $n \in \mathbb{Z}$ ssi $a - b$ es un múltiplo de n . Notación: $a \equiv b \pmod{n}$.

Luego $a \equiv b \pmod{n}$ ssi $a - b = kn$, cierto $k \in \mathbb{Z}$ ssi $a = b + kn$, cierto $k \in \mathbb{Z}$. Esta relación es llamada **congruencia módulo n** .

Observamos que si $a \equiv b \pmod{n}$ ssi $a \equiv b \pmod{-n}$, luego n y $-n$ definen la misma clase de equivalencia por lo tanto hablaremos de congruencias módulo n con $n \in \mathbb{N}$.

Además notemos que $cl(a) = \{a, a \pm n, a \pm 2n, \dots\}$ y como por el algoritmo de Euclides se tiene que $a = qn + r$ con $0 \neq r < n$, por lo tanto aRr y $cl(a) = cl(r)$. Esto quiere decir que para cada clase de equivalencia se puede tomar como representante uno de los números $0, 1, \dots, n - 1$.

Por otra parte si $0 \neq r < r' < n$, se tiene que r no es equivalente a r' . En efecto si $r' \equiv r \pmod{n}$ luego $r' - r = kn$ cierto $k \in \mathbb{Z}$, es decir $r' = r + kn$, con $k > 0$. Luego $r' > n$, contradicción.

Luego hay exactamente n clases de equivalencia, las que denotaremos por $\overline{0}, \overline{1}, \dots, \overline{n-1}$. \mathbb{Z}_n denotará \mathbb{Z}/R , el conjunto cociente de \mathbb{Z} por la relación R . Luego

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}.$$

Los elementos de \mathbb{Z}_n se llaman **enteros módulo n** .

Observe que el cardinal de \mathbb{Z}_n es n .

Ejemplo. Como caso particular de lo visto anteriormente, veamos la relación:

$$aRb \text{ ssi } a \equiv b \pmod{5}$$

En este caso tenemos:

$$cl(0) = \{x \in \mathbb{Z}; 0Rx\} = \{x \in \mathbb{Z}; x = 5k, k \in \mathbb{Z}\}.$$

Análogamente, se obtienen:

$$\begin{aligned} cl(1) &= \{5k + 1, k \in \mathbb{Z}\}, cl(2) = \{5k + 2, k \in \mathbb{Z}\}, \\ cl(3) &= \{5k + 3, k \in \mathbb{Z}\}, cl(4) = \{5k + 4, k \in \mathbb{Z}\}. \end{aligned}$$

Además se tiene: $\mathbb{Z}/R = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\} = \mathbb{Z}_5$

Ejercicios Resueltos

1. En \mathbb{Z} , considere la relación:

$$xRy \text{ ssi } x^2 - y^2 = 3y - 3x.$$

Demostremos que R es una relación de equivalencia y busquemos las clases de equivalencia de 0, 2 y a

Solución. Esta relación se puede escribir como:

$$xRy \text{ ssi } x^2 + 3x = y^2 + 3y.$$

- (a) R es refleja. En efecto, $xRx \text{ ssi } x^2 + 3x = x^2 + 3x$, lo cual es verdadero $\forall x \in \mathbb{Z}$.
 (b) R es simétrica. En efecto,

$$xRy \text{ ssi } x^2 + 3x = y^2 + 3y \text{ ssi } y^2 + 3y = x^2 + 3x \text{ ssi } yRx.$$

- (c) R es transitiva. En efecto,

$$xRy \wedge yRz \text{ ssi } x^2 + 3x = y^2 + 3y \wedge y^2 + 3y = z^2 + 3z$$

Luego $x^2 + 3x = z^2 + 3z$, es decir tenemos xRz

Por (a), (b) y (c) R es una relación de equivalencia.

Busquemos la clase del 0. Tenemos: $xR0 \text{ ssi } x^2 + 3x = 0^2 + 3 \cdot 0 \Rightarrow x^2 + 3x = 0 \Rightarrow x(x+3) = 0 \Rightarrow x = 0 \vee x = -3 \Rightarrow cl(0) = \{0, -3\}$

Busquemos la clase del 2. Tenemos: $xR2 \text{ ssi } x^2 + 3x = 2^2 + 3 \cdot 2 \Rightarrow x^2 + 3x - 10 = 0 \Rightarrow (x+5)(x-2) = 0 \Rightarrow x = -5 \vee x = 2 \Rightarrow cl(2) = \{2, -5\}$

Busquemos la clase de un elemento cualquiera a . Tenemos $xRa \text{ ssi } x^2 + 3x = a^2 + 3a \Rightarrow x^2 + 3x - (a^2 + 3a) = 0 \Rightarrow x^2 + 3x - a(a+3) = 0 \Rightarrow (x-a)(x+a+3) = 0 \Rightarrow x = a \vee x = -a-3 \Rightarrow cl(a) = \{a, -a-3\}$

2. **Construcción de \mathbb{Z} .** En $\mathbb{N} \times \mathbb{N}$, consideremos la relación:

$$(a, b)R(c, d) \text{ ssi } a + d = b + c.$$

Demostremos que R es una relación de equivalencia, busquemos una caracterización de cada clase de equivalencia y luego busquemos el conjunto cociente.

Solución.

- (a) R es refleja. En efecto, $(a, b)R(a, b)$ ssi $a + b = b + a$. Esto es verdadero para todo $(a, b) \in \mathbb{N}^2$.
- (b) R es simétrica. En efecto,

$$\begin{aligned} (a, b)R(c, d) &\Leftrightarrow a + d = b + c \\ &\Leftrightarrow c + b = d + a \\ &\Leftrightarrow (c, d)R(a, b) \end{aligned}$$

- (c) R es transitiva. En efecto,

$$\begin{aligned} (a, b)R(c, d) \wedge (c, d)R(e, f) &\Rightarrow (a + d = b + c) \wedge (c + f = d + e) \\ &\Rightarrow a + d + c + f = b + c + d + e \\ &\Rightarrow a + f = b + e \\ &\Rightarrow (a, b)R(e, f) \end{aligned}$$

Por (a), (b) y (c) R es una relación de equivalencia.

Busquemos la clase del elemento $(0, 0)$. En efecto, $(a, b)R(0, 0)$ ssi $a + 0 = b + 0$ ssi $a = b$. Luego $\overline{(0, 0)} = \{(a, a); a \in \mathbb{N}\}$

Busquemos la clase del elemento $(1, 2)$. En efecto $(a, b)R(1, 2)$ ssi $a + 2 = b + 1$ ssi $b = a + 1$. Luego $\overline{(1, 2)} = \{(a, a + 1); a \in \mathbb{N}\}$

Busquemos la clase del elemento $(2, 1)$: En efecto $(a, b)R(2, 1)$ ssi $a + 1 = b + 2$ ssi $a = b + 1$. Luego $\overline{(2, 1)} = \{(b + 1, b); b \in \mathbb{N}\}$.

En un gráfico:

Busquemos el representante más simple posible de la clase de (a, b)

- (a) Sea $a < b$. Luego $\exists n \in \mathbb{N}$ tal que $a + n = b$. Luego $(a, b) = (a, a + n)$. Entonces $cl(a, a + n) = cl(0, n)$. Luego si $a < b$, la clase de (a, b) tiene un representante de la forma $(0, n)$
- (b) Sea $a > b$. Luego $\exists n \in \mathbb{N}$ tal que $a = b + n$. Luego $(a, b) = (b + n, b)$. Pero $cl(b + n, b) = cl(n, 0)$. Entonces si $a > b$, la clase de (a, b) tiene un representante de la forma $(n, 0)$
- (c) Sea $a = b$. Luego $cl(a, b) = cl(a, a) = cl(0, 0)$. Entonces si $a = b$, la clase (a, b) tiene un representante de la forma $(0, 0)$.

Notaciones: La $cl(n, 0)$ será denotada por n . La $cl(0, n)$ será denotada por $-n$ y la $cl(0, 0)$ será denotada por 0 .

Se define: $\mathbb{Z} = \mathbb{N} \times \mathbb{N}/R$, donde cada elemento de \mathbb{Z} es una clase de equivalencia de $\mathbb{N} \times \mathbb{N}$

3. **Construcción de \mathbb{Q} .** En $\mathbb{Z} \times \mathbb{Z}$ hemos definido la relación:

$$(a, b)R(a', b') \text{ ssi } a \cdot b' = b \cdot a'$$

Solución. Nosotros vimos que R es una relación de equivalencia. Busquemos el representante más simple posible de cada clase. La clase $cl(a, b)$ será denotada $\frac{a}{b}$

Si a y b no son primos entre sí, entonces existe $k \in \mathbb{Z}$ tal que $a = ka'$ y $b = kb'$ con a' y b' primos entre sí. Luego $\frac{a}{b} = \frac{ka'}{kb'} = \frac{a'}{b'}$. Se deduce que para cada clase se puede tomar un representante (a, b) con a y b relativamente primos, es decir, toda clase se puede escribir en la forma $\frac{a}{b}$ relativamente primos entre sí. Los elementos del conjunto cociente son llamados números racionales. Notación $\mathbb{Z} \times \mathbb{Z} / R = \mathbb{Q}$, llamado el conjunto de los números racionales.

4. **Números reales módulo 1.** En \mathbb{R} consideremos la relación de equivalencia siguiente:

$$rRr' \text{ ssi } r - r' \text{ es un entero}$$

Busquemos una representación de las clases de equivalencia y de su conjunto cociente.

Solución. Todo número real r' se puede escribir como $r' = r + n$, donde n es la parte entera de r' y $0 \leq r < 1$. Luego para cada clase de equivalencia hay un representante r tal que $0 \leq r < 1$. Además, dos números reales r, r' con $0 \leq r < r' < 1$, no pueden tener por diferencia un número entero, luego pertenecen a clases distintas. Por lo tanto el conjunto de los números reales r , $0 \leq r < 1$ contiene uno y sólo un representante de cada clase de equivalencia entre 0 y 1.

El conjunto cociente es llamado conjunto de los números reales módulo 1

5. En \mathbb{R}^2 , consideremos la relación R siguiente:

$$(x, y)R(u, v) \text{ ssi } x^2 + y^2 = u^2 + v^2$$

Demostremos que R es una relación de equivalencia y busquemos la clase de $(0, 0)$, $(1, 0)$, $(3, 4)$, (a, b) . Describamos además la partición de \mathbb{R}^2 según R .

Solución.

- (a) R es reflexiva. En efecto, $(x, y)R(x, y)$ ssi $x^2 + y^2 = x^2 + y^2$. Afirmación que es verdadera $\forall (x, y) \in \mathbb{R}^2$. Observemos que un elemento cualquiera de \mathbb{R}^2 no es un par (x, x) sino (x, y) .
- (b) R es simétrica. En efecto, $(x, y)R(u, v) \Rightarrow x^2 + y^2 = u^2 + v^2 \Rightarrow u^2 + v^2 = x^2 + y^2 \Rightarrow (u, v)R(x, y)$
- (c) R es transitiva. En efecto, $(x, y)R(u, v) \wedge (u, v)R(s, t) \Rightarrow x^2 + y^2 = u^2 + v^2 \wedge u^2 + v^2 = s^2 + t^2 \Rightarrow x^2 + y^2 = s^2 + t^2 \Rightarrow (x, y)R(s, t)$

Por (a), (b) y (c) R es una relación de equivalencia.

Busquemos la clase del elemento $(0, 0)$. En efecto, $(x, y)R(0, 0)$ ssi $x^2 + y^2 = 0^2 + 0^2$ ssi $x^2 + y^2 = 0$ ssi $x = 0 \wedge y = 0$. Luego $cl(0, 0) = \{(0, 0)\}$.

Busquemos la clase del elemento $(1, 0)$. Tenemos $(x, y)R(1, 0)$ ssi $x^2 + y^2 = 1^2 + 0^2$ ssi $x^2 + y^2 = 1$ ssi (x, y) pertenece a la circunferencia con centro en $(0, 0)$ y con radio 1. Luego

$$cl(1, 0) = C((0, 0), 1) = \{(x, y); x^2 + y^2 = 1\}$$

Busquemos la clase del elemento $(3, 4)$. En efecto, $(x, y)R(3, 4)$ ssi $x^2 + y^2 = 3^2 + 4^2$ ssi $x^2 + y^2 = 25$. Luego

$$cl(3, 4) = C((0, 0), 5) = \{(x, y); x^2 + y^2 = 25\}$$

Busquemos la clase de un elemento (a, b) cualquiera.

En efecto $(x, y)R(a, b)$ ssi $x^2 + y^2 = a^2 + b^2$. Entonces

$$cl(a, b) = C((0, 0), \sqrt{a^2 + b^2}) = \{(x, y); x^2 + y^2 = a^2 + b^2\}$$

Esta relación R , produce la partición de \mathbb{R}^2 , formada por todas las circunferencias con centro en $(0, 0)$. Al mirar \mathbb{R}^2 se ve como un tranquilo lago al cual le tiramos una piedra.

6. Sea $A = \{a \in \mathbb{Z}; -30 < a < 45\}$ y R la relación de equivalencia en A definida por:

$$xRy \text{ ssi } x^2 + y = y^2 + x$$

Determinemos la clase de equivalencia de un elemento cualquiera de A y luego determinemos todas las clases de equivalencia en A .

Solución. Busquemos la clase de a , $a \in A$. En efecto,

$$\begin{aligned} xRa & \text{ ssi } x^2 - x = a^2 - a \\ & \text{ ssi } x^2 - x - (a^2 - a) = 0 \\ & \text{ ssi } x^2 - x + a(1 - a) = 0 \\ & \text{ ssi } (x - a)(x - (1 - a)) = 0 \\ & \text{ ssi } x = a \vee x = 1 - a \end{aligned}$$

Luego $cl(a) = \{a, 1 - a\}$

Entonces $cl(0) = \{0, 1\}$, $cl(-1) = \{-1, 2\}$, $cl(-2) = \{-2, 3\}$, ..., $cl(-30) = \{-30, 31\}$, $cl(32) = \{32\}$, $cl(33) = \{33\}$, ..., $cl(45) = \{45\}$.

Hay 31 clases con 2 elementos cada una y 14 clases con un único elemento, luego hay un total de 45 clases de equivalencia.

7. Consideremos una relación R en \mathbb{R}^2 , definida por

$$(x, y)R(z, t) \text{ ssi } x = z$$

Demostremos que R es una relación de equivalencia. Encontremos la $cl(\pi, 3)$ y de un elemento cualquiera (a, b) y describamos el conjunto cuociente.

Solución.

- (a) R es refleja. En efecto, $(x, y)R(x, y)$, pues $x = x \forall (x, y) \in \mathbb{R}^2$.
- (b) R es simétrica pues, $(x, y)R(z, t) \Rightarrow x = z \Rightarrow (z, t)R(x, y)$.
- (c) R es transitiva. En efecto, $(x, y)R(z, t) \wedge (z, t)R(u, v) \Rightarrow x = z \wedge z = u \Rightarrow x = u \Rightarrow (x, y)R(u, v)$.

Busquemos la clase de $(\pi, 3)$. Tenemos $(x, y)R(\pi, 3)$ ssi $x = \pi$. Luego $cl(\pi, 3) = \{(\pi, x); x \in \mathbb{R}\}$. Corresponde a la recta que pasa por $(\pi, 0)$ y es paralela al eje Y

Busquemos la clase de un elemento cualquiera (a, b) .

Tenemos $(x, y)R(a, b)$ ssi $x = a$, luego $cl(a, b) = \{(a, y); y \in \mathbb{R}\}$, es decir la recta paralela al eje Y que pasa por el punto $(a, 0)$.

El conjunto cuociente, es el conjunto formado por todas las rectas paralelas al eje Y . es decir si miramos \mathbb{R}^2/R , veremos el plano cartesiano formado por todas las rectas paralelas al eje Y , llenando todo \mathbb{R}^2 . Ahora \mathbb{R}^2 no son puntos. En cada punto del eje X , pasa una de estas rectas.

8. En el conjunto de los números reales, se define la relación S de la manera siguiente:

$$aSb \text{ ssi } a^4 - b^4 = a^2 - b^2$$

Demostremos que S es una relación de equivalencia. Determinemos la $cl(0)$, $cl(1)$. Demostremos que $cl(x) = cl(-x)$

Solución. Es más fácil escribir: $aSb \text{ ssi } a^4 - a^2 = b^4 - b^2$

- (a) S es refleja, pues $aSa \text{ ssi } a^4 - a^2 = a^4 - a^2$ lo cual es verdadero $\forall a \in \mathbb{R}$
- (b) S es simétrica, pues $aSb \text{ ssi } a^4 - a^2 = b^4 - b^2 \text{ ssi } b^4 - b^2 = a^4 - a^2 \text{ ssi } bSa$.
- (c) S es transitiva. En efecto: $aSb \wedge bSc \Rightarrow a^4 - a^2 = b^4 - b^2 \wedge b^4 - b^2 = c^4 - c^2 \Rightarrow a^4 - a^2 = c^4 - c^2 \Rightarrow aSc$

Por (a), (b) y (c) se tiene que S es una relación de equivalencia.

Busquemos la clase del elemento 0. Tenemos $aS0 \text{ ssi } a^4 - a^2 = 0^4 - 0^2 \text{ ssi } a^4 - a^2 = 0 \text{ ssi } a^4 = a^2 \text{ ssi } a = 0, 1, -1$. Luego $cl(0) = \{0, 1, -1\}$

Busquemos la clase del 2. Tenemos $aS2 \text{ ssi } a^4 - a^2 = 16 - 4 \text{ ssi } a^4 - a^2 - 12 = 0 \text{ ssi } (a^2 - 4)(a^2 + 3) = 0 \text{ ssi } (a^2 = 4 \vee a^2 = -3) \Rightarrow a^2 = 4 \Rightarrow a = 2 \vee a = -2 \Rightarrow cl(2) = \{2, -2\}$

Demostremos que $cl(x) = cl(-x)$. En efecto $xS-x$ pues $x^4 - x^2 = (-x)^4 - (-x)^2$, $\forall x \in \mathbb{R}$, es decir x está relacionado con $-x$, $\forall x \in \mathbb{R}$ por lo tanto están en la misma clase.

9. Sean R_1 y R_2 dos relaciones sobre un conjunto E . Se define

$$R_1 \wedge R_2 \Leftrightarrow (x(R_1 \wedge R_2)y) \Leftrightarrow (xR_1y \wedge xR_2y)$$

$$R_1 \vee R_2 \Leftrightarrow (x(R_1 \vee R_2)y) \Leftrightarrow (xR_1y \vee xR_2y)$$

Estudiemos las propiedades de la conjunción y la disyunción de las relaciones según las propiedades de R_1 y R_2

Solución. Estudiemos $R_1 \wedge R_2$

- (a) Sean R_1 y R_2 reflejas, luego xR_1x y $xR_2x \forall x \in E$, luego $xR_1 \wedge R_2x \forall x \in E$. Luego $R_1 \wedge R_2$ es refleja.

- (b) Sean R_1 y R_2 simétricas, luego $x(R_1 \wedge R_2)y \Rightarrow xR_1y \wedge xR_2y \Rightarrow (yR_1x \wedge yR_2x) \Rightarrow y(R_1 \wedge R_2)x$. Luego $R_1 \wedge R_2$ es simétrica.
- (c) Sean R_1 y R_2 transitivas, luego $x(R_1 \wedge R_2)y \wedge y(R_1 \wedge R_2)z \Rightarrow (xR_1y \wedge xR_2y) \wedge (yR_1z \wedge yR_2z) \Rightarrow (xR_1y \wedge yR_1z) \wedge (xR_2y \wedge yR_2z) \Rightarrow xR_1z \wedge xR_2z \Rightarrow x(R_1 \wedge R_2)z$. Luego $R_1 \wedge R_2$ es transitiva.

Estudiamos $R_1 \vee R_2$

- (a) Sean R_1 y R_2 reflejas, luego $xR_1x \wedge xR_2x \forall x \in E \Rightarrow xR_1x \vee xR_2x \forall x \in E \Rightarrow x(R_1 \vee R_2)x \forall x \in E$. Luego $R_1 \vee R_2$ es refleja.
- (b) Sean R_1 y R_2 simétricas, luego $x(R_1 \vee R_2)y \Rightarrow (xR_1y \vee xR_2y) \Rightarrow yR_1x \vee yR_2x \Rightarrow y(R_1 \vee R_2)x$
- (c) $R_1 \vee R_2$ no es transitiva. Contraejemplo: Sea $R_1 = \{(x, y)\}$ $R_2 = \{(y, z)\}$. Tenemos xR_1y , luego $x(R_1 \vee R_2)y$. También tenemos yR_2z , luego tenemos $y(R_1 \vee R_2)z$ sin embargo no se tiene $x(R_1 \vee R_2)z$

4.6 Relaciones de orden

Observación. Consideremos el conjunto

$$A = \{1, 2, 3, 4, 5, 6, 8, 10, 12, 40, 120\}$$

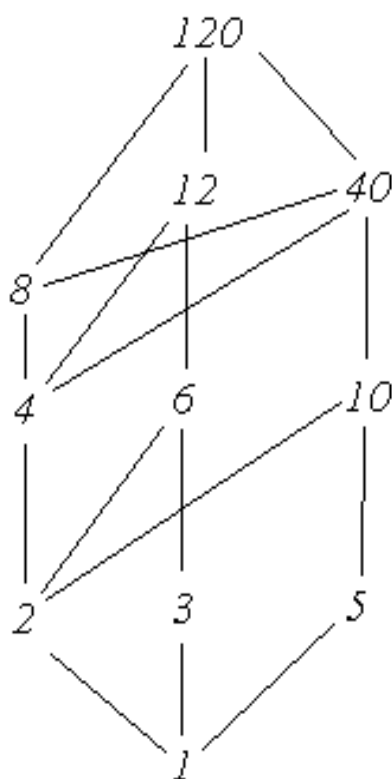
En A definamos la siguiente relación

$$aRb \text{ ssi } a \text{ divide a } b$$

Veamos sus propiedades y cierto diagrama para representar la relación.

1. R es refleja pues $xRx, \forall x \in \mathbb{R}$
2. R es antisimétrica. En efecto, si $x|y \wedge y|x \Rightarrow x = y$
3. R es transitiva. $x|y \wedge y|z \Rightarrow x|z$

Una forma visual muy agradable de entender es el llamado "diagrama de Hasse". Este diagrama supone la transitividad y la reflexividad.



Observemos que hay un "orden". Esto se diferencia de las relaciones de equivalencia, debido a la antisimetría. Esta observación nos inspira la definición siguiente:

Definición 4.6.1 Una relación R en A , es llamada **Relación de orden en A** , si es simultáneamente

refleja, antisimétrica y transitiva

Un conjunto A provisto de una relación de orden R , es llamado **conjunto ordenado por R**

Ejemplos

1. La relación " \leq " es una relación de orden en \mathbb{R} .
2. Sean $A = \{1, 2, 3\}$ y $P(A)$ su conjunto potencia. La inclusión \subset es una relación de orden en $P(A)$. Recordemos que

$$P(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, A\}$$

Observación. Consideremos \mathbb{Z} con la relación " \leq ". Observamos que cada vez que tomamos dos elementos de \mathbb{Z} , estos están relacionados. es decir:

$$a, b \in \mathbb{Z} \Rightarrow a \leq b \vee b \leq a$$

Esta observación nos inspira la siguiente definición

Definición 4.6.2 Sea A un conjunto y R una relación de orden en A . Si todos los elementos están relacionados entre sí, diremos que R es una **relación de orden total**. Es decir, R es una relación de orden total si

$$\forall x, y \in A \text{ se tiene } xRy \text{ o } yRx$$

En caso contrario diremos que es una **relación de orden parcial**.

Ejemplo. En el caso que tomamos $A = \{1, 2, 3\}$ y consideramos la inclusión en $P(A)$, es una relación de orden parcial.

Nota. También se puede decir que $R \subset A \times A$ es una relación de orden parcial ssi: R es una relación de orden y

$$\exists x, y \in A \text{ tal que } x \not R y \wedge y \not R x$$

4.7 Ejercicios Propuestos

1. Sea $A = [1, 4] \subseteq \mathbb{R}$, $B = [0, 4] \subseteq \mathbb{R}$, $C = [0, 3] \subseteq \mathbb{R}$; $D = [1, 2] \subseteq \mathbb{R}$.

Dibuje en un diagrama $(A \times B) \cap (C \times D)$

2. Sean E, F dos conjuntos y $S_{E,F}$ definido por:

$$S_{E,F} = \{A \times B; A \subset E, B \subset F\}$$

Muestre que:

- a) $S_{E,F} \subset P(E \times F)$
 b) $S_{E,F} = P(E \times F) \Leftrightarrow E$ o F es un singleton.
 3. Sea $A = \{a, b, c\}$
 a) ¿ Cuántas relaciones se pueden establecer de A en A ?
 b) ¿ Cuántas reflexivas ? ¿ Simétricas ?
 c) Construya todas las relaciones de equivalencia posibles sobre A .

4. Sea $n \in \mathbb{N}$

$$xRy \iff \begin{cases} x = y \\ \sum_{k=0}^n x^k y^{n-k} = 1 \quad \text{si } x \neq y \end{cases}$$

Demuestre que R es una relación de equivalencia.

5. Sea $A = \{1, 2, 3, 4\}$. Determine los gráficos de las relaciones R, S , definidas en A por (i) $aRb \iff a + b \leq 4$, (ii) $aSb \iff a(b+1) \leq 6$

6. Las relaciones R_1 y R_2 están definidas por

(i) $xR_1y \iff -10 \leq x + 5y \leq 10$

(ii) $xR_2y \iff x^2 + y^2 \leq 4, x \geq y$

Haga un gráfico de estas relaciones.

7. Discuta la reflexividad, simetría, antisimetría y transitividad de las siguientes relaciones en el conjunto $\{a, b, c\}$:
- (i) $\{(a, a), (b, b)\}$ (ii) $\{(c, c), (c, b)\}$ (iii) $\{(a, a), (a, b), (b, a), (b, b)\}$
(iv) $\{(a, a), (b, b), (c, c)\}$ (v) $\{(a, a), (b, b), (c, c), (a, b), (b, a)\}$
8. Sobre $\mathbb{R} \times \mathbb{R}$, discuta las relaciones siguientes:
- (a) $\{(a, b) \in \mathbb{R} \times \mathbb{R}; a^2 + b^2 \geq 0\}$
(b) $\{(a, b) \in \mathbb{R} \times \mathbb{R}; 0 < ab < 1\}$
9. Estudie si la relación en \mathbb{Z} definida por $aRb \iff ab \geq 0$ es una relación de equivalencia.
10. En \mathbb{Z} definimos: $aRb \iff a^2 + a = b^2 + b$. Demuestre que R es una relación de equivalencia y encuentre las clases de equivalencia de los elementos 0, 1 y a .
11. Consideremos $P(A)$, donde A es un conjunto. En $P(A)$ se define una relación como sigue: ARB ssi $A \subset B$. Determine si R es una relación de orden.
12. Sea $A \neq \emptyset$ y R una relación en A . Se dice que R es circular si $(x, y) \in R$ y $(y, z) \in R$ entonces $(z, x) \in R$. Demuestre que si R es refleja y circular, entonces R es simétrica.

Capítulo 5

Funciones

En este capítulo pondremos la atención en un tipo muy particular de relaciones entre dos conjuntos. Una función se determina dando dos conjuntos y asociando a cada elemento del primer conjunto, un único elemento del segundo conjunto. Una función puede no estar definida por una expresión aritmética, ni analítica. Lo importante es que asocie a los elementos del primer conjunto, elementos del segundo conjunto.

5.1 Definiciones básicas

Definición 5.1.1 Sea $R \subset A \times B$. Diremos que R es una **función** de A en B , si a cada elemento x de A , se le hace corresponder un único elemento y de B .

Notación. Usaremos generalmente las letras minúsculas f, g, h , para denotar las funciones y escribiremos

$$(x, y) \in f \text{ ssi } f(x) = y$$

En vez de escribir $f \subset A \times B$, usaremos la notación

$$f : A \rightarrow B; f(x) = y$$

A es llamado el **dominio de f** , denotado $\text{Dom}(f)$. B es llamado el **codominio de f** . También A puede ser llamado el conjunto de partida y B el conjunto de llegada. Las palabras "transformación" y "aplicación" son utilizadas como simónimos de la palabra función.

Definición 5.1.2 Sea $f : A \rightarrow B$. Si $f(x) = y$, diremos que y es la **imagen** de x por f o el valor de f en x . Diremos que x es la **preimagen** de y . El conjunto formado por todas las imágenes de los elementos de A por f será denotado $\text{Im}(f)$, $f(A)$ o $\text{Rec}(f)$, se define por:

$$\text{Im}(f) = \{y \in B, \exists x \in A; f(x) = y\}$$

Llamado conjunto imagen de f o recorrido de f .

Notación

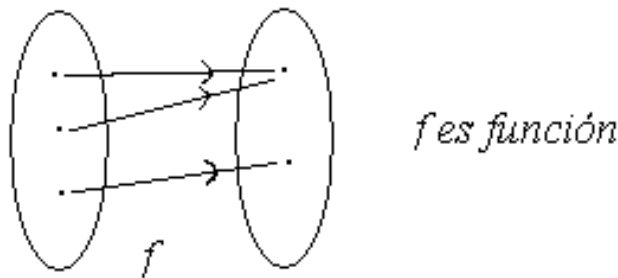
Sea $f : A \rightarrow B$, una función. Sea $X \subset A$, tenemos la siguiente notación:

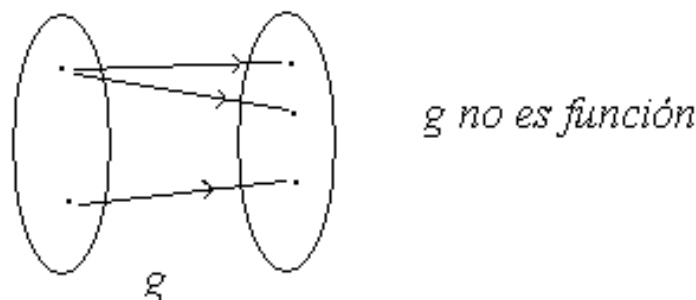
$$f(X) = \{f(x); x \in X\}$$

Observación. Las funciones deben estar definidas para todo elemento del conjunto de partida. Por ejemplo en el caso particular $A = \{1, 2\}$, $B = \{a, b, c\}$ y $f = \{(1, a), (1, b)\}$. Entonces f no es función pues el 2 no tiene imagen y también porque el 1 tiene dos imágenes.

Nota. Dos elementos distintos pueden tener la misma imagen. Por ejemplo para $f : \mathbb{Z} \rightarrow \mathbb{Z}; f(n) = |n|$. Se tiene que $f(n) = f(-n)$, con $n \neq -n \forall n \in \mathbb{Z}^*$. En este caso f es una función.

Ejemplo. Veamos gráficamente un caso en que una relación f es función y una relación g que no es función.





Ejemplos

- Sean $A = \{1, 2, 3\}$, $B = \{a, b, c, d\}$ y $f = \{(1, a), (2, b), (3, d)\}$.
Notación: $f : A \rightarrow B$. Se tiene $Dom(f) = \{1, 2, 3\}$, $Codom(f) = B$ y $Im(f) = \{a, b, d\}$

- Sea $s : \mathbb{N} \rightarrow \mathbb{N}$; $s(n) = n + 1$. Con $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.

$Dom(s) = \mathbb{N}$, pues a todo número natural se le puede sumar

- El 0 no tiene preimagen, luego $Im(s) = \mathbb{N}^* = \mathbb{N} - \{0\}$;
 $Codom(s) = \mathbb{N}$

- Sean $A = \{1, 2, 3\}$ y $f : P(A) \rightarrow P(A)$; $f(X) = X \cap \{2\}$.

Recordemos que $P(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, A\}$

Busquemos la imagen de f .

$$\begin{aligned} f(\emptyset) &= \emptyset \cap \{2\} = \emptyset; & f(\{1\}) &= \{1\} \cap \{2\} = \emptyset \\ f(\{2\}) &= \{2\} \cap \{2\} = \{2\}; & f(\{3\}) &= \emptyset \\ f(\{1, 2\}) &= \{1, 2\} \cap \{2\} = \{2\}; & f(\{1, 3\}) &= \emptyset \\ f(\{2, 3\}) &= \{2\}; & f(A) &= \{2\} \end{aligned}$$

Entonces $Im(f) = \{\emptyset, \{2\}\}$

- Sean $A = \{1, 2, 3\}$, $f : P(A) \rightarrow P(A)$; $f(X) = X \cup \{2\}$.

Entonces $Im(f) = \{\{2\}, \{1, 2\}, \{3, 2\}, A\}$; $Dom(f) = P(A)$

5. Sean $A = \{1, 2, 3\}$ y $h: P(A) \rightarrow P(A)$; $h(X) = X - \{2\}$. Tenemos

$$\begin{aligned} h(\emptyset) &= \emptyset - \{2\} = \emptyset; & h(\{1\}) &= \{1\} - \{2\} = \{1\} \\ h(\{2\}) &= \{2\} - \{2\} = \emptyset; & h(\{3\}) &= \{3\} - \{2\} = \{3\} \\ h(\{1, 2\}) &= \{1, 2\} - \{2\} = \{1\}; & h(\{1, 3\}) &= \{1, 3\} \\ h(\{2, 3\}) &= \{3\}; & h(A) &= A - \{2\} = \{1, 3\} \end{aligned}$$

Luego $Im(h) = \{\emptyset, \{1\}, \{3\}, \{1, 3\}\}$. $Dom(h) = P(A)$

6. Sea $f: \mathbb{N} \rightarrow \mathbb{N}$, definida por:

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

Tenemos que $Dom(f) = \mathbb{N}$ y $Im(f) = \{2n; n \in \mathbb{N}\} = 2\mathbb{N}$

7. Sea $f: \mathbb{N} \rightarrow \mathbb{N}$, definida por:

$$f(n) = \begin{cases} n+3; & \text{si } n \text{ es múltiplo de } 3 \\ n; & \text{si } n \text{ no es múltiplo de } 3 \end{cases}$$

Tenemos que $Dom(f) = \mathbb{N}$ y $Im(f) = \mathbb{N}^*$

8. Idem ejercicio anterior, pero $f: \mathbb{Z} \rightarrow \mathbb{Z}$.

Si $m \in Codom(f)$ y m un múltiplo de 3, se tiene $f(m-3) = m$.

Si m no es un múltiplo de 3, entonces se tiene $f(m) = m$. Luego $Im(f) = \mathbb{Z}$

9. Sea $f: P(\mathbb{N}) \rightarrow P(\mathbb{N})$, definida por $f(X) = X \cap A$, donde $A = \{4n; n \in \mathbb{N}\}$. Entonces $Dom(f) = P(\mathbb{N})$ y $Im(f) = \{B \in P(\mathbb{N}); B \text{ contiene sólo múltiplos de } 4\}$. Es decir, es el conjunto formado por todos los conjuntos que solamente tienen múltiplos de 4.

10. Sea $f: \mathbb{N} \rightarrow \mathbb{N}$ definido por:

$$f(n) = \begin{cases} \frac{n}{2}; & \text{si } n \text{ es par} \\ \frac{n+3}{2}; & \text{si } n \text{ es impar} \end{cases}$$

$Im(f) = \mathbb{N}$, pues dado $m \in Codom(f) = \mathbb{N}$, $\exists 2m \in \mathbb{N}$ tal que $f(2m) = \frac{2m}{2} = m$. Al menos tiene a $2m$ como preimagen, pero además puede venir de un número impar, a saber: $f(2m-3) = \frac{(2m-3)+3}{2} = \frac{2m}{2} = m$, siempre que $m \geq 2$.

11. Sean $A = \{0, 1, \dots, 99\}$ y $f : A \rightarrow A$; tal que $f(a) = |a - 99|$.
Tenemos que $Dom(f) = A$ y $Im(f) = A$; En efecto, sea $b \in A$, entonces $f(99 - b) = |(99 - b) - 99| = |-b| = b$, pues $b \geq 0$.
12. Sea $s : P_f(\mathbb{N}) \rightarrow \mathbb{N}$, donde $P_f(\mathbb{N})$ denotará los subconjuntos finitos de \mathbb{N} sin repetir números. Se define s por:

$$s(\{a_1, a_2, \dots, a_n\}) = a_1 + a_2 + \dots + a_n$$

$Dom(s) = P_f(\mathbb{N})$ y $Im(s) = \mathbb{N}$, pues dado $n \in \mathbb{N}$, basta tomar $\{n\} \in P_f(\mathbb{N})$ y se tiene $s(\{n\}) = n$

13. Sean $A = \{1, 2, \dots, n\}$ y $f : A \rightarrow A$; $f(k) = n - k + 1$.
Sea $m \in Codom(f) = A$, entonces $f(n+1-m) = n - (n+1-m) + 1 = m$. Además tenemos que $1 \leq m \leq n$, luego $-1 \geq -m \geq -n$, luego $-1 + n + 1 \geq n + 1 - m \geq n + 1 - n$, luego $n \geq n + 1 - m \geq 1$.
Luego $Im(f) = A$

14. Sea $f : \mathbb{Z} \rightarrow \mathbb{Z}$, definida por

$$f(z) = \begin{cases} -1; & \text{si } z < 0 \\ 0; & \text{si } z = 0 \\ 1; & \text{si } z > 0 \end{cases}$$

Llamada la función signo. En este caso $Dom(f) = \mathbb{Z}$ y $Im(f) = \{-1, 0, 1\}$.

15. Sea $\mathcal{X}_{\mathbb{Z}} : \mathbb{R} \rightarrow \mathbb{R}$ tal que

$$\mathcal{X}_{\mathbb{Z}}(x) = \begin{cases} 1; & \text{si } x \in \mathbb{Z} \\ 0; & \text{si } x \notin \mathbb{Z} \end{cases}$$

Llamada la función cacterística de \mathbb{Z} . $Dom(\mathcal{X}_{\mathbb{Z}}) = \mathbb{R}$, $Codom(\mathcal{X}_{\mathbb{Z}}) = \mathbb{R}$ e $Im(\mathcal{X}_{\mathbb{Z}}) = \{0, 1\}$

16. Función de Dirichlet. Sea $f : \mathbb{R} \rightarrow \mathbb{R}$, definida por:

$$f(x) = \begin{cases} 1; & \text{si } x \text{ es racional} \\ 0; & \text{si } x \text{ no es racional} \end{cases}$$

En este caso $Dom(f) = \mathbb{R}$ y $Im(f) = \{0, 1\}$

17. Sea $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}; f(a, b) = a + b + 2ab$. Estudiemos el dominio y recorrido de f .

(a) $Dom(f) = \mathbb{Z} \times \mathbb{Z}$, pues a todo par de números (a, b) enteros se les puede efectuar la operación: $a + b + 2ab$.

(b) $Rec(f) = \mathbb{Z}$. en efecto, dado $z \in \mathbb{Z}$, tenemos que $f(0, z) = 0 + z + 2 \cdot 0 \cdot z = z$, luego $f(0, z) = z$

18. Sea $f : \mathbb{N} \rightarrow \mathbb{N}$ tal que

$$f(n) = \begin{cases} 3n; & \text{si } n \text{ es par} \\ n + 1; & \text{si } n \text{ es impar} \end{cases}$$

$Dom(f) = \mathbb{N}$, pues todo número par puede ser multiplicado por 3 y a todo número impar se le puede sumar 1.

Veamos ahora su recorrido. Si n es impar, entonces $f(n)$ es par. Por esto, $Rec(f)$ contiene todos los números pares, menos el 0. Si n es par, $f(n)$ contiene todos los múltiplos de 6, los cuales también son pares, incluyendo el 0. Luego $Rec(f) = \{2n; n \in \mathbb{N}\}$

Definición 5.1.3 Sean A y B dos conjuntos y $f, g : A \rightarrow B$ funciones. Diremos que f es **igual a** g , denotado $f = g$ ssi

1. $Dom(f) = Dom(g)$

2. $f(a) = g(a), \forall a \in A$

Ejemplos

1. Sean $f, g : \mathbb{R} \rightarrow \mathbb{R}; f(x) = (x + 1)(x - 1); g(x) = x^2 - 1$. Entonces se tiene que $f = g$

2. Sean $f, g : \mathbb{R} \rightarrow \mathbb{R}; f(x) = \frac{x^2-1}{x+1}; g(x) = x - 1$. $Dom(f) = \mathbb{R} - \{-1\}$, $Dom(g) = \mathbb{R}$. Luego $f \neq g$, a pesar de tener $f(x) = g(x)$, $\forall x \in \mathbb{R} - \{-1\}$.

5.2 Propiedades de una función

Proposición 5.2.1 *Sea $f : A \rightarrow B$ una función. Sean X e Y dos subconjuntos cualesquiera de A , entonces*

1. Si $X \subset Y$ entonces $f(X) \subset f(Y)$
2. $f(X \cup Y) = f(X) \cup f(Y)$
3. $f(X \cap Y) \subset f(X) \cap f(Y)$

Demostración.

1. Sea $z \in f(X)$, luego $z = f(x)$, cierto $x \in X$, luego $z = f(x)$, cierto $x \in Y$, pues $X \subset Y$ luego $z \in f(Y)$
2. Demostremos que $f(X \cup Y) \subset f(X) \cup f(Y)$. En efecto sea $y \in f(X \cup Y)$, luego $y = f(x)$, algún $x \in X \cup Y$, luego $y = f(x)$, algún $x \in X$ o $x \in Y$, luego $y \in f(X)$ o $y \in f(Y)$, luego $y \in f(X) \cup f(Y)$.

Demostremos ahora que $f(X) \cup f(Y) \subset f(X \cup Y)$.

En efecto sea $y \in f(X) \cup f(Y)$, luego $y = f(x)$, cierto $x \in X$ o $y = f(t)$; $t \in Y$, luego $y = f(x)$; $x \in X \cup Y$ o $y = f(t)$; $t \in X \cup Y$, luego $y \in f(X \cup Y)$.

3. En efecto, sea $y \in f(X \cap Y)$, luego $y = f(x)$, cierto $x \in X \cap Y$, es decir, $y = f(x)$, cierto $x \in X$ y $x \in Y$, luego $y \in f(X) \cap f(Y)$.

Observación. No se tiene necesariamente $f(X) \cap f(Y) \subset f(X \cap Y)$. Por ejemplo consideremos

$$f : \mathbb{Z} \rightarrow \mathbb{Z}; f(n) = |n|$$

Sea $X = \{-2, -1, 0\}$, $Y = \{0, 1, 2\}$. Tenemos que $X \cap Y = \{0\}$, $f(X) = \{0, 1, 2\}$, $f(Y) = \{0, 1, 2\}$ y $f(X) \cap f(Y) = \{0, 1, 2\} \not\subset \{0\} = f(X \cap Y)$

5.3 Imagen recíproca

Observación. Sea $f : \mathbb{Z} \rightarrow \mathbb{Z}; f(n) = |n|$. Consideremos $Y = \{0, 1, 2\} \subset \text{Codom}(f)$. Estamos interesados en todos los elementos de $\text{Dom}(f)$ que tienen por imagen un elemento de Y . Tenemos que $f^{-1}(Y) = \{-2, -1, 0, 1, 2\}$. Diremos que $f^{-1}(Y)$ es la "imagen recíproca de Y por f ".

Entonces tenemos la definición siguiente:

Definición 5.3.1 Sea $f : A \rightarrow B$ una función. Sea $Y \subset B$. Se llama **imagen recíproca de Y por f** o **preimagen de Y por f** , al subconjunto de A definido por:

$$f^{-1}(Y) = \{x \in A; f(x) \in Y\} = \{x \in A; \exists y \in Y \text{ tal que } y = f(x)\}$$

Es decir: $x \in f^{-1}$ ssi $f(x) \in Y$. También se dice: $f^{-1}(Y)$ es la **imagen inversa de Y por f**

Proposición 5.3.1 Sea $f : A \rightarrow B$ una función. Sean X e Y dos subconjuntos cualesquiera de B , entonces

1. $X \subset Y \Rightarrow f^{-1}(X) \subset f^{-1}(Y)$
2. $f^{-1}(X \cup Y) = f^{-1}(X) \cup f^{-1}(Y)$
3. $f^{-1}(X \cap Y) = f^{-1}(X) \cap f^{-1}(Y)$
4. $f^{-1}(X - Y) = f^{-1}(X) - f^{-1}(Y)$

Demostración.

1. $x \in f^{-1}(X) \Rightarrow f(x) \in X \Rightarrow f(x) \in Y$ (pues $X \subset Y$) $\Rightarrow x \in f^{-1}(Y)$.

2. (a) Tenemos

$$\begin{aligned} x \in f^{-1}(X \cup Y) &\Rightarrow f(x) \in X \cup Y \\ &\Rightarrow f(x) \in X \text{ o } f(x) \in Y \\ &\Rightarrow x \in f^{-1}(X) \text{ o } x \in f^{-1}(Y) \\ &\Rightarrow x \in f^{-1}(X) \cup f^{-1}(Y) \end{aligned}$$

- (b) $X \subset X \cup Y$ y $Y \subset X \cup Y \Rightarrow f^{-1}(X) \subset f^{-1}(X \cup Y)$ y $f^{-1}(Y) \subset f^{-1}(X \cup Y)$.

Luego $f^{-1}(X) \cup f^{-1}(Y) \subset f^{-1}(X \cup Y)$.

3. (a) En efecto,

$$\begin{aligned} x \in f^{-1}(X) \cap f^{-1}(Y) &\Rightarrow x \in f^{-1}(X) \text{ y } x \in f^{-1}(Y) \\ &\Rightarrow f(x) \in X \text{ y } f(x) \in Y \\ &\Rightarrow f(x) \in X \cap Y \\ &\Rightarrow x \in f^{-1}(X \cap Y) \end{aligned}$$

- (b) $X \cap Y \subset X$ y $X \cap Y \subset Y$. Por la proposición anterior, $f^{-1}(X \cap Y) \subset f^{-1}(X)$ y $f^{-1}(X \cap Y) \subset f^{-1}(Y)$. Luego $f^{-1}(X \cap Y) \subset f^{-1}(X) \cap f^{-1}(Y)$

4. (a) Tenemos

$$\begin{aligned} x \in f^{-1}(X - Y) &\Rightarrow f(x) \in X - Y \\ &\Rightarrow f(x) \in X \text{ y } f(x) \notin Y \\ &\Rightarrow x \in f^{-1}(X) \text{ y } x \notin f^{-1}(Y) \\ &\Rightarrow x \in f^{-1}(X) - f^{-1}(Y) \end{aligned}$$

- (b) En efecto

$$\begin{aligned} x \in f^{-1}(X) - f^{-1}(Y) &\Rightarrow x \in f^{-1}(X) \text{ y } x \notin f^{-1}(Y) \\ &\Rightarrow f(x) \in X \text{ y } f(x) \notin Y \\ &\Rightarrow f(x) \in X - Y \\ &\Rightarrow x \in f^{-1}(X - Y) \end{aligned}$$

Definición 5.3.2 Sea $f : A \rightarrow B$ y sea $X \subset A$. Una función $g : X \rightarrow B$ tal que $g(x) = f(x) \forall x \in X$ es llamada la **restricción de f a X**. La función g se denota por $f|_X$. Luego la restricción de f a X es la función

$$f|_X : X \rightarrow B; f|_X(x) = f(x)$$

Definición 5.3.3 Sea $f : A \rightarrow B$ y sea $Y \supset A$. Entonces toda función $h : Y \rightarrow B$ tal que $h(y) = f(y) \forall y \in A$ es llamada una **extensión de f a Y**

Nota. Dada $f : A \rightarrow B$. La restricción de f a un subconjunto X de A es única, sin embargo hay más de una extensión a un conjunto Y que contenga a A .

Definición 5.3.4 Sea $f : A \rightarrow A$; tal que $f(a) = a; \forall x \in A$. Denotaremos esta función, $f = id_A$ y será llamada la **función identidad** de A .

5.4 Inyectividad, epiyectividad y biyectividad

Observación. Sea $A = \{a, b, c\}$, $B = \{1, 2\}$ y $f = \{(a, 1), (b, 1), (c, 2)\}$. Debido a que a y b tienen la misma imagen, diremos que f no es inyectiva. Es decir una función deja de ser inyectiva cuando dos elementos distintos tienen la misma imagen.

Definición 5.4.1 Sea $f : A \rightarrow B$. Diremos que f es **inyectiva** si

$$x \neq y \Rightarrow f(x) \neq f(y)$$

Nota. La proposición $(x \neq y \Rightarrow f(x) \neq f(y))$ es lógicamente equivalente a la proposición $(f(x) = f(y) \Rightarrow x = y)$. Para comprender el concepto es más evidente la primera versión y para demostrar que una función es inyectiva es preferible la segunda versión.

Ejemplo. Sea $f : \mathbb{R} \rightarrow \mathbb{R}; f(x) = x^2$. Tenemos que $f(-2) = 4$ y $f(2) = 4$. Luego f no es inyectiva. Sin embargo, la función $g : \mathbb{R}_0^+ \rightarrow \mathbb{R}; g(x) = x^2$ es inyectiva. En efecto, si $g(x_1) = g(x_2)$, entonces $x_1^2 = x_2^2$. Luego $x_1 = x_2$, de donde g es inyectiva.

Observación. Sean $A = \{a, b, c\}$, $B = \{1, 2\}$ y $f = \{(a, 1), (b, 1), (c, 1)\}$. Diremos que esta función no es epiyectiva pues el 2 no tiene preimagen. Es decir una función deja de ser epiyectiva cuando hay un elemento en el codominio que no tiene preimagen. Tenemos la definición siguiente:

Definición 5.4.2 Sea $f : A \rightarrow B$ una función. Diremos que

f **epiyectiva** si $\forall b \in B, \exists a \in A$ tal que $f(a)=b$

Ejemplo. Sea $f : \mathbb{R} \rightarrow \mathbb{R}; f(x) = x^2$. Se tiene que f no es epiyectiva. Un contraejemplo es $\nexists x \in \mathbb{R}$ tal que $f(x) = -5$.

Sin embargo $g : \mathbb{R} \rightarrow \mathbb{R}_0^+; g(x) = x^2$ es epiyectiva, pues dado $y \in \mathbb{R}_0^+$, siempre existe $x \in \mathbb{R}$ tal que $g(x) = y$, pues si tomamos $x = \sqrt{y}$, se tiene $f(\sqrt{y}) = (\sqrt{y})^2 = y$, pues $y \geq 0$.

Definición 5.4.3 Sea $f : A \rightarrow B$ una función. Diremos que f es **biyectiva** ssi f es inyectiva y epiyectiva.

Ejemplo. Sea $f : \mathbb{R} \rightarrow \mathbb{R}; f(x) = 7x + 1$

1. f es inyectiva. En efecto: $f(x_1) = f(x_2) \Rightarrow 7x_1 + 1 = 7x_2 + 1 \Rightarrow x_1 = x_2$
2. f es epiyectiva. En efecto: dado $y \in \text{Codom}(f)$, supongamos que existe $x \in \mathbb{R}$ tal que $f(x) = y$. Luego $7x + 1 = y$, luego $x = \frac{y-1}{7}$. Luego $f(\frac{y-1}{7}) = y$. De donde f es epiyectiva.

5.5 Composición de funciones

Observación. Sean A, B, C, D cuatro conjuntos,

$$f : A \rightarrow B, \quad g : C \rightarrow D$$

tal que $\text{Im}(f) \subset \text{Dom}(g)$. A todo $x \in A$, le corresponde un único $y \in B$ tal que $f(x) = y$. A este $y \in \text{Im}(f)$ (luego $y \in \text{Dom}(g)$), le corresponde un único $z \in D$ tal que $z = g(y)$. Tenemos entonces $z = g(y) = g(f(x))$. Y así hemos definido una nueva función de A en D tal que a cada $x \in A$ le asocia $z = g(f(x))$ en D .

Definición 5.5.1 Esta nueva función es llamada **g compuesta con f**, se denota $g \circ f$. Es decir, $(g \circ f)(x) = g(f(x))$

Ejemplo. Sean $f, g : \mathbb{Z} \rightarrow \mathbb{Z}$; $f(x) = 2x - 5$, $g(x) = x^2$. Entonces $(g \circ f)(x) = g(f(x)) = g(2x - 5) = (2x - 5)^2 = 4x^2 - 20x + 25$ y $(f \circ g)(x) = f(g(x)) = f(x^2) = 2x^2 - 5$.

En este caso ambas proposiciones tienen sentido y ambas son diferentes.

Proposición 5.5.1 Sea $f : A \rightarrow B$ entonces

$$f \circ id_A = f \text{ y } id_B \circ f = f$$

Demostración. En efecto,

$$(f \circ id_A)(x) = f(id_A(x)) = f(x), \quad \forall x \in A$$

$$(id_B \circ f)(x) = id_B(f(x)) = f(x), \quad \forall x \in A$$

Luego $f \circ id_A = f$ y $id_B \circ f = f$.

Observe que las dos primeras igualdades ocurren en B y las otras dos igualdades son igualdades de funciones.

Nota. La composición de funciones no es conmutativa.

Contraejemplo: Sean $f, g : \mathbb{Z} \rightarrow \mathbb{Z}$; $f(n) = n^2$ y $g(n) = n + 3$.

Entonces $(g \circ f)(n) = g(f(n)) = g(n^2) = n^2 + 3$.

Por otra parte $(f \circ g)(n) = f(g(n)) = f(n + 3) = (n + 3)^2$. Luego $g \circ f \neq f \circ g$

Nota. En general no tiene sentido la composición inversa. Observemos el caso siguiente: $f, g : \mathbb{Q}^* \rightarrow \mathbb{Q}$; $f(r) = \frac{2}{r}$, $g(r) = 0$. Entonces $(g \circ f)(r) = 0$ y $f \circ g$ no tiene sentido.

5.6 Función inversa

Nota. La relación inversa de una función no es necesariamente una función. Solamente en el caso de una función biyectiva podemos hablar de una función inversa.

Definición 5.6.1 Se llama **función inversa de una función biyectiva** $f : A \rightarrow B$, denotada f^{-1} , a la función $f^{-1} : B \rightarrow A$ tal que a cada elemento $b \in B$ le hace corresponder el único elemento $a \in A$ cuya imagen por f es b . Es decir $f^{-1}(b) = a$ ssi $f(a) = b$. En el caso que la función inversa exista, diremos que f es invertible.

Ejemplo. Sean $A = \{1, 2, 3\}$, $B = \{a, b, c\}$ y $f = \{(1, b), (2, c), (3, a)\}$ es biyectiva, luego existe f^{-1} . Esta es $f^{-1} = \{(b, 1), (c, 2), (a, 3)\}$

Ejemplo. Consideremos la función biyectiva $f : \mathbb{R} \rightarrow \mathbb{R}$; $f(x) = 2x - 3$. Busquemos su función inversa.

Como f es biyectiva, luego existe su función inversa f^{-1} . Si $f(x) = 2x - 3$, entonces $f^{-1}(2x - 3) = x$. Escribámosla más elegante: Sea $y = 2x - 3$, luego $x = \frac{y+3}{2}$. Luego $f^{-1}(y) = \frac{y+3}{2}$ o también podemos escribir $f^{-1}(x) = \frac{x+3}{2}$

Nota. Sea $f : A \rightarrow B$ biyectiva. Puesto que $f^{-1} : B \rightarrow A$ también es una función biyectiva, podemos hablar de su función inversa, denotada $(f^{-1})^{-1} : A \rightarrow B$. Tenemos $(f^{-1})^{-1}(x) = y$ ssi $f^{-1}(y) = x$ ssi $f(x) = y$ $\forall x \in A$. Luego $(f^{-1})^{-1}(x) = f(x) \forall x \in A$. Luego $(f^{-1})^{-1} = f$.

Proposición 5.6.1 Sea $f : A \rightarrow B$ una función biyectiva. Entonces $f^{-1} \circ f = id_A$ y $f \circ f^{-1} = id_B$

Demostración. Sea $f(x) = y$, luego $f^{-1}(y) = x$. Entonces

$$(f^{-1} \circ f)(x) = f^{-1}(f(x)) = f^{-1}(y) = x = id_A(x) \quad \forall x \in A$$

Por otra parte,

$$(f \circ f^{-1})(y) = f(f^{-1}(y)) = f(x) = y = id_B(y) \quad \forall y \in B$$

Luego $f^{-1} \circ f = id_A$ y $f \circ f^{-1} = id_B$.

Proposición 5.6.2 (Caracterización de función inversa)

Sean $f : A \rightarrow B$ y $g : B \rightarrow A$ biyectivas. Entonces

$$f \circ g = id_B \text{ y } g \circ f = id_A \text{ ssi } g = f^{-1}$$

Demostración. Sea $g = f^{-1}$, entonces por la proposición anterior tenemos que $f \circ g = id_B$ y $g \circ f = id_A$.

Por otra parte, sea $f \circ g = id_B$ y $g \circ f = id_A$. Por demostrar

$$g(y) = f^{-1}(y) \quad \forall y \in B$$

es decir, por demostrar,

$$g(y) = x \Leftrightarrow f^{-1}(y) = x \Leftrightarrow f(x) = y$$

es decir, por demostrar

$$g(y) = x \Leftrightarrow f(x) = y$$

En efecto,

$$g(y) = x \Leftrightarrow f(g(y)) = f(x) \Leftrightarrow (f \circ g)(y) = f(x)$$

Pero $f \circ g = id_A$, luego $id_A(y) = f(x) \Leftrightarrow y = f(x)$.

Ejemplo. Sea $f : \mathbb{R} \rightarrow \mathbb{R}; f(x) = 2x + 5$. Esta función es biyectiva. Calculemos su función inversa, f^{-1} , utilizando el resultado recién obtenido.

$$(f \circ f^{-1})(x) = x \Rightarrow f(f^{-1}(x)) = x \Rightarrow 2f^{-1}(x) + 5 = x \Rightarrow f^{-1}(x) = \frac{x-5}{2}$$

Ejemplo. Sea $s : \mathbb{N} \rightarrow \mathbb{N}^*; s(n) = n + 1$. La función sucesor en \mathbb{N} . Busquemos s^{-1} .

En efecto, $s(s^{-1}(n)) = id_{\mathbb{N}}(n) = n, n \in \mathbb{N}^*$; luego $s^{-1}(n) + 1 = n$, luego $s^{-1}(n) = n - 1, n \in \mathbb{N}^*$ y tiene sentido pues $n > 0$.

Ejemplo. Sea X un conjunto y $P(X)$ su conjunto potencia. Sea $f : P(X) \rightarrow P(X); f(X) = \overline{X}$, donde \overline{X} denota el complemento de X . Esta función es biyectiva, luego podemos buscar su función inversa. Se tiene $(f \circ f)(X) = f(\overline{X}) = \overline{\overline{X}} = X$. Luego $f^{-1} = f$.

Teorema 5.6.3 Consideremos las tres funciones siguientes:

$$f : A \rightarrow B; \quad g : B \rightarrow C; \quad h : C \rightarrow D$$

tales que

$$\text{Im}(f) \subset \text{Dom}(g), \text{Im}(g) \subset \text{Dom}(h)$$

y las funciones compuestas siguientes:

$$g \circ f : A \rightarrow C; \quad h \circ (g \circ f) : A \rightarrow D; \quad h \circ g : B \rightarrow D; \quad (h \circ g) \circ f : A \rightarrow D$$

Entonces

1. $\text{Dom}(h \circ (g \circ f)) = \text{Dom}((h \circ g) \circ f)$ (Igualdad de conjuntos).
2. $h \circ (g \circ f) = (h \circ g) \circ f$ (Igualdad de funciones).

Demostración. La parte 1 es evidente por lo tanto demostraremos sólo 2. En efecto

$$(h \circ (g \circ f))(a) = h((g \circ f)(a)) = h(g(f(a))), \quad \forall a \in A$$

Por otra parte

$$((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h(g(f(a))) \quad \forall a \in A$$

Luego $(h \circ g) \circ f = h \circ (g \circ f)$. Puesto que la composición es asociativa podemos obviar los paréntesis y escribir simplemente $h \circ g \circ f$

Proposición 5.6.4 (Composición de funciones epiyectivas) Sean $f : A \rightarrow B$ y $g : B \rightarrow C$ con $\text{Im}(f) \subset \text{Dom}(g)$ epiyectivas, entonces la función $g \circ f : A \rightarrow C$ es epiyectiva.

Demostración. Sea $c \in C$. Puesto que g es epiyectiva, entonces $c = g(b)$, cierto $b \in B$. Puesto que f es epiyectiva $b = f(a)$, cierto $a \in A$. Luego $c = g(b) = g(f(a)) = (g \circ f)(a)$. Luego $g \circ f$ es epiyectiva.

Proposición 5.6.5 (Composición de funciones inyectivas) Sean $f : A \rightarrow B$ y $g : B \rightarrow C$ con $\text{Im}(f) \subset \text{Dom}(g)$ inyectivas, entonces la función $g \circ f : A \rightarrow C$ es inyectiva.

Demostración. En efecto

$$(g \circ f)(a) = (g \circ f)(b) \Rightarrow g(f(a)) = g(f(b)) \Rightarrow f(a) = f(b) \Rightarrow a = b$$

Luego $g \circ f$ es inyectiva.

Proposición 5.6.6 (Composición de funciones biyectivas) Sean $f : A \rightarrow B$ y $g : B \rightarrow C$ biyectivas tal que $\text{Im}(f) \subset \text{Dom}(g)$, entonces la función compuesta $g \circ f : A \rightarrow C$ también es biyectiva.

Demostración

Se obtiene de las dos proposiciones anteriores.

Proposición 5.6.7 Sean $f : A \rightarrow B$, $g : B \rightarrow C$, ambas biyectivas, tal que $\text{Im} \subset \text{Dom}(g)$, entonces la función inversa de $g \circ f : A \rightarrow C$, denotada por $(g \circ f)^{-1}$, es la siguiente:

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

Demostración. La función $g \circ f : A \rightarrow C$ es biyectiva, luego existe su función inversa:

$$\begin{aligned} (g \circ f) \circ (f^{-1} \circ g^{-1}) &= g \circ (f \circ f^{-1}) \circ g^{-1} \\ &= g \circ \text{id}_B \circ g^{-1} \\ &= (g \circ \text{id}_B) \circ g^{-1} \\ &= g \circ g^{-1} \\ &= \text{id}_C \end{aligned}$$

Por otra parte, tenemos:

$$\begin{aligned} (f^{-1} \circ g^{-1}) \circ (g \circ f) &= f^{-1} \circ (g^{-1} \circ g) \circ f \\ &= f^{-1} \circ \text{id}_B \circ f \\ &= f^{-1} \circ f \\ &= \text{id}_A \end{aligned}$$

Por la caracterización de función inversa, tenemos que:

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

5.7 Funciones biyectivas sobre conjuntos finitos o permutaciones

Observación. Consideremos un conjunto formado por tres elementos. Por ejemplo $I_3 = \{1, 2, 3\}$. Nuestra primera tarea será encontrar todas las funciones biyectivas en I_3 . Denotémoslas por f_1, f_2, \dots, f_6

1. Sea f_1 definida por $f_1(1) = 1, f_1(2) = 2, f_1(3) = 3$. Para escribir más simplificado, usemos la siguiente notación:

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

2. Sea f_2 definida por $f_2(1) = 1, f_2(2) = 3, f_2(3) = 2$. Escribimos:

$$f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

3. Sea f_3 definida por: $f_3(1) = 2, f_3(2) = 1, f_3(3) = 3$. Escribimos:

$$f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

4. Definamos $f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

¡Obvio que no hay más funciones biyectivas ! Cada una de estas funciones es llamada una **permutación**. Diremos que f_1, f_2, \dots, f_6 son todas las permutaciones de I_3 . Sea $G_I = \{f_1, f_2, f_3, f_4, f_5, f_6\}$

Observación. Consideremos el conjunto de tres elementos

$$B_3 = \{*, \triangle, \square\}$$

Queremos encontrar todas las funciones biyectivas de B_3 .

Denotémoslas por g_1, g_2, \dots, g_6 . Las definimos como sigue:

$$g_1 = \begin{pmatrix} * & \triangle & \square \\ * & \triangle & \square \end{pmatrix}, g_2 = \begin{pmatrix} * & \triangle & \square \\ * & \square & \triangle \end{pmatrix}, g_3 = \begin{pmatrix} * & \triangle & \square \\ \triangle & * & \square \end{pmatrix}$$

$$g_4 = \begin{pmatrix} * & \triangle & \square \\ \triangle & \square & * \end{pmatrix} g_5 = \begin{pmatrix} * & \triangle & \square \\ \square & * & \triangle \end{pmatrix} g_6 = \begin{pmatrix} * & \triangle & \square \\ \square & \triangle & * \end{pmatrix}$$

No hay más permutaciones. Entonces el conjunto formado por todas las permutaciones de B_3 es $G_B = \{g_1, g_2, g_3, g_4, g_5, g_6\}$

Observación. G_I tiene el mismo comportamiento que G_B .

Definición 5.7.1 S_3 denotará el conjunto formado por todas las permutaciones de un conjunto formado por 3 elementos.

5.7.1 Permutaciones de I_n

Consideremos un conjunto formado por n elementos $I_n = \{1, 2, \dots, n\}$. Denotemos por S_n el conjunto formado por todas las biyecciones de I_n en I_n . Estas biyecciones son llamadas permutaciones de n elementos.

Notación: $f : I_n \rightarrow I_n$ será denotada

$$f = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$$

Existe una permutación identidad, denotada id y está definida por

$$id = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{pmatrix}$$

Dada la permutación

$$f = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ f(1) & f(2) & f(3) & \dots & f(n) \end{pmatrix}$$

existe f^{-1} definida por:

$$f^{-1} = \begin{pmatrix} f(1) & f(2) & f(3) & \dots & f(n) \\ 1 & 2 & 3 & \dots & n \end{pmatrix}$$

Ejemplo. Sea $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$

$$\text{Entonces } f^{-1} = \begin{pmatrix} 4 & 2 & 1 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

Definición 5.7.2 La composición de estas funciones biyectivas será llamada producto de permutaciones.

Ejemplo. Sea $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$ y $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$

$$g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$$

$$(g \circ f)(4) = g(f(4)) = g(3) = 1; \text{ es decir, } 4 \mapsto 3 \mapsto 1$$

$$(g \circ f)(3) = g(f(3)) = g(1) = 3; \text{ es decir, } 3 \mapsto 1 \mapsto 3$$

$$(g \circ f)(2) = g(f(2)) = g(2) = 4; \text{ es decir, } 2 \mapsto 2 \mapsto 4$$

$$(g \circ f)(1) = g(f(1)) = g(4) = 2; \text{ es decir, } 1 \mapsto 4 \mapsto 2$$

Notación: f^n denotará $f \circ f \circ \cdots \circ f$, n veces

Ejemplos

1. Sea $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$. Encontremos n tal que $f^n = id$ y luego calculemos f^{200} .

En efecto

$$f^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

$$f^3 = f^2 \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = id$$

Usando el hecho que $f^3 = id$, podemos calcular fácilmente varias composiciones de f consigo misma. Por ejemplo:

Calculemos f^{200} . Tenemos que $200 = 3 \cdot 66 + 2$. Luego

$$f^{200} = f^{3 \cdot 66 + 2} = (f^3)^{66} f^2 = id^{66} \cdot f^2 = f^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

2. Sean $f, g \in S_5$ definidas por

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 2 & 3 \end{pmatrix} \quad y \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 5 & 1 \end{pmatrix}$$

Busquemos $h \in S_5$ de manera que $g = h \circ f$.

En efecto, para obtener las imágenes de h lo hacemos de la manera siguiente:

$$\begin{aligned} g(5) = 1; f(5) = 3, \text{ luego } h(3) = 1. \text{ Así } g(5) &= (h \circ f)(5) \\ g(4) = 5; f(4) = 2, \text{ luego } h(2) &= 5 \\ g(3) = 2; f(3) = 4; \text{ luego } h(4) &= 2 \\ g(2) = 4; f(2) = 1; \text{ luego } h(1) &= 4 \\ g(1) = 3; f(1) = 5; \text{ luego } h(5) &= 3 \end{aligned}$$

Luego tenemos:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 5 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 2 & 3 \end{pmatrix}$$

También podríamos haber hecho el cálculo de la manera siguiente:

$$g = h \circ f \Rightarrow g \circ f^{-1} = h. \text{ Tenemos}$$

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

3. Sea $\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix}$. Busquemos el menor $n \in \mathbb{N}$, tal que $\theta^n = id$. Además busquemos el valor de $\theta^{2.001}$ y θ^{-1}

En efecto

$$\theta^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 3 & 2 \end{pmatrix}$$

$$\theta^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix}$$

$$\theta^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 5 & 1 \end{pmatrix}$$

$$\theta^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 5 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

Luego $\theta^5 = id$ y 5 es el menor número que cumple esta condición.

Busquemos $\theta^{2.001}$. Se tiene que $2.001 = 5 \cdot 400 + 1$. Luego $\theta^{2.001} = \theta^{5 \cdot 400 + 1} = (\theta^5)^{400} \cdot \theta^1 = id^{400} \cdot \theta = \theta$.

Luego $\theta^{2.001} = \theta$.

5.8 Funciones sobre conjuntos finitos

5.8.1 Propiedades

Principio del palomar o principio de los casilleros

Si se tienen n nidos y m palomas y $m > n$ (más palomas que nidos), entonces hay al menos dos palomas que ocupan el mismo nido.

Ejemplo. Si hay 8 personas entonces hay al menos dos personas que nacieron el mismo día de la semana.

Proposición 5.8.1 Sea $f : A \rightarrow B$; $|A| = m$, $|B| = n$ y $m < n$. Entonces f no puede ser epiyectiva.

Demostración. Supongamos que f es epiyectiva. Como a B llegan al menos n flechas, entonces hay al menos n flechas que parten desde A . Luego hay al menos un elemento de A del cual parten dos flechas. Luego f no es función. Lo cual es una contradicción. Luego f no es epiyectiva.

Proposición 5.8.2 Sea $f : A \rightarrow B$; $|A| = m$, $|B| = n$ y $m > n$. Entonces f no puede ser inyectiva.

Demostración. En A hay m elementos, luego parten m flechas desde A , luego llegan a B m flechas. Puesto que $m > n$ entonces hay al menos dos flechas que llegan al mismo elemento en B . Luego f no es inyectiva.

Proposición 5.8.3 Si f biyectiva entonces $|A| = |B|$

Demostración Sea f biyectiva. En A hay m elementos. Luego parten m flechas desde A , Luego llegan m flechas a B . Puesto que f es inyectiva hay m elementos en la imagen. Por ser epiyectiva, en el Codominio hay m elementos. Luego $|A| = |B|$

Proposición 5.8.4 (Todo o nada) Sea $f : A \rightarrow B$; Si $|A| = n$, $|B| = n$ (es decir A y B tienen el mismo número de elementos) Entonces

f es epiyectiva ssi f es inyectiva.

Demostración.

Sea $|A| = |B| = n$ entonces

1. Sea f epiyectiva. Por demostrar que f es inyectiva.

En A y en B hay la misma cantidad de elementos. Puesto que f es epiyectiva, entonces llegan al menos n flechas a B . Luego parten al menos n flechas desde A y puesto que en A hay exactamente n elementos, entonces no puede haber dos elementos que tengan la misma imagen, luego f es inyectiva.

2. Sea f inyectiva. Por demostrar que f epiyectiva. En A hay n elementos, luego parten n flechas. Puesto que f es inyectiva, llegan n flechas a B a elementos distintos. Como en B hay exactamente n elementos distintos, se tiene que f es epiyectiva.

Observación. Sean $I = \{1, 2, 3\}$, $f : P(I) \rightarrow \{n, s\} \times \{n, s\} \times \{n, s\}$, definida por:

Esta función es biyectiva. Luego en el dominio y en el codominio hay la misma cantidad de elementos. Luego $|P(I)|$ tiene 2^3 elementos.

En general se tiene la proposición siguiente:

Proposición 5.8.5 Existe una biyección de $P(I)$ en $\{n, s\}^m$ donde $I = \{1, 2, \dots, m\}$

Demostración. Sea $f : P(I) \rightarrow \{n, s\}^m$; definida por

$$f(\{i_1, i_2, \dots, i_p\}) = x = (x_1, x_2, \dots, x_m)$$

donde, $x_k = s$ ssi $k \in \{i_1, i_2, \dots, i_p\}$ y $x_k = n$ ssi $k \notin \{i_1, i_2, \dots, i_p\}$

1. Demostremos que f es epiyectiva. Dado $x = (x_1, x_2, \dots, x_m) \in \{n, s\}^m$, le asociamos el subconjunto $X = \{i \in I; x_i = s\}$.

Por ejemplo. Sea $(n, s, s, n, s, n, s, n, \dots, n) \in \{n, s\}^m$. Entonces existe X tal que $f(\{2, 3, 5, 7\}) = (n, s, s, n, s, n, s, n, \dots, n)$

2. Demostremos que f es inyectiva. Sean

$$f(\{i_1, i_2, \dots, i_p\}) = (x_1, x_2, \dots, x_m) \text{ y}$$

$$f(\{j_1, j_2, \dots, j_q\}) = (y_1, y_2, \dots, y_m)$$

Supongamos $f(\{i_1, i_2, \dots, i_p\}) = f(\{j_1, j_2, \dots, j_q\})$,

luego $(x_1, x_2, \dots, x_p) = (y_1, y_2, \dots, y_q)$, es decir $x_k = y_k$, luego $i_k = j_k \forall k \in \{1, 2, \dots, p\}$, de donde f es inyectiva.

Corolario 5.8.6 Sea $I = \{1, 2, \dots, m\}$. Entonces $|P(I)| = 2^m = 2^{|I|}$

Demostración. $|P(I)| = |\{n, s\}^m| = 2^m = 2^{|I|}$

Proposición 5.8.7 El número de subconjuntos de un conjunto finito A es $2^{|A|}$

Demostración. Sea A un conjunto tal que $|A| = m$. Luego existe una biyección

$$f : A \rightarrow I = \{1, 2, \dots, m\}$$

Luego $|P(A)| = P(I) = 2^m = 2^{|A|}$

5.8.2 Número de funciones entre dos conjuntos finitos

Observación. Sea $A = \{1, 2\}$, $B = \{a, b, c\}$. Buscamos el número de funciones que se pueden tener de A en B . Tenemos:

La imagen de 1 puede ser obtenida de 3 maneras diferentes. La imagen de 2 también se puede obtener de tres maneras diferentes. Luego el número de funciones distintas de A en B es 3^2

Observación. Sea $A = \{1, 2, 3\}$ y $B = \{a, b\}$. La imagen de 1 puede ser elegida de 2 maneras diferentes. Idem para 2 y para 3. Luego el número de funciones distintas de A en B es 2^3 .

Veamos otra manera de obtener este resultado. Consideremos $F(A, B) = \{f : A \rightarrow B\}$. Construyamos una biyección:

$$\varphi : F(A, B) \rightarrow B \times B \times B$$

definida por $\varphi(f(a_1, a_2, a_3)) = (f(a_1), f(a_2), f(a_3))$

Luego $|F(A, B)| = 2^3$. Por ejemplo la función f tal que $f(1) = a$, $f(2) = a$, $f(3) = b$ es llevada al trío (a, a, b) . En general, la función f tal que $f(1) = x$, $f(2) = y$, $f(3) = z$ es llevada al trío (x, y, z) , donde $x, y, z \in \{a, b\}$

Proposición 5.8.8 Sea $|A| = m$, $|B| = n$. Entonces el número de funciones de A en B es n^m .

Demostración. Sea

$$\varphi : F(A, B) \rightarrow B^m; \quad f \mapsto \varphi(f)$$

tal que si

$$f(a_1) = b_{i_1}, f(a_2) = b_{i_2}, \dots, f(a_m) = b_{i_m}$$

Entonces

$$\varphi(f) = (b_{i_1}, b_{i_2}, \dots, b_{i_m}) \in B^m$$

Tenemos que φ es una biyección. Luego $|F(A, B)| = n^m$.

Observación. Sea $A = \{1, 2, 3\}$ y $B = \{a, b, c, d, e\}$. Buscamos el número de funciones inyectivas entre A y B .

El 1 tiene 5 posibles imágenes. El 2 tiene 4 posibles imágenes. El 3 tiene 3 posibles imágenes. Luego hay $5 \cdot 4 \cdot 3$ funciones inyectivas de A en B . Tenemos que $5 \cdot 4 \cdot 3$ puede ser escrito como sigue: $\frac{5!}{(5-3)!}$. Esto nos induce a la proposición siguiente:

Proposición 5.8.9 Sean A y B dos conjuntos finitos tal que $|A| = m$, $|B| = n$ y $|A| \leq |B|$. Entonces el número de funciones inyectivas de A en B es $\frac{n!}{(n-m)!}$.

Demostración. Para la primera componente hay n posibilidades. Para la segunda componente hay $n - 1$ posibilidades. Para la tercera componente hay $n - 2$ posibilidades, etc. Son m componentes luego hay $\frac{n!}{(n-m)!}$ funciones inyectivas.

Corolario 5.8.10 Si $|A| = |B| = n$. Entonces el número de funciones inyectivas es $n!$

Corolario 5.8.11 Sean A y B dos conjuntos tal que $|A| = m$, $|B| = n$ y $m \leq n$. Entonces existen $m!$ funciones inyectivas que tienen el mismo conjunto imagen.

Proposición 5.8.12 Sean A y B dos conjuntos tal que $|A| = m$, $|B| = n$ y $m \leq n$. Entonces el número de clases de funciones inyectivas con distinto conjunto imagen es $\binom{n}{m} = \frac{n!}{(n-m)!m!}$.

5.9 Algunas funciones sobre conjuntos no finitos

El sentido común nos dice que \mathbb{Z} tiene el doble de elementos que \mathbb{N} . Sin embargo en el infinito el sentido común falla. En efecto se tiene la siguiente proposición

Proposición 5.9.1 *Se puede establecer una biyección entre \mathbb{N} y \mathbb{Z} .*

Demostración. La función definida por $f : \mathbb{N} \rightarrow \mathbb{Z}$, tal que

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

es una función biyectiva.

Nota. Diremos que \mathbb{N} y \mathbb{Z} tienen el mismo cardinal, es decir el mismo número de elementos.

Ejercicio. Se puede establecer una biyección entre \mathbb{N} y el conjunto de los números naturales pares.

Solución. Construimos una biyección de la siguiente manera:

$$f : \mathbb{N} \rightarrow \{n \in \mathbb{N}; n \text{ es par}\}; f(n) = 2n.$$

Ejercicios Resueltos

1. Sea $f : P(\mathbb{N}) \rightarrow P(\mathbb{N}); f(X) = X \cup \{2\}$. Estudiemos esta función.

Solución. Tenemos que $Dom(f) = P(\mathbb{N})$, pues todo subconjunto de $P(\mathbb{N})$ puede ser unido al conjunto formado por el 2.

La $Im(f)$ es el conjunto formado por todos los subconjuntos de \mathbb{N} que contienen el 2.

Afirmación: f no es inyectiva. En efecto, podemos dar como contraejemplo $f(\{1, 2\}) = f(\{1\}) = \{1, 2\}$ y $\{1, 2\} \neq \{1\}$

Afirmación: f no es epiyectiva. Vimos que la imagen está formada por todos los subconjuntos que tiene el 2. Por ejemplo $\{3\}$ no tiene preimagen.

2. Sea $g : P(\mathbb{N}) \rightarrow P(\mathbb{N}); g(X) = X \cap \{2\}$. Estudiemos las propiedades de g .

Solución. $Dom(g) = \mathbb{N}$, pues todo subconjunto de \mathbb{N} puede ser intersectado con $\{2\}$.

Además $Im(g) = \{\emptyset, \{2\}\}$.

Afirmación: f no es inyectiva. En efecto $g(\{1, 2, 3, 5\}) = g(\{2, 7\}) = \{2\}$ y $\{1, 2, 3, 5\} \neq \{2, 7\}$.

Afirmación: g no es epiyectiva, pues $Im(g) = \{\emptyset, \{2\}\} \neq Codom(g)$ o bien Contraejemplo: dado $\{1\} \in Codom(g) = P(\mathbb{N})$, $\nexists X \in Dom(g)$ tal que $g(X) = \{1\}$

3. Sea $h : P(\mathbb{N}) \rightarrow P(\mathbb{N})$; $h(X) = X - \{2\}$. Estudiemos h .

Solución. $Dom(h) = P(\mathbb{N})$. El conjunto $Im(h)$ está formado por todos los subconjuntos de $P(\mathbb{N})$ que no contienen el número 2.

Afirmación: h no es inyectiva. En efecto $h(\{1, 2, 3\}) = h(\{1, 3\}) = \{1, 3\}$ y $\{1, 2, 3\} \neq \{1, 3\}$.

Afirmación: h no es epiyectiva. Vimos que $Im(h)$ es subconjunto estricto del $Codom(h)$, por ejemplo $\{2\} \in Codom(h)$ y $\nexists X \in Dom(h)$ tal que $h(X) = \{2\}$, es decir tal que $X - \{2\} = \{2\}$

4. Sea $f : P(\mathbb{N}) \rightarrow P(\mathbb{N})$ tal que $f(A) = A \cap B$, donde $B = \{x^2; x \in \mathbb{N}\}$. Estudiemos f .

Solución. $Dom(f) = P(\mathbb{N})$, pues todo conjunto de $P(\mathbb{N})$ puede ser intersectado con B . La $Im(f)$ es el conjunto formado por todos los subconjuntos que tienen solamente cuadrados perfectos.

f no es inyectiva. En efecto, $f(\{1, 2, 3, 5\}) = f(\{1, 2, 7, 8\}) = \{1\}$

f no es epiyectiva. En efecto, dado $\{1, 2, 3\} \in Codom(f) = P(\mathbb{N})$, $\nexists X \in Dom(f)$ tal que $f(X) = \{1, 2, 3\}$.

5. Sea $g : \mathbb{N} \rightarrow \mathbb{N}$ definida por $g(n) = n + 5$. Estudiemos si f es inyectiva o epiyectiva.

Solución. Estudiemos si es inyectiva. Sea $g(n) = g(m)$, luego $n + 5 = m + 5$, cancelando el 5, tenemos $n = m$. Es decir f es inyectiva.

Estudiemos si f es epiyectiva. Sea $m \in \mathbb{N}$ y supongamos que existe $n \in \mathbb{N}$ tal que $g(n) = m$, luego $n + 5 = m$. Observemos que los números 1, 2, 3, 4 no tienen preimagen. Luego f no es

epiyectiva. Podríamos haber pensado, cuándo $g(m - 5) = m$ tiene sentido.

6. Sea $f : \mathbb{N} \rightarrow \mathbb{N}$ definida por:

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

Estudiemus si f es inyectiva o epiyectiva.

Solución. Tenemos que f no es inyectiva. Contraejemplo: $f(4) = 8$ y $f(7) = 8$.

Además f no es epiyectiva, pues la imagen de f está formada por los números pares solamente y $\text{Codom}(f)$ es todo \mathbb{N} . $\text{Im}(f) = \{2m; m \in \mathbb{N}\} \neq \text{Codom}(f)$

7. Sea $f : \mathbb{Z} \rightarrow \mathbb{Z}$ tal que $f(n) = 4n^2 + 5$. Estudiemus si f es inyectiva. Busquemos $\text{Im}(f)$ y luego concluyamos si f es epiyectiva.

Solución. Tenemos que f no es inyectiva, pues $f(a) = f(-a)$, $\forall a \in \mathbb{Z}$.

Sea $m \in \text{Im}(f)$, luego $4n^2 + 5 = m$, cierto $n \in \mathbb{Z}$. Luego un número está en la imagen de f si al restarle 5 es 4 veces un cuadrado perfecto. Es decir $\text{Im}(f) = \{4n^2 + 5; n \in \mathbb{Z}\} \neq \mathbb{Z}$

8. Sea $f : \mathbb{N} \rightarrow \mathbb{N}$ definida por

$$f(n) = \begin{cases} n + 3; & \text{si } n \text{ es múltiplo de 3} \\ n; & \text{si } n \text{ no es múltiplo de 3} \end{cases}$$

Estudiemus si f es inyectiva o epiyectiva.

Solución. Estudiemus si f es inyectiva. Sea $f(n) = f(m)$, luego tenemos los casos siguientes:

- (a) Si n y m son múltiplos de 3, entonces $n + 3 = m + 3$.
Cancelando el 3, tenemos $n = m$
- (b) Si n es múltiplo de 3 y m no es múltiplo de 3, entonces $n + 3 = m$. Pero $n + 3$ también es un múltiplo de 3. Contradicción, luego no se tiene este caso.

- (c) Si n y m no son múltiplos de 3, entonces $n = m$.

Entonces f es inyectiva

f no es epiyectiva, pues no existe $n \in \mathbb{N}$ tal que $f(n) = 0$. Más aun $Im(f) = \mathbb{N}^*$

Nota. Si consideramos $f : \mathbb{Z} \rightarrow \mathbb{Z}$ con la misma escritura anterior entonces f es epiyectiva. En efecto, sea $m \in \mathbb{Z}$ entonces:

- (a) m es múltiplo de 3. Luego $f(m - 3) = m$, pues $m - 3$ también es múltiplo de 3.
- (b) m no es múltiplo de 3, entonces $f(m) = m$.
9. Sean $A = \{0, 1, 2, \dots, 99\}$ y $f : A \rightarrow A$ tal que $f(a) = |a - 99|$. Estudiemos si f es inyectiva o epiyectiva.

Solución. Puesto que $a \in A$, $a - 99 \leq 0$ y $|a - 99| = 99 - a$

- (a) Sea $f(a) = f(b)$, luego $99 - a = 99 - b$, luego $a = b$. Es decir f es inyectiva.
- (b) Sea $b \in A$. Supongamos que existe $a \in A$ tal que $f(a) = b$. Luego $99 - a = b$. Luego $a = 99 - b$. Pregunta ¿ $99 - b \in A$? En efecto $0 \leq b \leq 99$, luego $0 \geq -b \geq -99$. Sumemos 99. Tenemos $99 \geq 99 - b \geq 0$. Luego $99 - b \in A$ y $f(99 - b) = b$. Luego f es epiyectiva.
10. Sea $f : \mathbb{N} \rightarrow \mathbb{N}$, definida por:

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

Busquemos f^n

Solución.

- (a) Si n es par: $f^2(n) = f(n + 2) = (n + 2) + 2 = n + 2 \cdot 2$.
Si n es impar: $f^2(n) = f(n + 1) = (n + 1) + 2$
Si n es par: $f^3(n) = f(n + 2 \cdot 2) = (n + 2 \cdot 2) + 2 = n + 3 \cdot 2$
Si n es impar: $f^3(n) = f((n + 1) + 2) = ((n + 1) + 2) = ((n + 1) + 2) + 2 = (n + 1) + 2 \cdot 2$

(b) Hipótesis de inducción

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

(c) Por demostrar:

$$f^{m+1}(n) = \begin{cases} n + (m + 1) \cdot 2; & \text{si } n \text{ es par} \\ (n + 1) + m \cdot 2; & \text{si } n \text{ impar} \end{cases}$$

Si n es par:

$$f^{m+1}(n) = f(f^m(n)) = f(n + m \cdot 2) = (n + m) + 2 = n + (m + 1) \cdot 2$$

Si n es impar:

$$\begin{aligned} f^{m+1}(n) = f(f^m(n)) &= f((n + 1) + (m - 1) \cdot 2) \\ &= (n + 1) + (m - 1) \cdot 2 + 2 \\ &= (n + 1) + m \cdot 2 \end{aligned}$$

Por (a), (b) y (c) tenemos que la hipótesis de inducción es verdadera para todo número natural.

11. Sea A no vacío, $f : A \rightarrow A$, una función. Definimos $f^n : A \rightarrow A$, por medio de la recurrencia $f^0 = f$, $f^{n+1} = f^n \circ f$. Demostremos que:

(1) f biyectiva $\Rightarrow f^n$ biyectiva.

(2) f biyectiva $\Rightarrow (f^n)^{-1} = (f^{-1})^n$

Solución (1)

(a) Para $n = 2$ tenemos

$$\begin{aligned} f^2(x_1) = f^2(x_2) &\Rightarrow f(f(x_1)) = f(f(x_2)) \Rightarrow f(x_1) = f(x_2) \\ &\Rightarrow x_1 = x_2 \end{aligned}$$

Luego f^2 es inyectiva

(b) Hipótesis de inducción. Supongamos que f^n es inyectiva.

(c) Por demostrar que f^{n+1} es inyectiva.

$$\begin{aligned} f^{n+1}(x_1) = f^{n+1}(x_2) &\Rightarrow (f^n \circ f)(x_1) = (f^n \circ f)(x_2) \\ &\Rightarrow f^n(f(x_1)) = f^n(f(x_2)) \\ &\Rightarrow f(x_1) = f(x_2) \\ &\Rightarrow x_1 = x_2 \end{aligned}$$

Luego f^{n+1} es inyectiva.

Por (a), (b) y (c) tenemos que f^n es inyectiva $\forall n \in \mathbb{N}$. La epiyectividad queda de tarea.

Solución (2)

(a) $n = 1$ tenemos $(f^1)^{-1} = f^{-1} = (f^{-1})^1$

(b) Hipótesis de inducción. Supongamos que $(f^n)^{-1} = (f^{-1})^n$

(c) Por demostrar: $(f^{n+1})^{-1} = (f^{-1})^{n+1}$. En efecto,

$$(f^{-1})^{n+1} = (f^{-1})^n \circ f^{-1} = (f^n)^{-1} \circ f^{-1} = (f \circ f^n)^{-1} = (f^{n+1})^{-1}$$

Por (a), (b) y (c) tenemos que la proposición es válida para todo número natural n .

5.10 Ejercicios Propuestos

1. Para cada una de las funciones dadas, estudie: dominio, codominio, imagen, inyectividad y epiyectividad.

(a) $f : P(U) \rightarrow P(U)$; $f(X) = \overline{X}$, donde U es un conjunto.

(b) $g : \mathbb{Z} \rightarrow \mathbb{Z}$; $g(a) = a^2 + 1$.

(c) $s : \mathbb{N} \rightarrow \mathbb{N}$; $s(n) = n + 1$.

(d) $h : \mathbb{Z} \rightarrow \mathbb{Z}$ tal que $h(n) = 4n + 5$.

(e) $t : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$; $t(a, b) = a + b + 2ab$.

2. Sea $f_{a,b} : \mathbb{R} \rightarrow \mathbb{R}$; $f_{a,b}(x) = ax + b$. Determine $f_{a,b}^n$

3. Sea $f : \mathbb{Z} \rightarrow \mathbb{Z}$ una función con la propiedad siguiente:

$$f(n + m) = f(n) + f(m)$$

para cada par de enteros n y m

(a) Se define la relación R en \mathbb{Z} por:

$$nRm \Leftrightarrow f(n) = f(m)$$

Pruebe que R es una relación de equivalencia.

(b) Pruebe que $f(0) = 0$, recuerde para ello que $0 + 0 = 0$

(c) Pruebe que $f(-m) = -f(m); \forall m \in \mathbb{Z}$. Indicación use que $m - m = 0$.

4. Sea $A = \mathbb{R} \times \mathbb{R}^*$ y $f : A \rightarrow A$ tal que $f(a, x) = (ax, 2x)$. Demuestre que f es biyectiva.

5. Sea $f : \mathbb{R} \rightarrow \mathbb{R}; f(x) = x + 3$. Encuentre f^n , donde $n \in \mathbb{N}$.

6. Establezca una biyección entre:

(a) \mathbb{N} y $\{n \in \mathbb{N}; n \text{ es impar}\}$

(b) \mathbb{N} y $\{n^2; n \in \mathbb{N}\}$

(c) \mathbb{N} y $\{n^3; n \in \mathbb{N}\}$.

Capítulo 6

Estructuras Algebraicas

6.1 Ley de composición interna

En este capítulo vamos a trabajar con conjuntos y operaciones definidas en ellos. Estudiaremos algunas propiedades que cumplen en cada caso.

Por ejemplo estudiaremos \mathbb{N} y la suma ahí definida. O bien \mathbb{Z} con la suma o el producto ahí definidos.

Comencemos por estudiar algunos casos.

Observación. Cuando estudiamos las proposiciones lógicas, vimos que su valor de verdad podía ser Verdadero o Falso. Sea $B = \{F, V\}$. Pensemos en B con los conectivos " \vee " e " \wedge " separadamente.

\vee	V	F
V	V	V
F	V	F

\wedge	F	V
F	F	F
V	F	V

Puesto que al componer dos elementos de B obtenemos un elemento de B , diremos que " \vee " e " \wedge " son "leyes de composición interna de B ".

Observamos que (B, \vee) tiene el mismo comportamiento que (B, \wedge) , sólo que F y V hacen el comportamiento cambiado.

Observación. Consideremos $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$ con la operación suma:

+	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

Diremos que la suma es una "ley de composición interna" de \mathbb{Z}_2

Observación. Consideremos $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ sin el $\bar{0}$, es decir $\mathbb{Z}_3^* = \{\bar{1}, \bar{2}\}$ con la multiplicación siguiente:

\cdot	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{2}$	$\bar{1}$

Diremos que \cdot es una "ley de composición interna" de \mathbb{Z}_3^* . Observamos que $(\mathbb{Z}_2, +)$ tiene un comportamiento análogo a (\mathbb{Z}_3^*, \cdot) . Basta cambiar el $\bar{0}$ de \mathbb{Z}_2 por el $\bar{1}$ de \mathbb{Z}_3^* y el $\bar{1}$ de \mathbb{Z}_2 por el $\bar{2}$ de \mathbb{Z}_3^* .

Diremos que tienen la misma "estructura algebraica"

Definición 6.1.1 Sea A un conjunto no vacío. Diremos que $*$,

$$*: A \times A \longrightarrow A; (x, y) \rightarrow x * y$$

es una **ley de composición interna** en A , debido a que al componer dos elementos de A obtenemos un elemento de A . Abreviaremos simplemente l.c.i.

Definición 6.1.2 Un conjunto dotado de una ley de composición interna es llamado una **estructura algebraica**. Diremos que $(A, *)$ es una estructura algebraica.

También diremos que " A es cerrado para $*$ ".

Ejemplos

1. La multiplicación es una l.c.i. en \mathbb{N} . Diremos también que (\mathbb{N}, \cdot) es una estructura algebraica. O bien que \mathbb{N} es cerrado para la multiplicación.

2. La multiplicación es una l.c.i. en \mathbb{Z} , pues la multiplicación de dos números enteros es un número entero. O bien diremos que (\mathbb{Z}, \cdot) es una estructura algebraica, o bien diremos que \mathbb{Z} es cerrado para la multiplicación.
3. \mathbb{Z} no es cerrado para la división, pues la división de dos números enteros no es siempre un número entero. O bien, \mathbb{Z} con la división no es una estructura algebraica. O bien la división no es una l.c.i. en \mathbb{Z}
4. \mathbb{N} con la resta no es una estructura algebraica.
5. La multiplicación es una l.c.i. en \mathbb{Q} y también en \mathbb{R}

6.1.1 Propiedades de una l.c.i. en un conjunto

Definición 6.1.3 Diremos que una l.c.i. $*$ es **asociativa** en un conjunto A si

$$x * (y * z) = (x * y) * z; \quad \forall x, y, z \in A$$

Ejemplos

1. La multiplicación es una l.c.i. asociativa en \mathbb{Z} , pues

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c; \quad \forall a, b, c \in \mathbb{Z}$$

2. La resta no es asociativa en \mathbb{Z} . La elevación a potencia tampoco lo es. Contraejemplo

$$(2^2)^3 = 2^6; \quad 2^{(2^3)} = 2^8$$

Definición 6.1.4 Diremos que una l.c.i. $*$ es **conmutativa** en A si

$$x * y = y * x; \quad \forall x, y \in A$$

Ejemplos

1. La suma y la multiplicación son conmutativas en \mathbb{N} , \mathbb{Z} y \mathbb{Q}
2. La resta y la división no son conmutativas en \mathbb{N} , o bien en \mathbb{Z} , etc.

Definición 6.1.5 Dadas dos l.c.i. en A , $*$ y \triangleleft , entonces $*$ se distribuye con respecto a \triangleleft si

$$x * (y \triangleleft z) = (x * y) \triangleleft (x * z); \quad \forall x, y, z \in A$$

Ejemplos

1. En \mathbb{Z} tenemos que la suma y el producto son l.c.i. Ocurre que el producto se distribuye con respecto a la suma. Es decir:

$$a \cdot (b + c) = a \cdot b + a \cdot c; \quad \forall a, b, c \in \mathbb{Z}$$

2. En un conjunto formado por proposiciones lógicas, se tiene que \vee se distribuye con respecto a \wedge y recíprocamente \wedge se distribuye con respecto a \vee . En efecto:

$$p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$$

$$p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$$

3. Sea X un conjunto y $P(X)$ su conjunto potencia. En $P(X)$ se tiene

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C); \quad \forall A, B, C \in P(X)$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C); \quad \forall A, B, C \in P(X)$$

Es decir, la intersección se distribuye con respecto a la unión en $P(X)$ y en el segundo caso, la unión se distribuye con respecto a la intersección en $P(X)$

Definición 6.1.6 Una l.c.i. $*$ sobre A , admite un elemento neutro e si

$$e * x = x * e = x; \quad \forall x \in A$$

Ejemplos

1. El 0 es el neutro para la suma en \mathbb{Z} . El 1 es el neutro para el producto en \mathbb{Z} , pues

$$z + 0 = 0 + z = z; \quad \forall z \in \mathbb{Z}$$

$$1 \cdot z = z \cdot 1 = z; \quad \forall z \in \mathbb{Z}$$

2. Sea $A = \mathbb{R}^{\mathbb{R}} = \{\text{funciones}; f : \mathbb{R} \rightarrow \mathbb{R}\}$, entonces $id_{\mathbb{R}} : \mathbb{R} \rightarrow \mathbb{R}$ es el neutro para la composición en A . Se tiene

$$f \circ id_{\mathbb{R}} = id_{\mathbb{R}} \circ f = f; \quad \forall f \in A$$

3. Sea $A = \{e, a, b\}$ con la multiplicación dada por la siguiente tabla:

*	<i>e</i>	<i>a</i>	<i>b</i>
<i>e</i>	<i>e</i>	<i>a</i>	<i>b</i>
<i>a</i>	<i>a</i>	<i>b</i>	<i>e</i>
<i>b</i>	<i>b</i>	<i>e</i>	<i>a</i>

Entonces e es el neutro de la operación $*$.

4. Sea A un conjunto y $P(A)$ su conjunto potencia. Se tiene que

$$X \cup \emptyset = \emptyset \cup X = X; \quad \forall X \in P(A)$$

Luego \emptyset es el neutro para la unión en $P(A)$. Además

$$X \cap A = A \cap X = X; \quad \forall X \in P(A)$$

Luego A es el neutro para la intersección de conjuntos en $P(A)$.

5. En \mathbb{Z}_4 consideremos su producto, el cual vemos en la siguiente tabla:

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Luego en \mathbb{Z}_4 el 1 es el elemento neutro para el producto.

Definición 6.1.7 Un elemento $z \in A$ es llamado **cero** o **absorbente** en A con respecto a una l.c.i. $*$ si:

$$z * x = x * z = z; \quad \forall x \in A$$

Ejemplos

1. El 0 es absorbente con respecto a la multiplicación en \mathbb{Z} .

2. Sea A un conjunto y $P(A)$ su conjunto potencia.

El \emptyset es absorbente con respecto a la intersección de conjuntos.

Es decir:

$$X \cap \emptyset = \emptyset \cap X = \emptyset; \quad \forall X \in P(A)$$

Por otra parte, A es absorbente con respecto a la unión de conjuntos, es decir:

$$X \cup A = A \cup X = A; \quad \forall X \in P(A)$$

Definición 6.1.8 Un elemento $x \in A$ es llamado **idempotente** si:

$$x * x = x;$$

Ejemplos

1. El 1, en \mathbb{Z} , es un idempotente con respecto a la multiplicación, pues $1 \cdot 1 = 1$.

El 0 es un idempotente en \mathbb{Z} , con respecto a la suma pues $0 + 0 = 0$

2. Sea F un conjunto de proposiciones lógicas, entonces toda proposición en F es idempotente con respecto a la disyunción y a la conjunción. Es decir, para toda proposición $p \in F$ se tiene:

$$p \vee p = p; \quad p \wedge p = p$$

3. Sea A un conjunto. Todo $X \in P(A)$ es idempotente para la unión y la intersección:

$$X \cup X = X; \quad X \cap X = X$$

4. Sea $A = \{f; f : \mathbb{R} \rightarrow \mathbb{R}\}$. Se tiene que la función $id : \mathbb{R} \rightarrow \mathbb{R}; id(x) = x$ es idempotente en A con respecto a la composición de funciones, pues:

$$(id \circ id)(x) = id(id(x)) = id(x) = x; \quad \forall x \in A$$

Luego

$$id \circ id = id$$

Además

$$O : \mathbb{R} \rightarrow \mathbb{R}; O(x) = 0; \quad \forall x \in \mathbb{R}$$

Entonces la función O es idempotente en A , pues:

$$(O \circ O)(x) = O(O(x)) = O(0) = 0 = O(x); \quad \forall x \in A$$

Luego

$$O \circ O = O$$

Definición 6.1.9 Dado $x \in A$, diremos que $y \in A$ es **inverso** de x ssi

$$x * y = y * x = e$$

donde e es el neutro con respecto a la operación $*$.

Notación aditiva: $-x$; Notación multiplicativa x^{-1}

Ejemplos

1. Consideremos el conjunto $A = \{e, a, b\}$ y la operación $*$ definida por la tabla siguiente:

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

En este caso $a^{-1} = b$ y $b^{-1} = a$

2. En \mathbb{Z}_3^* con el producto dado por la tabla siguiente:

\cdot	1	2
1	1	2
2	2	1

En este caso $2^{-1} = 2$. Podemos escribir: $\frac{1}{2} = 2$

3. Consideremos (\mathbb{Z}_5^*, \cdot) , con el producto dado por la tabla sgte.:

\cdot	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Tenemos que $2^{-1} = 3$, $3^{-1} = 2$, $4^{-1} = 4$. También podemos escribir:

$$\frac{1}{2} = 3; \quad \frac{1}{3} = 2; \quad \frac{1}{4} = 4$$

4. (\mathbb{Z}_4, \cdot) es una estructura algebraica con producto definido por la tabla siguiente:

\cdot	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Entonces el 0 y el 2 no tienen inverso multiplicativo.

No existe $x \in \mathbb{Z}_4$ tal que $2 \cdot x = 1$. Idem para el 0. El inverso de 3 es 3, es decir, $3^{-1} = 3$ o bien $\frac{1}{3} = 3$.

5. Sea X un conjunto universo y sea $A \subset X$. Tenemos las tablas siguientes:

\cup	A	\emptyset	X
A	A	A	X
\emptyset	A	\emptyset	X
X	X	X	X

\cap	A	\emptyset	X
A	A	\emptyset	A
\emptyset	\emptyset	\emptyset	\emptyset
X	A	\emptyset	X

En el caso de la unión, el conjunto \emptyset es el neutro. X es absorbente. Son idempotentes X, A, \emptyset . En el caso de la intersección, X es neutro. Absorbente es \emptyset y son idempotentes: \emptyset, A, X . No hay inversos.

6. En \mathbb{R} , estudiemos la operación $*$ definida por:

$$a * b = a + b + ab$$

- (a) $*$ es una l.c.i. en \mathbb{R} , pues la suma de números reales es un número real y el producto de números reales es un número real, luego $a * b$ es un número real.
- (b) $*$ es asociativa. En efecto:

$$\begin{aligned} (a * b) * c &= (a + b + ab) * c \\ &= (a + b + ab) + c + (a + b + ab)c \\ &= a + b + ab + c + ac + bc + abc \\ a * (b * c) &= a * (b + c + bc) \\ &= a + b + c + bc + a(b + c + bc) \\ &= a + b + c + bc + ab + ac + abc \end{aligned}$$

- (c) $*$ es conmutativa
- (d) Existe un neutro. Busquémolo
 $a * x = a; \quad \forall a \in A$ ssi $a + x + ax = a; \quad \forall a \in A$ ssi
 $(1 + a)x = 0; \quad \forall a \in A$, luego $x = 0$, es decir, el neutro es el 0.
- (e) Busquemos si los elementos de A tienen inversos. Dado $x \in A$ buscamos encontrar $y \in A$, tal que $x * y = 0$.

$$x * y = 0 \Rightarrow x + y + xy = 0 \Rightarrow (1 + x)y = -x$$

Entonces

$$y = \frac{-x}{1+x}; \quad \text{ssi } x \neq -1$$

Luego -1 es el único elemento de \mathbb{R} que no tiene inverso con respecto a esta ley.

Proposición 6.1.1 Sea $(A, *)$ una estructura algebraica. Entonces, si existe un elemento neutro $e \in A$, éste es único.

Demostración. Sean $e, e' \in A$, neutros, entonces

$$e' = e' * e = e$$

En la primera igualdad utilizamos el hecho que e es neutro y en la segunda igualdad utilizamos el hecho que e' es neutro. Puesto que $e = e'$, el neutro es único.

Proposición 6.1.2 Sea $(A, *)$ una estructura algebraica. Si $*$ es una l.c.i. asociativa y si existe elemento neutro e , entonces:

1. El inverso de un elemento es único.
2. Si a^{-1} es el inverso de a y b^{-1} es el inverso de b , entonces el elemento $a * b$ tiene inverso y su inverso es $(a * b)^{-1} = b^{-1} * a^{-1}$

Demostración (1) Sea $a \in A$ un elemento cualquiera. Sean c y d dos inversos de a , entonces

$$c = c * e = c * (a * d) = (c * a) * d = e * d = d$$

En forma sucesiva utilizamos las propiedades siguientes: que e es el neutro, que d es inverso de a , que $*$ es asociativa, que c es inverso de a y que e es el neutro. Luego a tiene un único inverso. Esto quiere decir que todo elemento tiene un único inverso.

Demostración (2) $(b^{-1} * a^{-1}) * (a * b) = b^{-1} * ((a^{-1} * a) * b) = b^{-1} * (e * b) = b^{-1} * b = e$

En forma sucesiva utilizamos las propiedades siguientes: $*$ es asociativa, a^{-1} es el inverso de a , e es el neutro, b^{-1} es el inverso de b .

De la misma manera se demuestra también que $(a * b) * (b^{-1} * a^{-1}) = e$.

Luego $b^{-1} * a^{-1}$ es el inverso de $a * b$.

Ejemplo. En \mathbb{Z} , la suma es asociativa. Tenemos un único elemento neutro, denotado 0 y todo elemento $a \in \mathbb{Z}$, tiene un único inverso aditivo, denotado $-a$.

Definición 6.1.10 Diremos que un elemento $a \in A$ es **cancelable** con respecto a la l.c.i. $*$ si y sólo si para todo $b, c \in A$ se tiene:

$$\begin{aligned} a * b = a * c &\implies b = c \\ b * a = c * a &\implies b = c \end{aligned}$$

Ejemplo. En $(\mathbb{N}, +)$, se tiene:

$$\begin{aligned} 2 + b = 2 + c &\implies b = c \\ b + 2 = c + 2 &\implies b = c \end{aligned}$$

Nótese que no hemos sumado -2 a ambos lados, pues no existe $-2 \in \mathbb{N}$. Diremos que 2 es cancelable para la suma.

Observación. Un elemento a no es cancelable cuando en su tabla se tiene lo siguiente:

$*$	\dots	c	\dots	d	\dots
\dots	\dots	\dots	\dots	\dots	\dots
a	\dots	b	\dots	$b \dots$	\dots
\dots	\dots	\dots	\dots	\dots	\dots

Es decir, cuando tenemos $a * c = b$ y $a * d = b$. Luego tenemos $a * c = a * d$. No podemos cancelar a . Tendríamos $c = d$, lo cual es falso.

Ejemplo. Consideremos \mathbb{Z}_6^* , con la multiplicación siguiente. Su tabla es la siguiente:

\cdot	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

El 2 no es cancelable. Observemos que: $2 * 2 = 4$ y $2 * 5 = 4$. Es decir $2 * 2 = 2 * 5$ y $2 \neq 5$

El 3 no es cancelable. Contraejemplo: $3 * 3 = 3 * 5$ y $3 \neq 5$. O bien $3 * 2 = 3 * 4$ y $2 \neq 4$

Sin embargo el 5 es cancelable.

Proposición 6.1.3 Sea $(A, *)$ una estructura algebraica, con la l.c.i. $*$ asociativa y elemento neutro e , entonces todo elemento invertible es cancelable.

Demostración. Sea $a \in A$ invertible, con inverso a^{-1} . Entonces:

$$y * a = z * a \Rightarrow (y * a) * a^{-1} = (z * a) * a^{-1}$$

Asociando, tenemos: $y * (a * a^{-1}) = z * (a * a^{-1})$. Luego $y * e = z * e$. De donde $y = z$.

De la misma manera, a es cancelable al lado izquierdo.

Ejemplo. Consideremos nuevamente \mathbb{Z}_6^* , con la mutiplicación antes definida. Tenemos que 5 es invertible. Entonces

$$\begin{aligned} b \cdot 5 = a \cdot 5 &\Rightarrow (b \cdot 5) \cdot 5 = (a \cdot 5) \cdot 5 \Rightarrow b \cdot (5 \cdot 5) = a \cdot (5 \cdot 5) \Rightarrow \\ b \cdot 1 = a \cdot 1 &\Rightarrow b = a \end{aligned}$$

6.2 Subestructuras

Introducción. Si tenemos una estructura algebraica, $(A, *)$, estamos interesados en estudiar una estructura $(B, *)$, donde B es un subconjunto de A . Estamos interesados en encontrar propiedades en común entre A y B .

Observación. Consideremos (\mathbb{Q}, \cdot) . Sabemos que es una estructura algebraica. Tenemos que \mathbb{Z} es un subconjunto de \mathbb{Q} . Ocurre que (\mathbb{Z}, \cdot) es una estructura algebraica. Diremos que (\mathbb{Z}, \cdot) es una subestructura algebraica de (\mathbb{Q}, \cdot) . También diremos que " \cdot " es estable en \mathbb{Z} .

Definición 6.2.1 Diremos que la operación $*$ es **cerrado o estable** en A ssi

$$x * y \in A; \quad \forall x, y \in A$$

Ejemplos

1. La suma es estable en \mathbb{N} .

2. El producto es estable en \mathbb{N} .
3. Sea $I = \{\text{impares}\}$. Entonces la multiplicación es estable en I .
En efecto,

$$(2n+1)(2m+1) = 4nm+2n+2m+1 = 2(2nm+n+m)+1 = 2a+1$$

donde $a = 2nm + n + m$. Luego el producto de dos números impares es un número impar.

Pregunta: Sea $A \subset B$. Sean A y B cerrados para una l.c.i. $*$. ¿Qué propiedades de $*$ en B siguen cumpliéndose en A ? La respuesta a esta pregunta la tenemos en la siguiente proposición.

Proposición 6.2.1 *Sea $A \subset B$. Sean $(B, *)$ y $(A, *)$ dos estructuras algebraicas. Entonces*

1. *Si $*$ es asociativa en B , entonces $*$ es asociativa en A .*
2. *Si $*$ es conmutativa en B , entonces $*$ es conmutativa en A .*
3. *Si a es cancelable en B , entonces a es cancelable en A .*
4. *Si además se tiene otra l.c.i. \triangleleft en B entonces :*
Si $$ se distribuye con respecto a \triangleleft en B , entonces $*$ se distribuye con respecto a \triangleleft en A .*

Demostración (1) Si $*$ es asociativa en B , entonces

$$a * (b * c) = (a * b) * c; \quad \forall a, b, c \in B$$

En particular

$$a * (b * c) = (a * b) * c; \quad \forall a, b, c \in A$$

Para las demás demostraciones se tiene el mismo razonamiento, es decir, si es válido para todo elemento de B , entonces en particular es válido para todo elemento de A .

Nota. Si B tiene elemento neutro según $*$, no siempre es cierto que este elemento neutro se encuentre en A . Es decir, si $e \in B$, e neutro con respecto a $*$, no siempre se tiene $e \in A$.

Lo mismo ocurre para los elementos inversos de elementos de B .

Observación. Sabemos que $\mathbb{N} \subset \mathbb{Z}$ y que $(\mathbb{Z}, +)$ y $(\mathbb{N}, +)$ son estructuras algebraicas. Todo elemento $a \in \mathbb{Z}$ tiene inverso aditivo en \mathbb{Z} , sin embargo, ningún elemento de \mathbb{N} , tiene inverso aditivo en \mathbb{N} .

6.3 Grupos, anillos y cuerpos

Veremos en esta sección, algunas estructuras con algunos ejemplos de cada una de ellas.

Definición 6.3.1 Dada la estructura algebraica $(X, *)$, diremos que tiene estructura de **grupo** o que es un grupo, si la l.c.i. $*$ verifica:

G.1. $*$ es asociativa.

G.2. $*$ admite elemento neutro.

G.3. Cada elemento de X tiene su inverso en X , con respecto a $*$.

Si además $*$ es conmutativa, diremos que $(X, *)$ es un **grupo conmutativo o abeliano**

Ejemplos

1. Son grupos abelianos: $(\mathbb{Z}, +)$, (\mathbb{Q}^*, \cdot) , $(\mathbb{R}, +)$, (\mathbb{R}^*, \cdot) .
2. Consideremos las funciones reales siguientes: $f_i : \mathbb{R} \rightarrow \mathbb{R}$, definidas por:

$$f_1 = id; \quad f_2(x) = \frac{1}{x}; \quad f_3(x) = 1 - x; \quad f_4(x) = \frac{1}{1 - x};$$

$$f_5(x) = \frac{x - 1}{x}; \quad f_6(x) = \frac{x}{x - 1}$$

Estudiemos (G, \circ) , donde $G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ con respecto a la composición de funciones.

Tenemos la tabla siguiente:

\circ	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_4	f_3	f_6	f_5
f_3	f_3	f_5	f_1	f_6	f_2	f_4
f_4	f_4	f_6	f_2	f_5	f_1	f_3
f_5	f_5	f_3	f_6	f_1	f_4	f_2
f_6	f_6	f_4	f_5	f_2	f_3	f_1

Observemos que: El neutro para esta operación es f_1

$$f_2^{-1} = f_2; \quad f_3^{-1} = f_3; \quad f_4^{-1}f_5; \quad f_6^{-1} = f_6$$

Dos ejemplos de cómo obtener estos resultados son los siguientes:

$$(f_4 \circ f_3)(x) = f_4(f_3(x)) = f_4(1 - x) = \frac{1}{1 - (1 - x)} = \frac{1}{x} = f_2(x)$$

$$(f_6 \circ f_5)(x) = f_6\left(\frac{x-1}{x}\right) = \frac{\frac{x-1}{x}}{\frac{x-1}{x} - 1} = \frac{x-1}{-1} = 1 - x = f_3(x)$$

Observe que este grupo no es conmutativo.

3. Consideremos el grupo $G = \{N, I, D, O\}$. Donde se tiene:

N = no rotar; I = rotar en 90° a la izquierda; D = rotar en 90° a la derecha; O = rotar en 180° . Su tabla de composición es la siguiente:

\circ	N	I	D	O
N	N	I	D	O
I	I	O	N	D
D	D	N	O	I
O	O	D	I	N

Entonces (G, \circ) es un grupo conmutativo. El elemento neutro es N . El inverso de I es D . El inverso de O es el mismo.

4. **Rotaciones y simetrías del triángulo.** La notación $\triangle ABC$ considera los vértices en sentido horario. Definamos las rotaciones y simetrías siguientes:

$$r_1 : \triangle ABC \longrightarrow \triangle CAB; \quad r_2 : \triangle ABC \longrightarrow \triangle BCA$$

$$r_0 : \triangle ABC \longrightarrow \triangle ABC; \quad s_1 : \triangle ABC \longrightarrow \triangle ACB$$

$$s_2 : \triangle ABC \longrightarrow \triangle CBA; \quad s_3 : \triangle ABC \longrightarrow \triangle BAC$$

Sea $(G = \{r_0, r_1, r_2, s_1, s_2, s_3\}, \circ)$. Consideremos la composición funciones. Entonces tenemos la tabla de composiciones sgte:

\circ	r_0	r_1	r_2	s_1	s_2	s_3
r_0	r_0	r_1	r_2	s_1	s_2	s_3
r_1	r_1	r_2	r_0	s_2	s_3	s_1
r_2	r_2	r_0	r_1	s_3	s_1	s_2
s_1	s_1	s_2	s_3	r_0	r_2	r_1
s_2	s_2	s_3	s_1	r_1	r_0	r_2
s_3	s_3	s_2	s_1	r_2	r_1	r_0

Entonces (G, \circ) es un grupo. Es llamado el grupo de las rotaciones y simetrías del triángulo.

Ejercicio. Sea $A = \mathbb{Q} - \{\frac{-1}{4}\}$ y

$$* : A \times A \longrightarrow A; \quad \text{tal que } a * b = a + b + 4ab$$

Demostremos que $(A, *)$ es un grupo.

Solución.

1. Demostremos que $(A, *)$ es una estructura algebraica. Supongamos que no lo es, es decir, supongamos que $a * b = \frac{-1}{4}$ con $a, b \neq \frac{-1}{4}$. Tenemos $a * b = \frac{-1}{4}$, es decir, $a + b + 4ab = \frac{-1}{4}$. Luego $b(1 + 4a) = \frac{-1}{4} - a$. Luego $b = \frac{-1-4a}{4(1+4a)} = \frac{-1}{4}$. Contradicción pues $b \neq \frac{-1}{4}$

2. $*$ es asociativa.

$$\begin{aligned}
 (a * b) * c &= (a + b + 4ab) * c \\
 &= a + b + 4ab + c + 4(a + b + 4ab)c \\
 &= a + b + c + 4ab + 4ac + 4bc + 16abc \\
 a * (b * c) &= a * (b + c + 4bc) \\
 &= a + b + c + 4bc + 4a(b + c + 4bc) \\
 &= a + b + c + 4bc + 4ab + 4ac + 16abc
 \end{aligned}$$

3. Existe elemento neutro. Sea b el elemento neutro. Luego $a * b = a$; $\forall a \in A$. Luego $a + b + 4ab = a$; $\forall a \in A$. De donde $b(1 + 4a) = 0$; $\forall a \in A$. Puesto que $1 + 4a \neq 0$; $\forall a \in A$, tenemos que $b = 0$. Luego el neutro es el 0.

4. Todo elemento tiene inverso. Sea $a \in A$ cualquiera. Sea b su posible inverso. Luego $a * b = 0$. De donde $a + b + 4ab = 0$. Entonces $b = \frac{-a}{1+4a}$. Es decir $a^{-1} = \frac{-a}{1+4a}$. Conclusión: todo elemento tiene inverso.

5. $*$ es conmutativa pues su escritura es simétrica.

Definición 6.3.2 Supongamos que el conjunto X forma una estructura algebraica con las l.c.i. $*$ y \triangleleft . Diremos que $(X, *, \triangleleft)$ es un **anillo** si se tiene:

A.1. $(X, *)$ es un grupo abeliano.

A.2. \triangleleft es asociativa.

A.3. \triangleleft se distribuye con respecto a $*$.

Si además \triangleleft es conmutativa, diremos que $(X, *, \triangleleft)$ es un **anillo conmutativo**.

Si existe un elemento neutro con respecto a la segunda l.c.i., diremos que $(X, *, \triangleleft)$ es un **anillo con unidad**.

Ejemplo. $(\mathbb{Z}, +, \cdot)$ es un anillo con unidad.

Definición 6.3.3 Sea $(A, +, \cdot)$ un anillo. Diremos que $a \in A$, $a \neq 0$, es un **divisor de cero** si existe $b \in A$, $b \neq 0$, tal que $a \cdot b = 0$.

Definición 6.3.4 Diremos que $(X, *, \triangleleft)$ es un **cuerpo** si:

C.1. $(X, *, \triangleleft)$ es un anillo.

C.2. $(X - \{e\}, \triangleleft)$ es un grupo, donde e es el neutro de X , según $*$.

Si \triangleleft es una l.c.i. conmutativa, diremos que $(X, *, \triangleleft)$ es un cuerpo conmutativo.

Ejemplos. $(\mathbb{Q}, +, \cdot)$ y $(\mathbb{R}, +, \cdot)$ son cuerpos conmutativos.

Nota. La sección sub siguiente estará dedicada a dar ejemplos de anillos y cuerpos con un número finito de elementos.

6.4 Subgrupos

Observación. Se tiene que (\mathbb{Q}^*, \cdot) es un grupo. Además $H = (\{-1, 1\}, \cdot)$ también es un grupo y $H \subset \mathbb{Q}^*$. Diremos que " H es un subgrupo de \mathbb{Q}^* ", con respecto a la multiplicación.

Definición 6.4.1 Dado un grupo $(G, *)$, diremos que $(H, *)$ es un subgrupo de G si:

1. $H \neq \emptyset, H \subset G$
2. $(H, *)$ es un grupo

Ejemplo. Sea G el grupo de las rotaciones y simetría del triángulo.

Tenemos que $H_1 = \{r_0, r_1, r_2\}$ es un subgrupo de G .

$H_2 = \{r_0, s_1\}; H_3 = \{r_0, s_2\}; H_4 = \{r_0, s_3\}$ también son subgrupos de G . Sin olvidar que G y $\{r_0\}$ también lo son.

En total hay 6 subgrupos de (G, \circ)

Proposición 6.4.1 (Caracterización de subgrupo) Sea G un conjunto; $H \subset G, H \neq \emptyset$. Son equivalentes:

1. $(H, *)$ es un subgrupo de $(G, *)$

$$2. h * g^{-1} \in H; \forall h, g \in H$$

Demostración (1) \Rightarrow (2) Si H es un subgrupo de G , $*$ es una l.c.i. cerrada en H . Luego

$$h, g \in H \Rightarrow g^{-1} \in H, h \in H \Rightarrow h \cdot g^{-1} \in H$$

Demostración (2) \Rightarrow (1)

1. $*$ es asociativa en G , luego lo es también para los elementos de H .
2. $H \neq \emptyset$, luego existe $h \in H$, luego usando la hipótesis se concluye que $h * h^{-1} \in H$. Luego $e \in H$
3. Dado $h \in H$, entonces $e, h \in H$, entonces $e * h^{-1} \in H$, luego $h^{-1} \in H$. Es decir todo elemento de H , tiene su inverso en H .
4. $*$ es cerrado en H pues:

$$h, g \in H \Rightarrow h, g^{-1} \in H \Rightarrow h * (g^{-1})^{-1} \in H \Rightarrow h * g \in H$$

Luego $(H, *)$ es un subgrupo de $(G, *)$

Definición 6.4.2 Diremos que $(H, *)$ es un **subgrupo propio** de $(G, *)$, si $H \subset G$, $H \neq G$, $H \neq \{e\}$

Diremos que $\{e\}$ y G son los **subgrupos triviales** de $(G, *)$

Ejemplos

1. $(\mathbb{Z}, +)$ es un subgrupo propio de $(\mathbb{Q}, +)$.
2. Consideremos las funciones reales siguientes: $f_i : \mathbb{R} \rightarrow \mathbb{R}$, definidas por:

$$f_1 = id; \quad f_2(x) = \frac{1}{x}; \quad f_3(x) = 1 - x;$$

$$f_4(x) = \frac{1}{1-x}; \quad f_5(x) = \frac{x-1}{x}; \quad f_6(x) = \frac{x}{x-1}$$

Consideremos (G, \circ) , donde $G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ con respecto a la composición de funciones. Tenemos que $\{f_1\}$ y G son los dos subgrupos triviales de $(G, *)$.

Hay tres subgrupos propios de dos elementos cada uno, a saber: $\{f_1, f_2\}$, $\{f_1, f_3\}$, $\{f_1, f_6\}$

$\{f_1, f_4, f_5\}$ es un subgrupo propio de G con tres elementos.

Nota. El grupo de las rotaciones y simetrías del triángulo tienen los mismos subgrupos que el visto recientemente.

3. Consideremos $G = \{N, I, D, O\}$ del ejemplo visto anteriormente. Tenemos que $\{N\}$ y G son los dos subgrupos triviales de G . $\{N, O\}$ es un subgrupo propio de G
4. Consideremos $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$, con su tabla de la suma:

\oplus	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Tiene como único subgrupo propio a $H = (\{0, 2\}, \oplus)$. Tiene la misma estructura que el grupo $G = \{N, I, D, O\}$ visto anteriormente.

5. Sea $G = \{e, a, b, c\}$ y $*$ definida por la tabla siguiente:

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Tiene tres subgrupos propios de dos elementos cada uno, a saber:

$$\{e, a\}; \{e, b\}; \{e, c\}$$

Este grupo es llamado **grupo de Klein**. Este grupo no tiene la misma estructura que el grupo anterior.

Nota. Usted puede verificar que no hay más que estos dos grupos de 4 elementos.

6.5 Estructura de \mathbb{Z}_n

Estructura de (\mathbb{Z}_6, \oplus)

Sobre \mathbb{Z} se define:

$$aRb \text{ ssi } a - b = 6k; \text{ cierto } k \in \mathbb{Z}$$

la cual es una relación de equivalencia. Escribimos

$$\bar{a} = \{a + 6k; \quad k \in \mathbb{Z}\}$$

Tenemos que el conjunto cuociente es

$$\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$$

La suma está definida por:

$$\bar{a} + \bar{b} = \overline{a + b}$$

Es decir, está dada por la tabla siguiente:

\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

Se tiene que (\mathbb{Z}_6, \oplus) es un grupo abeliano. Hay dos subgrupos triviales: $\{0\}$ y \mathbb{Z}_6 . Hay un subgrupo formado por 2 elementos, a saber: $(\{0, 3\}, \oplus)$. Hay un subgrupo formado por tres elementos, a saber: $(\{0, 2, 4\}, \oplus)$

Estructura de (\mathbb{Z}_n, \oplus)

Generalizando la situación anterior, sobre \mathbb{Z} se define:

$$aRb \text{ ssi } a - b = nk; \text{ cierto } k \in \mathbb{Z}$$

la cual es una relación de equivalencia. Escribimos

$$\bar{a} = \{a + nk; \quad k \in \mathbb{Z}\}$$

Ahora el conjunto cociente es

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$$

Con la suma definida por:

$$\bar{a} \oplus \bar{b} = \overline{a + b}$$

Se tiene que (\mathbb{Z}_n, \oplus) es un grupo abeliano.

Teorema 6.5.1 (Teorema de Cayley) *Sea G un grupo de n elementos. Si H es un subgrupo de G con m elementos entonces m divide a n .*

Observación. \mathbb{Z}_p tiene p elementos, con p primo. Por el Teorema de Cayley, \mathbb{Z}_p no tiene subgrupos propios, pues el número de elementos del subgrupo debe dividir a p .

6.6 Estructura de S_n

Estructura de S_3 . Consideremos los siguientes elementos de S_3

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}; \quad a = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}; \quad a^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix};$$

$$a^3 = e; \quad c = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \tau_{12}; \quad c^2 = e$$

$$ac = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \tau_{23}; \quad a^2c = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \tau_{13}$$

Luego $S_3 = \{e, a, a^2, c, ac, a^2c\}$ Su tabla de multiplicación es la siguiente:

\cdot	e	a	a^2	c	ac	a^2c
e	e	a	a^2	c	ac	a^2c
a	a	a^2	e	ac	a^2c	c
a^2	a^2	e	a	a^2c	c	ac
c	c	a^2c	ac	e	a^2	a
ac	ac	c	a^2c	a	e	a^2
a^2c	a^2c	ac	c	a^2	a	e

Tenemos que $(\{e, a, a^2\}, \cdot)$, $(\{e, c\}, \cdot)$, $(\{e, ac\}, \cdot)$ y $(\{e, a^2c\}, \cdot)$ son subgrupos propios de S_3 .

Notación. La permutación $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ puede ser denotada por $\begin{pmatrix} 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}$,

o bien por $\begin{pmatrix} 2 & 1 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, etc. Escribiendo siempre la imagen de cada elemento debajo de él.

Ejercicios Resueltos

1. Dada $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 1 & 2 \end{pmatrix}$

(a) Encontremos n minimal, tal que $\sigma^n = id$.

(b) Busquemos σ^{-1}

(c) Busquemos τ tal que $\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}$

Solución.

(a) $\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix}; \quad \sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{pmatrix}$

$$\sigma^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 3 & 1 \end{pmatrix}; \quad \sigma^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = id$$

Luego $n = 5$.

- (b) Como $id = \sigma^5 = \sigma^4\sigma$. De esto se deduce que $\sigma^{-1} = \sigma^4$.
- (c) Multipliquemos por σ^{-1} a la izquierda de la igualdad siguiente:

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}$$

Se tiene entonces:

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$$

2. Estudiemos la estructura algebraica de $(\mathbb{Z}_3 \times \mathbb{Z}_2, \oplus, \odot)$, donde la suma y el producto son componente a componente.

Solución

\oplus	(0, 0)	(0, 1)	(1, 0)	(1, 1)	(2, 0)	(2, 1)
(0, 0)	(0, 0)	(0, 1)	(1, 0)	(1, 1)	(2, 0)	(2, 1)
(0, 1)	(0, 1)	(0, 0)	(1, 1)	(1, 0)	(2, 1)	(2, 0)
(1, 0)	(1, 0)	(1, 1)	(2, 0)	(2, 1)	(0, 0)	(0, 1)
(1, 1)	(1, 1)	(1, 0)	(2, 1)	(2, 0)	(0, 1)	(0, 0)
(2, 0)	(2, 0)	(2, 1)	(0, 0)	(0, 1)	(1, 0)	(1, 1)
(2, 1)	(2, 1)	(2, 0)	(0, 1)	(0, 0)	(1, 1)	(1, 0)

El elemento neutro es el (0, 0). Todo elemento es invertible, luego todo elemento es cancelable.

Veamos la tabla de multiplicación de $(\mathbb{Z}_3 \times \mathbb{Z}_2)^*$

\odot	(0, 1)	(1, 0)	(1, 1)	(2, 0)	(2, 1)
(0, 1)	(0, 1)	(0, 0)	(0, 1)	(0, 0)	(0, 1)
(1, 0)	(0, 0)	(1, 0)	(1, 0)	(2, 0)	(2, 0)
(1, 1)	(0, 1)	(1, 0)	(1, 1)	(2, 0)	(2, 1)
(2, 0)	(0, 0)	(2, 0)	(2, 0)	(1, 0)	(1, 0)
(2, 1)	(0, 1)	(2, 0)	(2, 1)	(1, 0)	(1, 1)

El elemento neutro es el (1, 1).

Son divisores de cero: (0, 1), (1, 0), (2, 0).

Solamente el (2, 1) es invertible, cancelable y su inverso es él mismo.

3. Demostremos que $S = \{2^n; n \in \mathbb{Z}\}$ es un subgrupo de (\mathbb{Q}^*, \cdot)

Solución. $S \neq \emptyset$, pues, por ejemplo $s = 2^1 = 2 \in S$. Además es claro que $S \subset \mathbb{Q}^*$.

Sean $s, t \in S$. Debemos probar que $s \cdot t^{-1} \in S$.

$$s \in S \implies s = 2^n, \text{ cierto } n \in \mathbb{Z}$$

Busquemos el elemento neutro. Llamémoslo 2^m . Tenemos

$$2^n \cdot 2^m = 2^n, \quad \forall n \in \mathbb{Z}$$

luego $n + m = n, \forall n \in \mathbb{Z}$, luego $m = 0$. El neutro es entonces 2^0 .

Dado $t = 2^m$, busquemos su inverso. Denotémoslo por 2^n . Luego $2^m \cdot 2^n = 2^0$. De donde $2^{m+n} = 2^0$. Entonces $n + m = 0$, es decir, $n = -m$. Luego $t^{-1} = 2^{-m}$

Sean $s, t \in S$, luego $s = 2^n, t = 2^m$, ciertos $n, m \in \mathbb{Z}$

Tenemos $s \cdot t^{-1} = 2^n \cdot 2^{-m} = 2^{n-m} \in S$, pues $n - m \in \mathbb{Z}$.

Luego (S, \cdot) es un subgrupo de (\mathbb{Q}^*, \cdot)

4. Consideremos el conjunto $G = \{e, \alpha, \beta, \gamma\}$, donde

$$e, \alpha, \beta, \gamma : \mathbb{R} \longrightarrow \mathbb{R}$$

están definidas por:

$$e(x) = x; \quad \alpha(x) = -x; \quad \beta(x) = \frac{1}{x}; \quad \gamma(x) = \frac{-1}{x}$$

Estudiemos (G, \circ)

Solución. Observemos que

$$(\alpha \circ \alpha)(x) = \alpha(\alpha(x)) = \alpha(-x) = -(-x) = x; \quad \forall x \in \mathbb{R}$$

Luego $\alpha^2 = e$.

$$\beta^2(x) = (\beta \circ \beta)(x) = \beta(\beta(x)) = \beta\left(\frac{1}{x}\right) = x; \quad \forall x \in \mathbb{R}$$

Luego $\beta^2 = e$

$$(\alpha \circ \beta)(x) = \alpha\left(\frac{1}{x}\right) = -\frac{1}{x} = \gamma(x); \quad \forall x \in \mathbb{R}$$

Luego $\alpha \circ \beta = \gamma$

$$(\beta \circ \alpha)(x) = \beta(\alpha(x)) = \beta(-x) = \frac{1}{-x} = -\frac{1}{x} = \gamma(x)$$

Luego $\beta \circ \alpha = \gamma$.

La tabla de composición es la siguiente:

\circ	e	α	β	γ
e	e	α	β	γ
α	α	e	γ	β
β	β	γ	e	α
γ	γ	β	α	e

El neutro es la identidad e . Los tres restantes elementos α, β y γ tienen inverso, luego son cancelables. No hay divisores de cero. En este conjunto la composición es conmutativa. Luego este grupo es conmutativo. Nuevamente tenemos el grupo de Klein.

5. Sea $I = \{1, 2, 3, 4\}$. Consideremos las siguientes permutaciones sobre este conjunto:

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}; \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}; \quad \mu = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix};$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

Estudiemos este subgrupo.

Solución Tenemos la siguiente tabla de multiplicación

\cdot	e	σ	μ	τ
e	e	σ	μ	τ
σ	σ	e	τ	μ
μ	μ	τ	e	σ
τ	τ	μ	σ	e

Nuevamente hemos obtenido el grupo de Klein. El neutro es el elemento e y cada elemento es el inverso de él mismo.

6.7 Aritmética

Estudiemos el reloj de 12 números.

Tenemos por ejemplo que el número 13 es el mismo que el 1. Escribiremos $13 \equiv 1(12)$. Decir "son las 15 horas" es lo mismo que decir "son las 3". Escribiremos $15 \equiv 3(12)$.

Escribiremos

$a \equiv b$ si y sólo si $a - b$ es un múltiplo de 12, es decir, si y sólo si $a - b = 12n$, cierto $n \in \mathbb{Z}$

Por ejemplo, tenemos las operaciones siguientes:

$$8 + 5 \equiv 1(12); \quad 6 + 7 \equiv 1(12); \quad 6 + 8 \equiv 2(12)$$

Anteriormente hemos visto:

$$\mathbb{Z}_{12} = \{\bar{0}, \bar{1}, \dots, \bar{11}\}$$

El inverso aditivo de 2 es 10. Escribiremos $-2 = 10$. Además $-3 = 9$, $-4 = 8$; $-5 = 7$; $-6 = 6$.

Observación. Consideremos \mathbb{Z}_3 , con la suma y el producto definidos por:

\oplus	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

\odot	1	2
1	1	2
2	2	1

Escribiremos: $-1 = 2$; $-2 = 1$. El inverso multiplicativo de 2 será denotado por $\frac{1}{2}$. Luego $\frac{1}{2} = 2$, pues $2 \cdot 2 = 1$

En \mathbb{Z}_3 , resolvamos la ecuación:

$$2x + 2 = 1$$

$$2x + 2 = 1 \implies 2x + 3 = 2 \implies 2x = 2 \implies x = 1$$

Veamos a qué corresponde el número $(\frac{1}{2})^{1.005}$.

Tenemos que $(\frac{1}{2})^{1.005} = 2^{1.005}$ y $2^2 = 4 = 1$. Como $1.005 = 2 \cdot 502 + 1$, luego $(2^{1.005}) = 2^{2 \cdot 502 + 1} = (2^2)^{502} \cdot 2^1 = 1^{502} \cdot 2 = 2$

Observación. Consideremos \mathbb{Z}_4 y en \mathbb{Z}_4^* . Sus tablas de adición y multiplicación son las siguientes:

\oplus	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

\odot	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

El elemento unidad es el 1. El 3 es invertible y su inverso multiplicativo es $\frac{1}{3} = 3$. El 2 es un divisor de cero, luego no es invertible y tampoco es cancelable.

En \mathbb{Z}_4 , estudiemos la ecuación

$$2x + 3 = 1$$

$$2x + 3 = 1 \implies 2x + 4 = 2. \text{ Luego } x = 1 \text{ o } x = 3.$$

Ejercicios Resueltos

1. En \mathbb{Z}_{12} , resolvamos la ecuación

$$2x + 3 = 10$$

Solución. $2x + 3 = 10 \text{ } / + 9 \implies 2x + 3 + 9 = 19 \implies 2x + 12 = 7$
 $2x = 7$, la cual no tiene solución.

2. Resolvamos en \mathbb{Z}_{12} , la ecuación:

$$2x + 3 = 11$$

Solución. $2x + 3 = 11 \text{ } / + 9 \implies 2x + 12 = 20 \implies 2x = 8 \implies$
 $x_1 = 4 \text{ } x_2 = 10$

3. En \mathbb{Z}_5 resolvamos la ecuación: $2x + 4 = 1$.

Solución. $2x + 4 = 1 \ / \ + 1 \implies 2x + 5 = 2 \implies 2x = 2 \implies x = 1$.

4. En \mathbb{Z}_5 resolvamos la ecuación $4x - 3 = 4$.

Solución. $4x - 3 = 4 \ / \ + 8 \implies 4x + 5 = 12 \implies 4x = 2 \implies x = 3$

5. En \mathbb{Z}_5 , busquemos el valor de $\frac{3}{4}$ y $\frac{2}{3}$.

Solución. $\frac{3}{4} = 3 \cdot \frac{1}{4} = 3 \cdot 4 = 12 = 2$. Luego $\frac{3}{4} = 2$

$\frac{2}{3} = 2 \cdot \frac{1}{3} = 2 \cdot 2 = 4$. Luego $\frac{2}{3} = 4$

6. En \mathbb{Z} estudiemos si el número $6^6 + 4^4$ es divisible por 5.

Solución. $6^6 + 4^4 = 1^6 + (-1)^4 = 1 + 1 = 2$. Luego $6^6 + 4^4$ no es divisible por 5.

7. En \mathbb{Z} veamos si el número: $2.006^{31} + 174^{12}$ es divisible por 5.

Solución. $2.006^{31} + 174^{12} = 1^{31} + 4^{12} = 1 + (-1)^{12} = 1 + 1 = 2$. Luego no es divisible por 5.

8. Probemos que el número:

$$2.001^{2.001} + 1.999^{1.999}$$

es divisible por 2.000.

Solución. Tenemos $2.001^{2.001} + 1.999^{1.999} = 1^{2.001} + (-1)^{1.999} = 1 + (-1) = 0$. Luego este número es divisible por 2.000.

9. ¿Qué números al ser multiplicados por 7, dan una unidad más que un múltiplo de 11?

Solución. Tenemos la ecuación: $7x \equiv 1(11)$. Luego $x = 8$

Luego los números de la forma $8 + 11k$, $k \in \mathbb{Z}$ cumplen lo pedido.

10. En \mathbb{Z}_{11} , calculemos el valor de:

$$\frac{2}{7} + \frac{1}{5} - \frac{2}{9}$$

Solución. $\frac{2}{7} + \frac{1}{5} - \frac{2}{9} = 2 \cdot \frac{1}{7} + \frac{1}{5} + 9 \cdot \frac{1}{9} = 2 \cdot 8 + 9 + 1 = 16 + 9 + 1 = 16 + 10 = 26 = 4$

11. Demostremos que $3^{2n} - 2^{2n}$ es divisible por 5.

Solución. $3^{2n} - 2^{2n} \equiv (3^2)^n - (2^2)^n \equiv 9^n - 4^n \equiv 4^n - 4^n \equiv 0$

12. Demostremos que $10^n + 3 \cdot 4^{n+2} + 5$ es divisible por 9.

Solución. $10^n + 3 \cdot 4^{n+2} + 5 \equiv 10^n + 3 \cdot 4^n \cdot 4^2 + 5 \equiv 1^n + 3 \cdot 4^n \cdot 7 + 5 \equiv 6 + 3 \cdot 7 \cdot 4^n \equiv 3(2 + 7 \cdot 4^n)$

Por demostrar que: $2 + 7 \cdot 4^n$ es divisible por 3.

En efecto:

$$2 + 7 \cdot 4^n \equiv 2 + 1 \cdot 1^n \equiv 2 + 1 \equiv 0$$

Luego se tiene la propiedad pedida.

13. Cuando estudiamos sumatoria, vimos que

$$\sum_{k=1}^n k(k+10) = \frac{n(n+1)(2n+31)}{6}$$

Ocurre que al lado izquierdo tenemos una sumatoria de números naturales, la cual es un número natural, luego al lado derecho también tenemos un número natural, de donde se concluye que la expresión:

$$n(n+1)(2n+31)$$

es divisible por 6. Demostremos que en efecto es divisible por 6.

Solución. Debemos demostrar que esta expresión es congruente a 0 módulo 6.

Primero observamos que $31 \equiv 1(6)$. Tenemos la tabla siguiente:

n	0	1	2	3	4	5
$n + 1$	1	2	3	4	5	0
$2n + 1$	1	3	5	1	3	5
$n(n + 1)(2n + 1)$	0	0	0	0	0	0

Luego la expresión $n(n + 1)(2n + 1)$ es divisible por 6.

6.8 Ejercicios Propuestos

1. En $\mathbb{R} \times \mathbb{R}$ se define la ley de composición siguiente:

$$(a, b) * (c, d) = (ac, bc + d)$$

(a) Estudie las propiedades de $*$

(b) Calcule $(1, 2)^3$, $(2, 1)^{-2}$, $(2, 4)^4$

2. Estudie las siguientes estructuras:

(a) $(\mathbb{R}^2, *)$; $(a, b) * (c, d) = (a + c, b + d + 2bd)$

(b) $(\mathbb{N}, *)$, $a * b = \max\{a, b\}$

(c) Sea $S = \{1, 2, 3, 4, 6\}$, Estudie $(S, *)$, donde $a * b = m.c.d.(a, b)$

(d) Sea $S = \{1, 2, 5, 10\}$, y considere $(S, +, *)$, donde $a + b = m.c.d.(a, b)$ y $a * b = m.c.m.(a, b)$

3. Dados \mathbb{Z}_2 y \mathbb{Z}_3 , se define la operación $*$ en $\mathbb{Z}_2 \times \mathbb{Z}_3$ dada por:

$$(a, b) * (c, d) = (a \otimes_2 c, b \oplus_3 d)$$

Estudie las propiedades de $*$.

4. En el conjunto de los números naturales, se da la siguiente ley de composición interna $x \otimes y = |x - y|$. Pruebe que esta ley de composición cumple las siguientes propiedades:

(a) No asociativa (basta un contra-ejemplo)

- (b) Conmutativa
- (c) Tiene neutro
- (d) Tiene inversos

5. Sabiendo que $A = \{a, b, c, d\}$ es un grupo, complete la siguiente tabla de composición:

\circ	a	b	c	d
a	c			
b				
c				
d			c	

6. Consideremos la permutación $\sigma \in S_5$, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix}$

(a) Determine σ^{12345}

(b) Determine $\theta \in S_5$, tal que $\sigma^{-1} \circ \theta \circ \sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}$

Capítulo 7

Números complejos

7.1 Construcción

Definiciones

Comenzaremos por ver la construcción de los números complejos. Sobre $\mathbb{R} \times \mathbb{R}$ definamos la suma y el producto de la manera siguiente:

$$\begin{aligned}(x, y) + (u, v) &= (x + u, y + v) \\ (x, y) \cdot (u, v) &= (xu - yv, xv + yu)\end{aligned}$$

Sea

$$A = \{(x, 0); x \in \mathbb{R}\}$$

Definamos la función biyectiva

$$f : A \longrightarrow \mathbb{R}; \quad (x, 0) \rightarrow x$$

Es decir al par $(x, 0)$, se le asocia el número real x . En matemáticas se dice que se hace una identificación entre el par ordenado $(x, 0)$ y el número real x .

Escribimos: $(x, 0) =: x$

Notación. El par $(0, 1)$ será denotado por la letra i , es decir

$$(0, 1) =: i$$

Luego

$$(a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0)(0, 1) =: a + bi$$

Es decir (a, b) será identificado con la expresión $a + bi$

Definición 7.1.1 *En este caso diremos que $z = a + bi$, $a, b \in \mathbb{R}$ es un número complejo, cuya **parte real** es a y cuya **parte imaginaria** es b y diremos que está expresado en su **forma normal**.*

Notaciones. $Re(z) = a$ y $Im(z) = b$

Nota. Los números complejos han sido construídos a partir de los números reales. En los números reales tenemos el concepto de igualdad, entonces este concepto será utilizado para definir el concepto de igualdad entre números complejos.

Definición 7.1.2 *Diremos que dos números complejos son iguales si coinciden sus partes reales y sus partes imaginarias. Es decir:*

$$a+bi=c+di \text{ ssi } a=c \text{ y } b=d$$

\mathbb{C} denotará el conjunto formado por todos los números complejos. Es decir

$$\mathbb{C} = \{a + bi; a, b \in \mathbb{R}\}$$

Sobre \mathbb{C} tenemos la suma y el producto definidos anteriormente. Usando la identificación, tenemos:

$$\begin{aligned} (a + bi) + (c + di) &=: (a, b) + (c, d) \\ &=: (a + c, b + d) \\ &=: (a + c) + (b + d)i \end{aligned}$$

$$\begin{aligned} (a + bi) \cdot (c + di) &=: (a, b) \cdot (c, d) \\ &=: (ac - bd, ad + bc) \\ &=: (ac - bd) + (ad + bc)i \end{aligned}$$

Conclusión:

$$(a+bi)+(c+di)=(a+c)+(b+d)i$$

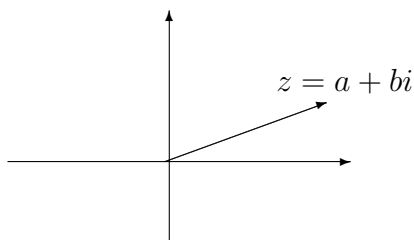
$$(a+bi) \cdot (c+di) = (ac-bd) + (ad+bc)i$$

$$i^2 = (0, 1) \cdot (0, 1) = (-1, 0) =: -1$$

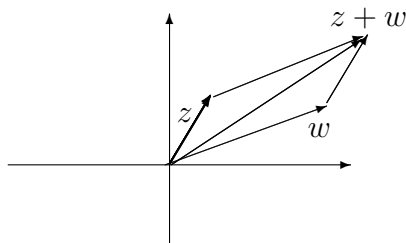
Estas definiciones se pueden obtener si multiplicamos como si fueran números reales y cada vez que aparezca i^2 , lo reemplazamos por -1 .

$$(a+bi) \cdot (c+di) = ac + adi + bci + bdi^2 = (ac-bd) + (ad+bc)i$$

Representación geométrica. El número complejo $z = a + bi$ lo representaremos en el sistema cartesiano como un vector que parte en el origen del sistema cartesiano y termina en el punto (a, b) .



La suma de dos números complejos corresponde a la suma según la ley del paralelogramo de ambos vectores, como se ve en la siguiente figura



7.2 Estructura algebraica de $(\mathbb{C}, +, \cdot)$

La suma definida anteriormente, es una ley de composición interna, pues, la suma de dos números complejos es un número complejo, es decir

$$\begin{aligned} + : \mathbb{C} \times \mathbb{C} &\rightarrow \mathbb{C}; \\ (a + bi, c + di) &\rightarrow (a + c) + (b + d)i \end{aligned}$$

Luego $(\mathbb{C}, +)$ es una estructura algebraica.

Proposición 7.2.1 $(\mathbb{C}, +)$ es un grupo abeliano.

Demostración. La suma es asociativa (se utiliza que la suma en \mathbb{R} es asociativa)

$$\begin{aligned} (a + bi) + ((c + di) + (e + fi)) &= (a + bi) + ((c + e) + (d + f)i) \\ &= (a + (c + e)) + (b + (d + f))i \\ &= ((a + c) + e) + ((b + d) + f)i \\ &= ((a + c) + (b + d)i) + (e + fi) \\ &= ((a + bi) + (c + di)) + (e + fi) \end{aligned}$$

Existe elemento neutro, a saber, $0 = 0 + 0i$; donde $0 \in \mathbb{R}$.

Todo elemento tiene inverso aditivo:

$$-(a + bi) = (-a) + (-b)i; \text{ donde } -a, -b \text{ son los inversos de } a, b \text{ en } \mathbb{R}$$

La suma es conmutativa. Nuevamente se utiliza la propiedad conmutativa de la suma en \mathbb{R} .

Luego $(\mathbb{C}, +)$ es un grupo abeliano.

Proposición 7.2.2 (\mathbb{C}^*, \cdot) es un grupo abeliano.

Demostración. Recordemos que $\mathbb{C}^* = \mathbb{C} - \{0\}$. La multiplicación es asociativa. (te lo dejamos de ejercicio)

Busquemos el neutro multiplicativo. Sea

$$(a + bi) \cdot (x + yi) = a + bi; \quad \forall a + bi \in \mathbb{C}$$

Luego $(ax - by) + (ay + bx)i = a + bi$

Es decir se debe cumplir el siguiente sistema de ecuaciones en \mathbb{R} :

$$\left. \begin{array}{l} (1) : ax - by = a \\ (2) : ay + bx = b \end{array} \right| \text{ Luego } \left. \begin{array}{l} b \cdot (1) : abx - b^2y = ab \\ a \cdot (2) : a^2y + abx = ab \end{array} \right|$$

$a \cdot (2) - b \cdot (1) : a^2y + b^2y = 0$. Luego $(a^2 + b^2)y = 0$. Luego $y = 0$.

Reemplazando en (1): $ax = a$; $\forall a \in \mathbb{R}$. Luego $x = 1$.

El neutro multiplicativo es entonces $1 = 1 + 0i$

Dado $z = a + bi$, busquemos su inverso multiplicativo. Sea

$$(a + bi)(x + yi) = 1 + 0i$$

Luego $(ax - by) + (ay + bx)i = 1 + 0i$.

Tenemos un sistema de ecuaciones en \mathbb{R} :

$$\left. \begin{array}{l} (1) : ax - by = 1 \\ (2) : ay + bx = 0 \end{array} \right| \text{ Luego } \left. \begin{array}{l} a \cdot (1) : a^2x - aby = a \\ b \cdot (2) : aby + b^2x = 0 \end{array} \right|$$

$a \cdot (1) + b \cdot (2) : a^2x + b^2x = a$, luego $x = \frac{a}{a^2 + b^2}$.

Reemplazando en (1) : $a \cdot \frac{a}{a^2 + b^2} - by = 1$. Luego $y = \frac{-b}{a^2 + b^2}$

Luego

$$(a + bi)^{-1} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2}i$$

Sólo queda por demostrar que el producto es conmutativo, te lo dejamos de ejercicio. Luego (\mathbb{C}^*, \cdot) es un grupo abeliano.

Proposición 7.2.3 $(\mathbb{C}, +, \cdot)$ es un cuerpo.

Demostración. $(\mathbb{C}, +)$ y (\mathbb{C}^*, \cdot) son grupos. Además el producto se distribuye con respecto a la suma.

Observación. $i^{4n+k} = i^k; \quad \forall n, k \in \mathbb{N}$

La demostración de esta propiedad la haremos por inducción sobre n .
En efecto: $i^2 = -1$, $i^3 = i^2 \cdot i = (-1)i = -i$; $i^4 = i^2 \cdot i^2 = (-1)(-1) = 1$. Además $i^{4 \cdot 1 + k} = i^{4 \cdot 1} \cdot i^k = i^k$.

Hipótesis de inducción. Supongamos que $i^{4 \cdot n + k} = i^k$.

Demostremos: $i^{4 \cdot (n+1) + k} = i^k$

Demostración. $i^{4 \cdot (n+1) + k} = i^{4n+4+k} = i^{4n+(4+k)} = i^{4+k} = i^k$

Luego $i^{4n+k} = i^k \quad \forall n, k \in \mathbb{N}$

Cuociente de dos números complejos

$$\frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i$$

Ejemplo. $\frac{1+2i}{3+4i} = \frac{(1+2i)(3-4i)}{(3+4i)(3-4i)} = \frac{11+2i}{25} = \frac{11}{25} + \frac{2}{25}i$

Proposición 7.2.4 En \mathbb{C} no hay divisores de cero.

Demostración. Por demostrar:

$$z \cdot w = 0 \implies z = 0 \text{ o } w = 0$$

Sea $z = x + yi$ y $w = u + vi$

Sea $z \cdot w = 0$. Supongamos $z \neq 0$, es decir $x^2 + y^2 \neq 0$

Tenemos $(x + yi) \cdot (u + vi) = 0 \implies (xu - yv) + (xv + yu)i = 0 + 0i$.

Luego se deben satisfacer las ecuaciones siguientes:

$$\left. \begin{array}{l} (1) : xu - yv = 0 \\ (2) : xv + yu = 0 \end{array} \right\} \text{ Luego } \left. \begin{array}{l} x \cdot (1) : x^2u - xyv = 0 \\ y \cdot (2) : xyv + y^2u = 0 \end{array} \right\}$$

Sumando tenemos $x^2u + y^2u = 0$, luego $(x^2 + y^2) \cdot u = 0$, luego $u = 0$, pues $z \neq 0$. Consideremos ahora

$$\left. \begin{array}{l} y \cdot (1) : xyu - y^2v = 0 \\ x \cdot (2) : x^2v + xyu = 0 \end{array} \right|$$

Tenemos $x \cdot (2) - y \cdot (1) : x^2v + y^2v = 0$, luego $(x^2 + y^2)v = 0$. Entonces $v = 0$. Luego $w = 0 + 0i$. Conclusión: $w = 0$.

Hemos demostrado que si $z \neq 0$, entonces $w = 0$

Complejos conjugados

Definición 7.2.1 Si $z = a + bi$, entonces **su conjugado**, denotado por \bar{z} , es el número complejo: $\bar{z} = a - bi$

Ejercicio. Escribamos en su forma normal la expresión:

$$\begin{aligned} \frac{(1 - 5i)(5 + 10i)}{3 + 4i} &= \frac{5(1 - 5i)(1 + 2i)(3 - 4i)}{(3 + 4i)(3 - 4i)} \\ \frac{5(11 - 3i)(3 - 4i)}{3^2 + 4^2} &= \frac{21}{5} - \frac{53}{5}i \end{aligned}$$

Proposición 7.2.5 Sean $z, w \in \mathbb{C}$, entonces

$$(1) : \overline{z + w} = \bar{z} + \bar{w}$$

$$(2) : \overline{z \cdot w} = \bar{z} \cdot \bar{w}$$

Demostración. Sea $z = x + yi$ y $w = u + vi$, entonces tenemos:

$$\begin{aligned} \overline{z + w} &= \overline{(x + yi) + (u + vi)} \\ &= \overline{(x + u) + (y + v)i} \\ &= (x + u) - (y + v)i \\ &= (x - yi) + (u - vi) \\ &= \bar{z} + \bar{w} \end{aligned}$$

Demostremos ahora la segunda parte

$$\begin{aligned} \overline{z \cdot w} &= \overline{(x + yi) \cdot (u + vi)} \\ &= \overline{(x \cdot u - y \cdot v) + (x \cdot v + y \cdot u)i} \\ &= (x \cdot u - y \cdot v) - (x \cdot v + y \cdot u)i \\ &= (x - yi) \cdot (u - vi) \\ &= \bar{z} \cdot \bar{w} \end{aligned}$$

Proposición 7.2.6 Si z es un número complejo, entonces se tiene

$$(1) \quad z + \bar{z} = 2\operatorname{Re}(z)$$

$$(2) \quad z \cdot \bar{z} = \operatorname{Re}(z)^2 + \operatorname{Im}(z)^2$$

En efecto, si $z = x + yi$, entonces

$$z + \bar{z} = (x + yi) + (x - yi) = 2x = 2\operatorname{Re}(z)$$

$$z \cdot \bar{z} = (x + yi)(x - yi) = x^2 + y^2 = \operatorname{Re}(z)^2 + \operatorname{Im}(z)^2$$

Nota Observe que $z + \bar{z}$ y $z \cdot \bar{z}$ son números reales.

Este resultado va a ser de gran utilidad cuando estudiemos polinomios. No lo olvide.

7.3 Valor absoluto y distancia

Recordemos que todo número complejo $z = a + bi$ puede ser considerado como un vector que parte en el origen del sistema cartesiano y termina en el punto (a, b) . Es natural entonces el preguntarse por la longitud de este vector, el cual denotaremos : $|a + bi|$

Por el teorema de Pitágoras tenemos que:

$$|a + bi|^2 = |a|^2 + |b|^2$$

donde $|x|$ denota el valor absoluto del número real x .

Puesto que $|a|^2 = a^2$ y $|b|^2 = b^2$ y puesto que $a^2 + b^2$ es una cantidad positiva o nula, entonces siempre podemos extraer raíz de ella. Se tiene:

$$|a + bi| = \sqrt{a^2 + b^2}$$

La longitud del vector $a + bi$ es entonces $\sqrt{a^2 + b^2}$

Definición 7.3.1 El valor absoluto del número complejo $a + bi$ es la longitud del vector que comienza en el origen del sistema cartesiano y termina en el punto (a, b)

Nota. Puesto que es una longitud, es siempre una cantidad positiva y la suma de cantidades positivas es positiva. Además todo número real al cuadrado es positivo o cero.

Ejemplo. $|3 + 4i| = \sqrt{3^2 + 4^2} = 5$; $|-3 + 4i| = \sqrt{(-3)^2 + 4^2} = 5$;
 $|-3 - 4i| = \sqrt{(-3)^2 + (-4)^2} = 5$

Simplemente podemos olvidar los signos, pues todos los números están elevados al cuadrado.

Nota. $|z| = |\bar{z}|, \forall z \in \mathbb{C}$

Nota filosófica. Una longitud no puede estar definida teniendo un i^2 , pues podemos obtener cantidades negativas y la longitud es siempre positiva.

Ejemplo: $\sqrt{1^2 + (2i)^2} = \sqrt{1 - 4} = \sqrt{-3}$

Observación. Si $z \in \mathbb{C}$ entonces

1. $|z| \geq |Re(z)| \geq Re(z)$
2. $|z| \geq |Im(z)| \geq Im(z)$
3. $|z|^2 = z \cdot \bar{z}$

Esto se verifica pues $|z|^2 = |Re(z)|^2 + |Im(z)|^2$ y si quitamos un sumando que es positivo obviamente la cantidad que queda es menor o igual a la anterior. Además $z \cdot \bar{z} = (a + bi)(a - bi) = a^2 + b^2$, con $z = a + bi$

Proposición 7.3.1 Si $z, w \in \mathbb{C}$, entonces

$$|z \cdot w| = |z| \cdot |w|$$

Demostración. En efecto

$$\begin{aligned} |z \cdot w|^2 &= (z \cdot w) \cdot (\overline{z \cdot w}) \\ &= (z \cdot w) \cdot (\bar{z} \cdot \bar{w}) \\ &= (z \cdot \bar{z}) \cdot (w \cdot \bar{w}) \\ &= |z|^2 \cdot |w|^2 \end{aligned}$$

Pero $|z|$, $|w|$, $|z \cdot w|$ son cantidades positivas, luego se les puede extraer raíz cuadrada y sigue cumpliéndose la igualdad.

Teorema 7.3.2 (Desigualdad triangular o de Minkowsky) *Si z y w son números complejos, entonces se tiene*

$$|z + w| \leq |z| + |w|$$

Demostración. Si $z = a + bi$, entonces tenemos las siguientes relaciones:

$$z + \bar{z} = 2a, \quad |a| \leq |z|$$

$$\text{Luego } |z + \bar{z}| \leq 2|z|$$

Entonces

$$\begin{aligned} |z + w|^2 &= (z + w) \cdot (\overline{z + w}) \\ &= (z + w) \cdot (\bar{z} + \bar{w}) \\ &= (z \cdot \bar{z}) + w \cdot \bar{z} + z \cdot \bar{w} + w \cdot \bar{w} \\ &= |z|^2 + (z \cdot \bar{w} + \overline{z \cdot \bar{w}}) + |w|^2 \end{aligned}$$

Pero por lo dicho anteriormente

$$|(z \cdot \bar{w} + \overline{z \cdot \bar{w}})| \leq 2 \cdot |z \cdot \bar{w}| = 2 \cdot |z| \cdot |\bar{w}| = 2 \cdot |z| \cdot |w|$$

Notando que se trata de una desigualdad de números reales podemos escribir

$$|z + w|^2 \leq |z|^2 + 2 \cdot |z| \cdot |w| + |w|^2$$

es decir:

$$|z + w|^2 \leq (|z| + |w|)^2$$

Puesto que tenemos números reales no negativos, podemos extraer raíz y luego se tiene la proposición.

Corolario 7.3.3 *Si $z_1, z_2, \dots, z_n \in \mathbb{C}$, entonces se tiene*

$$|z_1 + z_2 + \dots + z_n| \leq |z_1| + |z_2| + \dots + |z_n|$$

Demostración. Por inducción sobre n

1. Para $n = 2$ tenemos

$$|z_1 + z_2| \leq |z_1| + |z_2|$$

Lo cual ha sido demostrado.

2. Supongámoslo válido hasta n
3. Por demostrar para $n + 1$, es decir, por demostrar:

$$|z_1 + z_2 + \cdots + z_{n+1}| \leq |z_1| + |z_2| + \cdots + |z_{n+1}|$$

En efecto

$$\begin{aligned} |z_1 + z_2 + \cdots + z_n + z_{n+1}| &= |(z_1 + \cdots + z_n) + z_{n+1}| \\ &\leq |z_1 + \cdots + z_n| + |z_{n+1}| \\ &\leq |z_1| + \cdots + |z_n| + |z_{n+1}| \end{aligned}$$

Corolario 7.3.4 Si $z, w \in \mathbb{C}$ entonces se tiene

$$|z - w| \geq ||z| - |w||$$

Demostración. Tenemos que: $z = z - w + w$. Utilizando la desigualdad triangular, tenemos:

$$|z| \leq |w - z| + |w|$$

Luego

$$|z| - |w| \leq |z - w| \quad (1)$$

Si cambiamos z por w , tenemos

$$|w| - |z| \leq |w - z|$$

Luego

$$-(|z| - |w|) \leq |z - w| \quad (2)$$

Pues $|w - z| = |z - w|$.

De (1) y de (2) se obtiene: $||z| - |w|| \leq |z - w|$

Noción de distancia. Queremos definir la noción de distancia entre dos números complejos.

Pensemos en los números complejos z y w , como puntos en el plano complejo. El vector que parte en z y termina en w , está definido como el número complejo $w - z$. Entonces la **distancia** entre w y z , $d(w, z)$ es la longitud del vector $w - z$.

Definición 7.3.2 Si $z, w \in \mathbb{C}$, se define la **distancia** entre z y w por $d(w, z) = |w - z|$

Nota. Si $w = a + bi$ y $z = c + di$, entonces $d(z, w) = |w - z| = |(a + bi) - (c + di)| = |(a - c) + (b - d)i| = \sqrt{(a - c)^2 + (b - d)^2}$.

Luego

$$d(w, z) = \sqrt{(a - c)^2 + (b - d)^2}$$

Nota. Desde el momento que tenemos el concepto de distancia, podemos definir lugares geométricos. Como vemos en los ejercicios siguientes.

Ejemplos

1. La expresión algebraica del lugar geométrico de todos los puntos del plano que están a 2 unidades de distancia del origen del plano complejo, es la siguiente:

$$\{z; |z - 0| = 2\} = \{z; |z| = 2\}$$

que corresponde a una circunferencia con centro en el origen y radio 2.

2. La expresión algebraica de todos los puntos del plano que están a 3 unidades del número complejo $1 + i$ es la siguiente:

$$\{z; |z - (1 + i)| = 3\}$$

que corresponde a una circunferencia con centro en el punto $(1, 1)$ y radio 3.

7.4 Forma polar o trigonométrica de un número complejo

Sea $z = a + bi$, un número complejo. Supongamos z en el primer cuadrante y supongamos que forma un ángulo θ con el lado positivo del eje real, en el sistema cartesiano.

Tenemos: $\cos \theta = \frac{x}{|z|}$ y $\sin \theta = \frac{y}{|z|}$

Luego $x = |z| \cos \theta$; $y = |z| \sin \theta$. De donde

$z = x + yi = |z| \cos \theta + i|z| \sin \theta$. Se tiene entonces que

$$z = |z|(\cos \theta + i \sin \theta)$$

Llamada forma polar o trigonométrica de un número complejo de módulo $|z|$ y argumento θ , denotado $Arg(z)$.

Se obtiene la misma fórmula si consideramos el número complejo en los otros tres cuadrantes.

Ejemplos de escritura en forma polar

1. Sea $z = \sqrt{2} + i\sqrt{2}$. Entonces

$$|z| = \sqrt{(\sqrt{2})^2 + (\sqrt{2})^2} = \sqrt{4} = 2 \text{ y } Arg(z) = \frac{\pi}{4}$$

Luego

$$z = 2(\cos \frac{\pi}{4} + i \sin \frac{\pi}{4})$$

2. Sea $z = 5\sqrt{3} + 5i$.

$$|z| = \sqrt{5^2(\sqrt{3})^2 + 5^2} = \sqrt{5^2(3+1)} = 5\sqrt{4} = 10$$

$$z = 10(\frac{\sqrt{3}}{2} + \frac{1}{2}i)$$

Luego

$$z = 10(\cos \frac{\pi}{6} + i \sin \frac{\pi}{6})$$

3. Sea $z = -3 + 3\sqrt{3}i$

Tenemos

$$z = 6\left(\frac{-1}{2} + \frac{\sqrt{3}}{2}i\right)$$

Luego

$$z = 6\left(\cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3}\right)$$

4. Sea $z = -7 - 7i$. Entonces

$$|z| = \sqrt{(-7)^2 + (-7)^2} = \sqrt{2 \cdot 49} = 7\sqrt{2}$$

$$\operatorname{tg}\theta = \frac{-7}{-7} = 1$$

Luego $\theta = \frac{\pi}{4}$ o bien $\theta = \frac{5\pi}{4}$. Puesto que este número complejo se encuentra en el tercer cuadrante, el $\operatorname{Arg}(z) = \frac{5\pi}{4}$. De donde, la forma polar de este número complejo es

$$z = 7\sqrt{2}\left(\cos \frac{5\pi}{4} + i \sin \frac{5\pi}{4}\right)$$

Para un ángulo cualquiera. Sea $z = x + yi$, con $\operatorname{Arg}(z) = \theta$, luego $\operatorname{tg}(\theta) = \frac{y}{x}$. Debemos comenzar por ver en qué cuadrante se encuentra z . Hay dos ángulos entre 0 y 2π que cumplen la ecuación de la tangente y con la información del cuadrante al que pertenece z , se obtiene el ángulo θ .

7.5 Multiplicación de números complejos

Proposición 7.5.1 Sea $z = r(\cos \alpha + i \sin \alpha)$ y $w = s(\cos \beta + i \sin \beta)$. Entonces

$$z \cdot w = (r \cdot s)(\cos(\alpha + \beta) + i \sin(\alpha + \beta))$$

Demostración.

$$\begin{aligned}
z \cdot w &= (r(\cos \alpha + i \sin \alpha)) \cdot (s(\cos \beta + i \sin \beta)) \\
&= r \cdot s[(\cos \alpha \cos \beta - \sin \alpha \sin \beta) + i(\cos \alpha \sin \beta + \sin \alpha \cos \beta)] \\
&= r \cdot s(\cos(\alpha + \beta) + i \sin(\alpha + \beta))
\end{aligned}$$

Nota. La proposición nos dice que al multiplicar dos números complejos, se multiplican los módulos y se suman los argumentos.

Ejemplo. Sea $z = \frac{1}{2} + \frac{\sqrt{3}}{2}i$ y $w = 3\sqrt{3} + 3i$.

Escribiendo estos números complejos en su forma polar se tiene

$$z = 1(\cos \frac{\pi}{3} + i \sin \frac{\pi}{3}); \quad w = 6(\cos \frac{\pi}{6} + i \sin \frac{\pi}{6})$$

Su producto es

$$z \cdot w = 6[\cos(\frac{\pi}{3} + \frac{\pi}{6}) + i \sin(\frac{\pi}{3} + \frac{\pi}{6})]$$

Luego

$$z \cdot w = 6(\cos \frac{\pi}{2} + i \sin \frac{\pi}{2})$$

En su forma normal, tenemos

$$z \cdot w = 6(0 + i \cdot 1) = 6i$$

7.6 Elevación a potencia

Proposición 7.6.1 Sea $z = r(\cos \theta + i \sin \theta)$. Entonces

$$z^n = r^n(\cos n\theta + i \sin n\theta), \quad \forall n \in \mathbb{N}$$

Demostración. La demostración la haremos por inducción sobre n

1. Demostremos que es válido para $n = 2$

$$\begin{aligned}
z^2 &= [r(\cos \theta + i \sin \theta)] \cdot [r(\cos \theta + i \sin \theta)] \\
&= r^2[(\cos^2 \theta - \sin^2 \theta) + i(2 \cos \theta \sin \theta)] \\
&= r^2(\cos 2\theta + i \sin 2\theta)
\end{aligned}$$

2. Hipótesis de inducción. Supongamos que

$$z^n = r^n(\cos n\theta + i \sin n\theta), \quad n \in \mathbb{N}$$

3. Por demostrar

$$z^{n+1} = r^{n+1}(\cos(n+1)\theta + i \sin(n+1)\theta)$$

Demostración

$$\begin{aligned} z^{n+1} &= z^n \cdot z \\ &= [r^n(\cos n\theta + i \sin n\theta)] \cdot [r(\cos \theta + i \sin \theta)] \\ &= r^{n+1}[(\cos n\theta \cos \theta - \sin n\theta \sin \theta) + i(\cos n\theta \sin \theta + \sin n\theta \cos \theta)] \\ &= r^{n+1}(\cos(n+1)\theta + i \sin(n+1)\theta) \end{aligned}$$

Por (1), (2) y (3) se tiene que esta propiedad es verdadera para todo número natural.

Ejemplo. Sea $z = 5(\cos \frac{\pi}{3} + i \sin \frac{\pi}{3})$. Entonces

$$\begin{aligned} z^3 &= 5^3(\cos \frac{3\pi}{3} + i \sin \frac{3\pi}{3}) \\ &= 5^3(\cos \pi + i \sin \pi) \\ &= -5^3 \end{aligned}$$

$$\begin{aligned} z^5 &= 5^5(\cos \frac{5\pi}{3} + i \sin \frac{5\pi}{3}) \\ &= 5^5(\frac{1}{2} - \frac{\sqrt{3}}{2}i) \\ &= \frac{5^5}{2} - \frac{5^5\sqrt{3}}{2}i \end{aligned}$$

$$\begin{aligned} z^6 &= 5^6(\cos \frac{6\pi}{3} + i \sin \frac{6\pi}{3}) \\ &= 5^6(1 + 0i) \\ &= 5^6 \end{aligned}$$

7.7 Inversos multiplicativos.

Busquemos el inverso multiplicativo de:

$$z = r(\cos \theta + i \sin \theta)$$

Sea $w = s(\cos \alpha + i \sin \alpha)$ su inverso multiplicativo. Entonces $z \cdot w = 1$.
Luego

$$r \cdot s(\cos(\theta + \alpha) + i \sin(\theta + \alpha)) = 1(\cos 0 + i \sin 0)$$

Luego $\theta + \alpha = 0 + 2k\pi$; $k \in \mathbb{Z}$; de donde $\alpha = -\theta$. Luego

$$z^{-1} = \frac{1}{r}(\cos -\theta + i \sin -\theta)$$

Ejemplo. Sea $z = 10(\cos 25^\circ + i \sin 25^\circ)$.

Entonces

$$z^{-1} = \frac{1}{10}(\cos -25^\circ + i \sin -25^\circ)$$

o bien

$$z^{-1} = \frac{1}{10}(\cos 335^\circ + i \sin 335^\circ)$$

Proposición 7.7.1 Sea $z = r(\cos \theta + i \sin \theta)$. Entonces

$$z^n = r^n(\cos n\theta + i \sin n\theta); \quad n \in \mathbb{Z}$$

Demostración. Para $n \geq 0$, está demostrado.

Para $n = -1$, también está demostrado.

Sea $n \in \mathbb{Z}$ tal que $n < -1$. Sea $n = -m$; $m \in \mathbb{N}$. Sabemos que:

$$z^{-m} = (z^{-1})^m \quad y \quad z^{-1} = r^{-1}(\cos -\theta + i \sin -\theta)$$

$$\begin{aligned} z^n &= z^{-m} = (z^{-1})^m \\ &= (r^{-1}(\cos -\theta + i \sin -\theta))^m \\ &= r^{-m}(\cos m(-\theta) + i \sin m(-\theta)) \\ &= r^{-m}(\cos -m\theta + i \sin -m\theta) \\ &= r^n(\cos n\theta + i \sin n\theta) \end{aligned}$$

Queda esto demostrado.

Ejemplo. Sea $z = 7(\cos \theta + i \sin \theta)$, entonces

$$z^{-5} = \left(\frac{1}{7}\right)^5 (\cos -5\theta + i \sin -5\theta)$$

7.8 Extracción de raíces

Sea $z = r(\cos \theta + i \sin \theta)$

Nos proponemos encontrar las raíces n -ésimas de z , es decir todos aquellos números complejos $w = s(\cos \alpha + i \sin \alpha)$, que satisfacen

$$w^n = z; \quad n \in \mathbb{Z}$$

Para ello se tiene la siguiente

Proposición 7.8.1 *Sea $z = r(\cos \theta + i \sin \theta)$. Entonces las raíces n -ésimas de z son:*

$$w_k = \sqrt[n]{r} \left(\cos \left(\frac{\theta}{n} + k \cdot \frac{2\pi}{n} \right) + i \sin \left(\frac{\theta}{n} + k \cdot \frac{2\pi}{n} \right) \right); \quad k \in \mathbb{Z}; 0 \leq k \leq n-1$$

Demostración.

Sea $w = s(\cos \alpha + i \sin \alpha)$ tal que $w^n = z; \quad n \in \mathbb{Z}$

Luego

$$s^n (\cos n\alpha + i \sin n\alpha) = r(\cos \theta + i \sin \theta)$$

Esta igualdad se desdobla en dos ecuaciones

$$\left. \begin{array}{lcl} (1) : s^n & = & r \\ (2) : n\alpha & = & \theta + 2k\pi \end{array} \right\}$$

Luego $s = \sqrt[n]{r}; \quad \alpha = \frac{\theta}{n} + k \cdot \frac{2\pi}{n}$. Luego

$$w_k = \sqrt[n]{r} \left(\cos \left(\frac{\theta}{n} + k \cdot \frac{2\pi}{n} \right) + i \sin \left(\frac{\theta}{n} + k \cdot \frac{2\pi}{n} \right) \right); \quad k \in \mathbb{Z}$$

Cada vez que sumamos $\frac{2\pi}{n}$, obtenemos la raíz siguiente. Dado que el período de las funciones seno y coseno es 2π , obtenemos todas las raíces si hacemos variar k entre 0 y $n - 1$. Es decir $0 \leq k \leq n - 1$.

Ejercicios Resueltos

1. Busquemos las raíces cuartas de la unidad.

Solución. En este caso tenemos

$$z = 1(\cos 0 + i \sin 0)$$

Todas las raíces tienen por módulo $\sqrt[4]{1} = 1$. La primera raíz tiene por argumento $\frac{0}{4} = 0$. Entonces

$$z_0 = 1(\cos 0 + i \sin 0) = 1$$

Para obtener la segunda raíz debemos sumar $\frac{2\pi}{4} = \frac{\pi}{2}$. Tenemos

$$z_1 = (\cos \frac{\pi}{2} + i \sin \frac{\pi}{2}) = i$$

Nuevamente volvemos a sumar $\frac{\pi}{2}$ al ángulo de z_1 . Tenemos:

$$z_2 = 1(\cos \pi + i \sin \pi) = -1$$

Lo mismo para obtener z_3

$$z_3 = 1(\cos \frac{3\pi}{2} + i \sin \frac{3\pi}{2}) = -i$$

Entonces z_0, z_1, z_2, z_3 son las raíces cuartas de la unidad.

2. Busquemos las raíces cúbicas de $z = -i$

Solución.

$$z = -i = 1(\cos \frac{3\pi}{2} + i \sin \frac{3\pi}{2})$$

Entonces sus raíces son las siguientes:

$$z_0 = \sqrt[3]{1}(\cos \frac{3\pi}{6} + i \sin \frac{3\pi}{6}) = \cos \frac{\pi}{2} + i \sin \frac{\pi}{2}$$

Para obtener la siguiente raíz debemos sumar $\frac{2\pi}{3}$ al argumento de z_0 . Tenemos:

$$\frac{\pi}{2} + \frac{2\pi}{3} = \frac{7\pi}{6}$$

Luego

$$z_1 = \cos \frac{7\pi}{6} + i \sin \frac{7\pi}{6}$$

Ahora debemos sumar $\frac{2\pi}{3}$ al argumento de z_1 . Luego la tercera raíz tiene argumento:

$$\frac{7\pi}{6} + \frac{2\pi}{3} = \frac{11\pi}{6}$$

y se tiene:

$$z_2 = \cos \frac{11\pi}{6} + i \sin \frac{11\pi}{6}$$

z_0, z_1 y z_2 son las tres raíces cúbicas del complejo $z = -i$.

Proposición 7.8.2 Sea $z = r(\cos \theta + i \sin \theta)$. Entonces

$$z^{\frac{m}{n}} = \sqrt[n]{r^m} \left(\cos \left(\frac{m\theta}{n} + k \cdot \frac{2\pi}{n} \right) + i \sin \left(\frac{m\theta}{n} + k \cdot \frac{2\pi}{n} \right) \right); \quad n, m, k \in \mathbb{Z}$$

$$0 < k < n$$

Esta fórmula es conocida como la fórmula de "De Moivre"

Demostración.

$$\begin{aligned} z^{\frac{m}{n}} &= (z^m)^{\frac{1}{n}} \\ &= (r^m(\cos m\theta) + i \sin m\theta)^{\frac{1}{n}} \\ &= \sqrt[n]{r^m} \left(\cos \left(\frac{m\theta}{n} + k \cdot \frac{2\pi}{n} \right) + i \sin \left(\frac{m\theta}{n} + k \cdot \frac{2\pi}{n} \right) \right) \end{aligned}$$

Proposición 7.8.3 Sea $z \in \mathbb{C}$ y sea ζ una raíz n -ésima de la unidad. Entonces las raíces n -ésimas de z , pueden ser obtenidas de la manera siguiente:

$$z_0, z_0\zeta, z_0\zeta^2, \dots, z_0\zeta^{n-1}$$

Donde z_0 es una raíz n -ésima de z .

Demostración. Al multiplicar por una raíz n -ésima de la unidad, no varía el módulo del complejo, sólo varía el ángulo. La raíz $z_0\zeta$, se encuentra a un ángulo $\frac{2\pi}{n}$ de z_0 , luego es la raíz siguiente a z_0 y así sucesivamente.

Ejercicios Resueltos

1. Demostremos que

$$|z - w|^2 + |z + w|^2 = 2(|z|^2 + |w|^2)$$

Solución.

$$\begin{aligned} |z - w|^2 + |z + w|^2 &= (z - w) \cdot \overline{(z - w)} + (z + w) \cdot \overline{(z + w)} \\ &= (z - w)(\bar{z} - \bar{w}) + (z + w)(\bar{z} + \bar{w}) \\ &= z\bar{z} - z\bar{w} - \bar{z}w + w\bar{w} + z\bar{z} + z\bar{w} + \bar{z}w + w\bar{w} \\ &= 2z\bar{z} + 2w\bar{w} \\ &= 2(|z|^2 + |w|^2) \end{aligned}$$

2. Demostremos que:

$$|z|^{-1} \cdot |z - w| \cdot |w|^{-1} = |z^{-1} - w^{-1}|$$

Solución.

$$\begin{aligned} |z|^{-1} \cdot |z - w| \cdot |w|^{-1} &= |z^{-1} \cdot (z - w) \cdot w^{-1}| \\ &= |z^{-1} \cdot z \cdot w^{-1} - z^{-1} \cdot w \cdot w^{-1}| \\ &= |w^{-1} - z^{-1}| \\ &= |z^{-1} - w^{-1}| \end{aligned}$$

3. Demostremos que:

$$\left| \frac{1 - z}{\bar{z} - 1} \right| = 1$$

Solución. $\left| \frac{1 - z}{\bar{z} - 1} \right| = \left| \frac{1 - z}{z - 1} \right| = \left| \frac{(1 - z)(z - 1)}{(z - 1)(z - 1)} \right| = \left| \frac{-(1 - z)^2}{|z - 1|^2} \right| =$

$$\frac{|1 - z|^2}{|1 - z|^2} = 1$$

4. Busquemos las raíces cuadradas de $z = 25i$

Solución. Las dos raíces tienen $|z| = 25$. Tenemos que z escrito en su forma polar es:

$$z = 25\left(\cos \frac{\pi}{2} + i \sin \frac{\pi}{2}\right)$$

Para obtener la primera raíz, debemos dividir el argumento de z por 2. Luego la primera raíz tiene argumento $\frac{\pi}{4}$. Esta es

$$z_0 = 5\left(\cos \frac{\pi}{4} + i \sin \frac{\pi}{4}\right)$$

Debemos sumar $\frac{2\pi}{2} = \pi$ al argumento de z_0 . Tenemos

$$z_1 = 5\left(\cos \frac{5\pi}{4} + i \sin \frac{5\pi}{4}\right)$$

Los dos raíces, z_0 y z_1 escritas en su forma normal son:

$$z_0 = \frac{5\sqrt{2}}{2} + \frac{5\sqrt{2}}{2}i; \quad z_1 = \frac{-5\sqrt{2}}{2} + \frac{-5\sqrt{2}}{2}i$$

7.9 Forma exponencial de un número complejo

Vimos que para multiplicar dos números complejos escritos en su forma polar se multiplican los módulos y se suman los argumentos, es decir:

$$(r(\cos \alpha + i \sin \alpha)) \cdot (t(\cos \beta + i \sin \beta)) = r \cdot t(\cos(\alpha + \beta) + i \sin(\alpha + \beta))$$

Consideremos la función $f : \mathbb{R} \rightarrow \mathbb{C}$, tal que $f(x) = \cos x + i \sin x$.

L.Euler(1707-1783), demostró la formula:

$$e^{ix} = \cos x + i \sin x$$

Esta función tiene las siguientes propiedades:

$$\begin{aligned}\overline{e^{ix}} &= e^{-ix} = (e^{ix})^{-1} \\ |e^{ix}| &= 1 \\ e^{ix} \cdot e^{iy} &= e^{i(x+y)} \\ e^{i\alpha} &= e^{i(\alpha+2k\pi)}, \quad k \in \mathbb{Z} \\ z &= |z|e^{i\text{Arg}(z)}, \quad \forall z \in \mathbb{C}\end{aligned}$$

Demostración. En efecto,

$$\overline{e^{ix}} = \overline{\cos x + i \sin x} = \cos x - i \sin x = \cos(-x) + i \sin(-x) = e^{i(-x)} = e^{-ix}$$

Como ejercicio queda demostrar que $e^{-ix} = (e^{ix})^{-1}$

Para demostrar la segunda propiedad tenemos:

$$|e^{ix}| = |\cos x + i \sin x| = \sqrt{\cos^2 x + \sin^2 x} = 1$$

En cuanto a la tercera propiedad,

$$e^{ix} \cdot e^{iy} = (\cos x + i \sin x)(\cos y + i \sin y) = \cos(x+y) + i \sin(x+y) = e^{i(x+y)}$$

Las dos restantes propiedades quedan de ejercicio para el lector.

Ejercicios Resueltos

1. ¿Qué condiciones debe cumplir z y w para tener

$$|z + w| = |z| + |w|?$$

Solución. Sea $z = a + bi$ y $w = c + di$. Luego supongamos que tenemos la igualdad, para ver las condiciones que cumplen z y w .

$$|(a + bi) + (c + di)| = |a + bi| + |c + di|$$

Entonces

$$\sqrt{(a+c)^2 + (b+d)^2} = \sqrt{a^2 + b^2} + \sqrt{c^2 + d^2}$$

$$a^2 + 2ac + c^2 + b^2 + 2bd + d^2 = a^2 + b^2 + c^2 + d^2 + 2\sqrt{(a^2 + b^2)(c^2 + d^2)}$$

Luego

$$\begin{aligned}ac + bd &= \sqrt{a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2}/^2 \\a^2c^2 + b^2d^2 + 2abcd &= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 \\0 &= a^2d^2 + b^2c^2 - 2abcd\end{aligned}$$

Luego $(ad - bc)^2 = 0$, de donde $ad - bc = 0$, es decir $ad = bc$
Tenemos

$$dz = da + dbi = bc + dbi = b(c + di) = bw$$

Luego $dz = bw$, es decir z y w son colineales.

2. Sea $z = \frac{\sqrt{3}}{2} + \frac{1}{2}i$. Calculemos z^{3525}

Solución. Comencemos por escribir z en su forma polar. Tenemos

$$z = \cos \frac{\pi}{6} + i \sin \frac{\pi}{6}$$

Entonces:

$$z^{3525} = \cos 3525 \cdot \frac{\pi}{6} + i \sin 3525 \cdot \frac{\pi}{6} = e^{i3525 \frac{\pi}{6}}$$

Se tiene que $3525 = 293 \cdot 12 + 9$, reemplazando en la expresión anterior, tenemos:

$$\begin{aligned}z^{3525} &= e^{i(293 \cdot 12 + 9) \frac{\pi}{6}} = e^{i(293 \cdot 2\pi + \frac{9\pi}{6})} = e^{i \cdot \frac{3\pi}{2}} \\z^{3525} &= \cos \frac{3\pi}{2} + i \sin \frac{3\pi}{2} = 0 + i(-1) = -i\end{aligned}$$

Luego

$$z^{3525} = -i$$

3. Describamos el lugar geométrico dado por

$$\{z \in \mathbb{C}; |\bar{z} + 5| < 3\}$$

Solución. Sea $z = x + yi$. Luego

$$\begin{aligned}|x - yi + 5| < 3 &\quad \text{ssi} \quad |(x + 5) - yi| < 3 \\&\quad \text{ssi} \quad \sqrt{(x + 5)^2 + (-y)^2} < 3 \\&\quad \text{ssi} \quad (x + 5)^2 + (y)^2 < 9\end{aligned}$$

Representa el conjunto de todos los números complejos que están dentro de la circunferencia con centro en $(-5, 0)$ y radio 3.

4. Resolvamos en \mathbb{C} , la ecuación siguiente:

$$z^2 - \sqrt{3}z + 1 = 0$$

Solución. Sea $z = x + yi$. Reemplazando en la ecuación, tenemos:

$$(x + yi)^2 - \sqrt{3}(x + yi) + 1 = 0$$

Luego:

$$x^2 - y^2 + 2xyi - \sqrt{3}x - \sqrt{3}yi + 1 = 0$$

Por la definición de igualdad de números complejos, tenemos, en \mathbb{R} , el sistema de ecuaciones siguiente:

$$\left. \begin{array}{rcl} x^2 - y^2 - \sqrt{3}x + 1 & = & 0 \\ 2xy - \sqrt{3}y & = & 0 \end{array} \right|$$

La segunda ecuación queda: $y(2x - \sqrt{3}) = 0$

Si $y = 0$, reemplazamos en la 1^{era} ecuación, se obtiene

$$x^2 - \sqrt{3}x + 1 = 0$$

de donde

$$x = \frac{\sqrt{3} \pm \sqrt{3-4}}{2} \notin \mathbb{R}$$

luego $y \neq 0$. Entonces $2x - \sqrt{3} = 0$, de donde $x = \frac{\sqrt{3}}{2}$

Reemplazando en la 1^{era} ecuación, tenemos:

$$\frac{3}{4} - y^2 - \sqrt{3} \cdot \frac{\sqrt{3}}{2} + 1 = 0$$

Luego $y^2 = \frac{1}{4}$. De donde $y = \pm \frac{1}{2}$.

Las soluciones de la ecuación son entonces:

$$z_1 = \frac{\sqrt{3}}{2} + \frac{1}{2}i \quad \text{y} \quad z_2 = \frac{\sqrt{3}}{2} - \frac{1}{2}i$$

5. Sean $z, w \in \mathbb{C}$. Entonces

$$z\bar{w} + \bar{z}w = 2|z \cdot w| \cos \phi$$

Donde ϕ es el ángulo comprendido entre z y w .

Solución. Sea $z = r(\cos \alpha + i \sin \alpha)$ y $w = t(\cos \beta + i \sin \beta)$.
Entonces:

$$\begin{aligned} z \cdot \bar{w} + \bar{z} \cdot w &= \\ rt(\cos(\alpha - \beta)) + i \sin(\alpha - \beta) + rt(\cos(-\alpha + \beta) + i \sin(-\alpha + \beta)) &= \\ rt(\cos(\alpha - \beta)) + i \sin(\alpha - \beta) + rt(\cos(\alpha - \beta) - i \sin(\alpha - \beta)) &= \\ 2rt \cos(\alpha - \beta) &= \\ 2|z| \cdot |w| \cos(\alpha - \beta) &= \\ 2|zw| \cos(\alpha - \beta) \end{aligned}$$

7.10 Ejercicios Propuestos

1. Compruebe que:

$$\begin{aligned} a) (1 - i\sqrt{3})i + (2i - \sqrt{3}) &= 3i; \quad b) \frac{10}{(1 - 2i)(3 + i)} = 1 + i; \\ c) (2 - \frac{1}{2}i)^4 &= 10\frac{1}{16} - 15i \end{aligned}$$

2. Escriba en la forma normal los siguientes números complejos:

$$\begin{aligned} a) \frac{(1-2i)}{(-3+2i)}; \quad b) (1+3i)^2 - (1-3i)^2; \quad c) \frac{a+bi}{a-bi} \\ d) (2-3i)^2 - (2+3i)^2; \quad e) (\frac{1}{2} + \frac{\sqrt{3}}{2}i)^3 - (\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i)^2; \quad d) (1+i)^4 \end{aligned}$$

3. Simplifique $\frac{a-bi}{c+di} + \frac{a+bi}{c-di}$

4. Sea $\omega = \frac{-1+i\sqrt{3}}{2}$. Encuentre $\omega^2, \omega^3, 1 + \omega + \omega^2$

5. Resuelva la ecuación: $z^2 = \frac{1}{2} + \frac{\sqrt{3}}{2}i$

6. Averigüe cuales de los siguientes números complejos son puramente imaginarios

a) $z + \bar{z}$ b) $z - \bar{z}$ c) $z \cdot \bar{z}$ d) $z_1 \bar{z}_2 + \bar{z}_1 z_2$

7. Encuentre mentalmente el valor de:

a) $(\frac{1}{2} + \frac{\sqrt{3}}{2}i)(\frac{1}{2} - \frac{\sqrt{3}}{2}i)$; b) $(\frac{1}{2} + \frac{\sqrt{3}}{2}i) + (\frac{1}{2} - \frac{\sqrt{3}}{2}i)$;
 c) $(3 + 4i)(3 - 4i)$; d) $(3 + 4i) + (3 - 4i)$

8. Escriba en su forma polar cada uno de los siguientes números complejos:

a) $\frac{1}{2} + \frac{\sqrt{3}}{2}i$; b) $\frac{\sqrt{3}}{2} + \frac{1}{2}i$; c) $-\frac{1}{2} - \frac{\sqrt{3}}{2}i$; d) $-\frac{\sqrt{3}}{2} - \frac{1}{2}i$
 e) $\frac{1}{2} - \frac{\sqrt{3}}{2}i$; f) $\frac{\sqrt{3}}{2} - \frac{1}{2}i$; g) $\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$; h) $-\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$
 i) $-\sqrt{3} - i$; j) $-\sqrt{3} + i$; k) $\sqrt{2} - \sqrt{2}i$; l) $1 - i$

9. Demuestre que:

a) $|\bar{z}| = |z|$ b) $|z^{-1}| = |z|^{-1}$ c) $|z|^2 = \operatorname{Re}(z)^2 + \operatorname{Im}(z)^2$

10. Encuentre un número complejo z que satisfaga :

a) $z = 2(z - (1 - 3i))$; b) $\frac{z-3}{z-2i} = \frac{1}{2}$

11. Describa geométricamente la región determinada por cada una de las siguientes condiciones:

a) $\operatorname{Im} z \geq 2$ b) $|\operatorname{Im} z| < 2$ c) $|z| \leq 1$
 d) $|z + 3| = 5$ e) $|z - 3i| > 5$ f) $|z - (1 + 2i)| \leq 2$

12. Sea z_0 un número complejo fijo y r una constante positiva. Demuestre que z está sobre la circunsferencia de radio r y centro z_0 cuando z satisface la ecuación : $|z - z_0| = r$.

13. Determine la totalidad de números complejos que satisfacen cada una de las siguientes condiciones:

a) $\bar{z} = \bar{z}^{-1}$ b) $z^{-1} = -z$ c) $|z + 3| = |z + 1|$ d) $z = z^{-2}$.

14. Dados los complejos

$$z_1 = \sqrt{3} + i, \quad z_2 = -\sqrt{3} + 3i, \quad z_3 = 2 - 2\sqrt{3}i$$

Calcule $2z_1 - (z_2^2 - z_3) - \frac{z_2}{z_1}$.

15. Exprese z en la forma $a + bi$, donde:

$$\text{a) } z = \frac{\sqrt{2} + \sqrt{3}i}{\sqrt{2} - \sqrt{3}i} \quad \text{b) } z = 1 + \frac{i}{1 + \frac{i}{1 + \frac{i}{1 + i}}}$$

16. Exprese en forma polar:

$$\text{a) } z_1 = \sqrt{3} + i, \quad \text{b) } z_2 = -2 - 2\sqrt{3}i, \quad \text{c) } z_3 = -1 - i, \\ \text{d) } z_4 = -3i$$

Además calcule $z_1 z_2$, $\frac{z_1 z_3}{z_4}$, z_k^{-1} , $\frac{z_1 z_2^{-1}}{z_k}$, z_k^{3525} con $k = 1, 2, 3, 4$

17. Calcule z^2 , siendo $z = -| -1 + i | + \sqrt{2}i$.

18. Dado $z = 1 + \operatorname{sen}\theta + i\cos\theta$, calcular $|z^2 - \bar{z}|$.

19. Determine los reales a y b que satisfacen:

$$(-1 + i)a + (1 + 2i)b = 1.$$

20. Resuelva las ecuaciones:

$$\text{(a) } z^2 = i$$

$$\text{(b) } z^3 - 2 + 2i = 0$$

$$\text{(c) } (z - 1 - i)(z - 1 + i)(z + 1 + i)(z + 1 - i) = 5$$

$$\text{(d) } z^2 + (-2 - 2i)z = 3 - 6i$$

21. Resuelva el siguiente sistema:

$$\begin{array}{lcl} \text{a) } (1 + i)x - iy & = & 2 + i \\ \text{b) } (2 + i)x + (2 - i)y & = & 2i \end{array}$$

22. Calcule y grafique:

$$\begin{array}{lll} \text{a) } \sqrt{1 + i\sqrt{3}} & \text{b) } \sqrt[3]{-8} & \text{c) } \sqrt[4]{8i} \\ \text{d) } \sqrt[4]{1 - i} & \text{e) } \sqrt[3]{-i} & \text{f) } \sqrt[3]{\sqrt{3} + i}. \end{array}$$

23. Grafique los siguientes conjuntos en el plano complejo:

$$\begin{array}{ll} a) \operatorname{Re}(z) = -2 & b) -2 \leq \operatorname{Im}(z) < 3 \\ c) \frac{\pi}{4} \leq \operatorname{Arg}(z) \leq \frac{3\pi}{4} \mid |z| < 2 & d) z - \bar{z} = i \\ e) |z| = z + \bar{z} & f) \bar{z} - z^{-1} = 0 \\ g) z + z^{-1} \in \mathbb{R} & h) z = \bar{z}^2 \\ i) |z+1| + |z-1| = 3 & j) |z+c| \mid |z-c| = c^2 \end{array}$$

24. Diga cuáles de los siguientes números están sobre el eje X o sobre el eje Y :

$$\begin{array}{ll} a) z^2 - (\bar{z})^2 & b) \frac{1}{z-\bar{z}} \left(\frac{1}{z} + \frac{1}{\bar{z}} \right) (z + \bar{z}) \\ c) z_1 \bar{z}_2 + \bar{z}_1 z_2 & d) z_1 \bar{z}_2 - \bar{z}_1 z_2 \end{array}$$

25. Pruebe que:

$$a) \operatorname{Re}(z\bar{\omega} + \bar{z}\omega) = z\bar{\omega} + \bar{z}\omega \quad b) -2\operatorname{Im}(z\bar{\omega} - \bar{z}\omega)i = z\bar{\omega} - \bar{z}\omega$$

26. Demuestre que:

$$|4z+1| = 2|z+1| \implies |z| = \frac{1}{2}$$

27. Pruebe que si $z \in \mathbb{C}$ satisface $az^2 + bz + c = 0$, con $a, b, c \in \mathbb{R}$, entonces $a(\bar{z})^2 + b\bar{z} + c = 0$

28. Sea z_0 en los complejos y $r > 0$. Demuestre que z está sobre una circunferencia de radio r y centro en $-z_0$, cuando z satisface cualquiera de las condiciones:

$$a) |z + z_0| = r \quad b) z\bar{z} + z\bar{z}_0 + \bar{z}z_0 + z_0\bar{z}_0 = r^2$$

29. Pruebe que:

$$\begin{array}{l} a) \text{ Si } z + \frac{1}{z} \in \mathbb{R} \text{ entonces } \operatorname{Im}(z) = 0 \text{ o } |z| = 1 \\ b) \text{ Si } |z| = 1 \text{ entonces } \left| \frac{z+\omega}{1+\bar{z}\omega} \right| = 1 \quad \forall \omega \in \mathbb{C} \end{array}$$

30. a) Demuestre que la ecuación $z\bar{z} - 2|z| + 1 = 0$ tiene infinitas soluciones

b) Demuestre que la ecuación $|z|^2 + 2\sqrt{z\bar{z}} + 1 = 0$, no tiene solución en los complejos

31. Sea $\omega \neq 1$, una raíz n -ésima de 1. Pruebe que

$$\omega^{n-1} + \omega^{n-2} + \dots + \omega^2 + \omega + 1 = 0$$

32. Si $\omega \neq 1$ es una raíz cúbica de 1, entonces $(1 - \omega)(1 - \omega^2) = 3$

33. Se define la exponencial compleja por: $e^z = e^x(\cos(y) + i\sin(y))$, donde $z = x + iy$. Pruebe que:

$$\begin{array}{ll} a) e^z \neq 0 & \forall z \in \mathbb{C} \\ b) e^{z+\omega} = e^z e^\omega & \forall z, \omega \in \mathbb{C} \\ c) (e^z)^{-1} = e^{-z} & \forall z \in \mathbb{C} \end{array}$$

34. Se define el seno y coseno de z en \mathbb{C} , por:

$$\sin(z) = \frac{1}{2i}(e^{iz} - e^{-iz}) \quad \cos(z) = \frac{1}{2}(e^{iz} + e^{-iz})$$

Pruebe que:

$$a) \sin(z + \omega) = \sin(z)\cos(\omega) + \cos(z)\sin(\omega)$$

$$b) \cos(z + \omega) = \cos(z)\cos(\omega) - \sin(z)\sin(\omega)$$

35. Demuestre que $\cos\alpha + \sin\alpha = \cos\beta + \sin\beta$ si y solo si $\alpha - \beta = 2k\pi$ donde k es un número entero.

36. Pruebe que, dado $\omega \in \mathbb{C}, \omega \neq 0$, entonces:

$$e^z = \omega \Leftrightarrow z = \ln|\omega| + i(\theta + 2k\pi)$$

donde θ es un argumento de ω y k es cualquier número entero.

37. Dado $z \in \mathbb{C}, z \neq 0, z = |z|(\cos\theta + i\sin\theta)$, denotemos por $\log(z)$, a cualquier complejo de la forma $\ln|z| + i(\theta + 2k\pi)$, donde k es un entero.

Calcule $\log(-1), \log(i), \log(-i)$.

Capítulo 8

Polinomios

8.1 Definiciones

Introducción

La más hermosa definición de polinomio se la vamos a dejar a aquellos alumnos que deseen conocer más profundamente las matemáticas. En este curso sólo veremos una definición formal de polinomios. Observemos que la palabra formal viene de forma. Se refiere a que solamente conoceremos su forma, pero, no su esencia. Estos entes matemáticos tiene esta forma y se trabaja de tal manera con ellos.

Ejemplos

1. $P(X) = X^3 - 7X^5 + \pi X^{24}$, es un polinomio.
Coeficientes: $1, -7, \pi$; Exponentes del polinomio: $3, 5, 24$
2. $Q(X) = 1 + 2X^{30.000}$
Coeficientes: $1, 2$; exponente del polinomio: 30.000
3. $R(X) = 2X^3 - e^{\sqrt{\pi}}X^7$
Coeficientes: $2, e^{\sqrt{\pi}}$; exponentes: $3, 7$

Antiejemplos. No son polinomios:

1. $1 + X^{\sqrt{5}}$, ya que el exponente de X es irracional.
2. $1 + X^{\pi}$, ya que el exponente de X es irracional.
3. $1 + 5X^{-3}$, pues el exponente de X es negativo.
4. $1 + X + X^2 + \cdots + X^n + \cdots$, debido a que la suma no es finita.
5. $1 + 5X^{\frac{1}{2}}$, pues el exponente es un racional no entero positivo.
6. $\frac{X^2+1}{1+X+7X^2}$, ya que es un cuociente.

Observación. Las X son mayúsculas.

Observación. Nunca jamás podremos escribir X^{-1} , cuando se trate de polinomios.

Definición 8.1.1 Diremos que la expresión

$$P(X) = a_0 + a_1X + \cdots + a_nX^n, \quad n \in \mathbb{N}, a_0, a_1, \dots, a_n \in K$$

donde K es un cuerpo, es un **polinomio sobre K** . El símbolo X se llama **indeterminada**, es decir, algo que no está determinado.

Si $K = \mathbb{R}$, diremos que es un **polinomio real**. Si $K = \mathbb{C}$, diremos que es un **polinomio complejo**. Si $K = \mathbb{Q}$, diremos que es un **polinomio racional**.

Ejemplos

1. $P(X) = X^7 + \pi X^9$, es un polinomio real.
2. $P(X) = X^5 + \sqrt{e^{\pi}} X^{30}$, es un polinomio real.
3. $P(X) = X^3 + iX^4$, es un polinomio complejo.
4. $P(X) = X + (7 + 7i)X^5$, es un polinomio complejo.
5. $P(X) = \frac{2}{3} - \frac{1}{5}X^4 + \frac{7}{12}X^{14}$, es un polinomio racional.
6. $P(X) = e + 5\pi X^7$, es un polinomio real que no es racional.

Definición 8.1.2 (*Igualdad de polinomios*) Sea $P(X) = a_0 + a_1X + \cdots + a_nX^n$ y $Q(X) = b_0 + b_1X + \cdots + b_mX^m$. Diremos que el polinomio $P(X)$ es igual al polinomio $Q(X)$ y lo denotaremos $P(X) = Q(X)$ si se cumplen simultáneamente:

1. $n = m$
2. $a_0 = b_0; a_1 = b_1; \cdots; a_n = b_n$

Ejercicio. Si $P(X) = a + bX + 5X^3 + 4X^7$ y $Q(X) = 2 + 5X^3 + cX^7$ y $P(X) = Q(X)$. Busquemos $P(X)$ y $Q(X)$.

Solución. Tenemos el siguiente sistema de ecuaciones:

$$\begin{array}{rcl} a & = & 2 \\ b & = & 0 \\ 4 & = & c \end{array}$$

Luego $P(X) = Q(X) = 2 + 5X^3 + 4X^7$

Definición 8.1.3 El conjunto formado por todos los polinomios con coeficientes en un cuerpo K , será denotado por $K[X]$, es decir:

$$K[X] = \{a_0 + a_1X + \cdots + a_nX^n; a_0, a_1, \cdots, a_n \in K\}$$

Notaciones. $\mathbb{R}[X] = \{\text{polinomios reales}\}; \mathbb{C}[X] = \{\text{polinomios complejos}\};$
 $\mathbb{Q}[X] = \{\text{polinomios racionales}\}$

Observación. Diremos que:

1. $P(X) = 1 + X - X^3$ tiene grado 3 y escribiremos $gr(P(X)) = 3$.
2. $Q(X) = 17 - X + 3X^2$ tiene grado 2 y escribiremos $gr(Q(X)) = 2$.
3. $R(X) = 15 + 4X$ tiene grado 1 y escribiremos $gr(R(X)) = 1$.
4. $S(X) = 14$ tiene grado 0 y escribiremos $gr(S(X)) = 0$.

Definición 8.1.4 El grado de un polinomio es el máximo exponente con coeficiente diferente de cero.

¿Qué pasa entonces con el polinomio $P(X) = 0$?

Respuesta: Hay dos posibilidades:

1. no asignarle grado.
2. asignarle el grado $-\infty$.

En este curso optaremos por la primera posibilidad.

Definición 8.1.5 Sea $P(X) = a_0 + a_1X + \cdots + a_nX^n$, entonces a_0 es llamado el término constante y a_n es llamado el **coeficiente supremo**.

Ejemplo. $P(X) = 5 - \sqrt{7}X^3 + \sqrt{e}X^8$, tiene término constante 5 y coeficiente supremo \sqrt{e} .

Definición 8.1.6 Diremos que el polinomio $P(X) = k$, $k \in K$, es un **polinomio constante**.

Ejemplo. Los números reales serán pensados como polinomios constantes.

Definición 8.1.7 Diremos que un polinomio es **mónico** si su coeficiente supremo es 1.

Ejemplo. $P(X) = 2 - 5X + 7X^6 + X^9$ y $Q(X) = 3 + X^4$ son polinomios mónicos.

Observación. Sean

$$P(X) = X^2 - 5X^3 + 2X^5$$

$$Q(X) = 2 - X^2 + 7X^8$$

Se define un nuevo polinomio a partir de estos dos polinomios, llamado el polinomio suma de $P(X)$ y $Q(X)$, denotado $P(X) + Q(X)$ y definido por:

$$P(X) + Q(X) = 2 + (1 - 1)X^2 - 5X^3 + 2X^5 + 7X^8$$

Nótese que $gr(P(X) + Q(X)) = 8$, $gr(P(X)) = 5$ y $gr(Q(X)) = 8$

Observación. Sean

$$P(X) = 2 + X^2 - 3X^5$$

$$Q(X) = 3 + X^2 + 2X^4 + 3X^5$$

Entonces

$$P(X) + Q(X) = 5 + 2X^2 + 2X^4$$

Nótese que $gr(P(X) + Q(X)) = 4$, $gr(P(X)) = 5$ y $gr(Q(X)) = 5$.

Observación. El grado de la suma no es la suma de los grados. Además el grado de la suma de dos polinomios, a veces es menor que ambos grados.

Definición 8.1.8 Sean

$$P(X) = a_0 + a_1X + \cdots + a_nX^n$$

$$Q(X) = b_0 + b_1X + \cdots + b_mX^m$$

Si $n \leq m$, se define **la suma de los polinomios $P(X)$ y $Q(X)$** , denotada $P(X) + Q(X)$, como sigue:

$$P(X) + Q(X) = (a_0 + b_0) + \cdots + (a_n + b_n)X^n + b_{n+1}X^{n+1} + \cdots + b_mX^m$$

Con respecto al grado de la suma se tiene:

$$gr(P(X) + Q(X)) \leq \max\{gr(P(X)), gr(Q(X))\}$$

Observación. Veamos como se comporta la multiplicación de polinomios.

Sea $P(X) = a_0 + a_1X$ y $Q(X) = b_0 + b_1X + b_2X^2$. Entonces:

$$P(X) \cdot Q(X) = (a_0 + a_1X) \cdot (b_0 + b_1X + b_2X^2)$$

$$= a_0b_0 + (a_0b_1 + a_1b_0)X + (a_0b_2 + a_1b_1)X^2 + a_1b_2X^3$$

Observación. Busquemos la fórmula del producto. Sean

$$P(X) = a_0 + a_1X + \cdots + a_nX^n$$

$$Q(X) = b_0 + b_1X + \cdots + b_mX^m$$

Entonces:

$$\begin{aligned} P(X) \cdot Q(X) &= a_0b_0 + (a_0b_1 + a_1b_0)X + (a_0b_2 + a_1b_1 + a_2b_0)X^2 + \cdots + \\ &\quad + (a_0b_j + a_1b_{j-1} + \cdots + a_{j-1}b_1 + a_jb_0)X^j + \cdots + a_nb_mX^{n+m} \\ gr(P(X) \cdot Q(X)) &= gr(P(X)) + gr(Q(X)) \end{aligned}$$

Fórmula del producto

$$P(X) \cdot Q(X) = \sum_{i=0}^{n+m} \left(\sum_{j+k=i} a_jb_k \right) X^i$$

Por ejemplo, en la sumatoria de adentro se puede tener:

$$\sum_{j+k=3} a_jb_k = a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0$$

o bien

$$\sum_{j+k=4} a_jb_k = a_0b_4 + a_1b_3 + a_2b_2 + a_3b_1 + a_4b_0$$

Ejercicio. Determine $a, b, c, d \in \mathbb{R}$ tal que:

$$X^4 - 1 = (X^2 + aX + b)(X^2 + cX + d)$$

Solución.

$$X^4 - 1 = X^4 + (a + c)X^3 + (b + ac + d)X^2 + (ad + bc)X + bd$$

Por definición de igualdad de polinomios, igualamos los coeficientes y tenemos el siguiente sistema de ecuaciones:

$$\left. \begin{array}{lll} cte : & (1) & bd = -1 \\ X : & (2) & ad + bc = 0 \\ X^2 : & (3) & b + ac + d = 0 \\ X^3 : & (4) & a + c = 0 \end{array} \right|$$

De (4) $c = -a$, (4) en (2): $ad - ab = 0$, entonces $a(d - b) = 0$

Se tiene dos posibilidades:

Caso (i): $a = 0$, entonces $c = 0$.

Reemplazando en (3) y en (1), se tiene:

$$\begin{array}{rcl} (3) & b + d & = 0 \\ (1) & bd & = -1 \end{array}$$

De (3) $d = -b$. (3) en (1): $b(-b) = -1$, luego $b^2 = 1$, de donde $b = 1$ o $b = -1$.

Si $b = 1$, entonces $d = -1$ y si $b = -1$, entonces $d = 1$.

Luego en el caso (i) se tiene :

$$X^4 - 1 = (X^2 + 1)(X^2 - 1) \text{ o bien } X^4 - 1 = (X^2 - 1)(X^2 + 1)$$

Caso (ii): $a \neq 0$, entonces $b - d = 0$, de donde $b = d$, reemplazando en (1), se tiene $b^2 = -1$, lo cual es una contradicción. Luego se tiene solamente el caso (i)

8.2 Función polinómica

Observación. Sea $P(X) = X^2 - 4 \in \mathbb{R}[X]$. $P(X)$ es un polinomio real. A este polinomio le asociaremos la función real, $\bar{p} : \mathbb{R} \rightarrow \mathbb{R}$, definida por $\bar{p}(\alpha) = \alpha^2 - 4$, $\forall \alpha \in \mathbb{R}$. Diremos que \bar{p} es la función polinómica asociada al polinomio $P(X)$.

Se tiene por ejemplo: $\bar{p}(1) = 1^2 - 4 = -3$; $\bar{p}(0) = -4$, $\bar{p}(5) = 21$. Diremos que $P(X)$ evaluado en 1, vale -3

Definición 8.2.1 Sea

$$P(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in K[X]$$

A $P(X)$ le asociamos la función

$$\bar{p} : K \rightarrow K$$

definida por:

$$\bar{p}(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

Diremos que \bar{p} es la **función polinómica asociada al polinomio** $P(X)$. Se dice que el valor del polinomio en α , es el número:

$$\bar{p}(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n$$

8.2.1 Raíces de un polinomio

Observaciones

1. Sea $P(X) = X^2 - 4 \in \mathbb{R}[X]$. Se tiene que $2^2 - 4 = 0$. Por este motivo diremos que 2 es una raíz de $P(X)$: Idem para -2 . Tenemos que $\bar{p}(2) = 0$ y $\bar{p}(-2) = 0$
2. Sea $P(X) = X^2 - 2 \in \mathbb{R}[X]$. Tenemos que $\bar{p}(\sqrt{2}) = 0$ y $\bar{p}(-\sqrt{2}) = 0$. Diremos que $\sqrt{2}$ y $-\sqrt{2}$ son raíces de $P(X)$. $P(X)$ no tiene raíces racionales. Es decir, no existe $\alpha \in \mathbb{Q}$, tal que $\bar{p}(\alpha) = 0$
3. Sea $P(X) = X + \pi \in \mathbb{R}[X]$. $P(X)$ tiene una raíz real, a saber, $-\pi$, es decir, $\bar{p}(-\pi) = 0$

Definición 8.2.2 Sea $P(X) \in K[X]$, K un cuerpo. Sea $P(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$. Diremos que $\alpha \in K$ es una **raíz** de $P(X)$ en $K[X]$ si $\bar{p}(\alpha) = 0$

Ejemplo. El polinomio $P(X) = X^2 + X + 1$, tiene por raíces a $\omega = \frac{-1}{2} + \frac{\sqrt{3}}{2}i$ y $\bar{\omega} = \frac{-1}{2} - \frac{\sqrt{3}}{2}i$, pues $\bar{p}(\omega) = 0$ y $\bar{p}(\bar{\omega}) = 0$

Definición 8.2.3 Si $P(X) = (X - \alpha)^n \cdot Q(X)$, entonces diremos que α es una **raíz de multiplicidad n** , si α no es una raíz de $Q(X)$.

Notas

1. Los polinomios constantes no nulos no tienen raíces.
2. El polinomio $P(X) = a_0 + a_1X$, con $a_1 \neq 0$, tiene sólo una raíz, a saber $\alpha = \frac{-a_0}{a_1}$.

3. Si α es una raíz del polinomio $P(X)$, entonces α es raíz del polinomio $H(X) = P(X) \cdot Q(X)$, $\forall Q(X) \in K[X]$.

Observación. Representación geométrica de $P(X) = X^2 - 4$ y su función polinómica asociada.

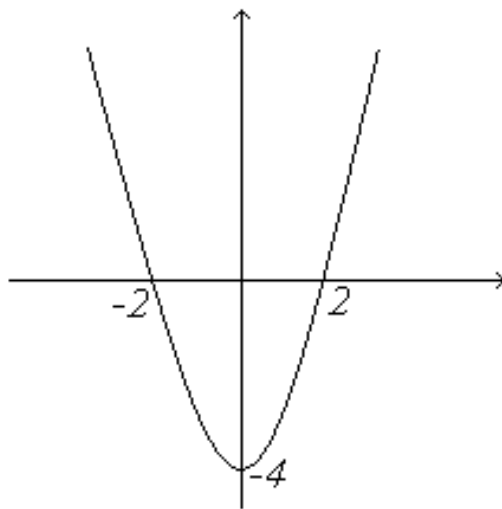
En efecto, sea $\bar{p} : \mathbb{R} \longrightarrow \mathbb{R}$; $\bar{p}(x) = x^2 - 4$, la función polinómica asociada a $P(X)$.

Tenemos $\bar{p}(0) = -4$, $\bar{p}(2) = 0$, $\bar{p}(-2) = 0$.

Cuando x crece, $\bar{p}(x)$ tiene un valor cada vez mayor y cuando x decrece, $\bar{p}(x)$ tiene un valor cada vez mayor, es decir,

$$\lim_{x \rightarrow +\infty} \bar{p}(x) = \infty \quad y \quad \lim_{x \rightarrow -\infty} \bar{p}(x) = \infty$$

Geométricamente, como se ve en la figura siguiente, es una parábola vertical cóncava, con vértice en $(0, -4)$. Intersecta al eje X , en $x = 2$ y en $x = -2$. Luego es un polinomio con raíces reales 2 y -2 .

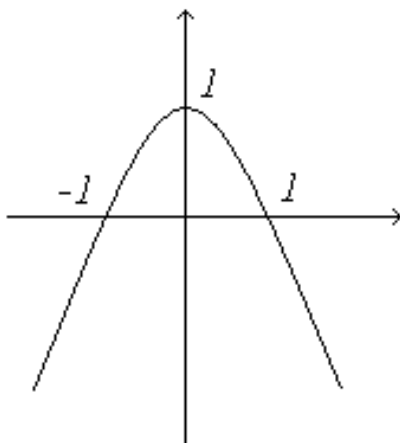


Observación. Estudiemos el polinomio $P(X) = -X^2 + 1$ y su función polinómica asociada.

En efecto, las raíces del polinomio son 1 y -1 .

$$\lim_{x \rightarrow +\infty} -x^2 + 1 = -\infty \quad y \quad \lim_{x \rightarrow -\infty} -x^2 + 1 = -\infty$$

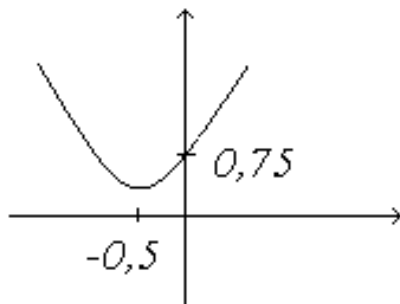
Geométricamente es una parábola vertical convexa con vértice en $(0, 1)$ que intersecta al eje X en 1 y en -1 . Se tiene $\bar{p}(1) = 0$, $\bar{p}(-1) = 0$, $\bar{p}(0) = 1$. Su gráfico es:



Observación. Estudiemos el polinomio $P(X) = X^2 + X + 1$ y su función polinómica asociada.

Solución. Encontrar las raíces reales del polinomio $P(X) = X^2 + X + 1$ es equivalente a resolver la ecuación: $x^2 + x + 1 = 0$ (x es una incógnita) y su solución es $x = \frac{-1 \pm \sqrt{1-4}}{2}$, de donde, $x = \frac{-1 \pm \sqrt{-3}}{2} \notin \mathbb{R}$, es decir, no hay un número real que cumpla la ecuación, es decir, el polinomio $P(X) = X^2 + X + 1$ no tiene raíces reales. Geométricamente esto quiere decir que el gráfico no toca el eje X , luego todo el gráfico está sobre el eje X o todo el gráfico está bajo el eje X . Basta ver solamente un valor, por ejemplo, $\bar{p}(0) = 1 > 0$, luego siempre es positivo, es decir, todo el gráfico está sobre el eje X .

Es una parábola cóncava vertical con vértice en $(-\frac{1}{2}, \frac{3}{4})$, como vemos en la figura siguiente:

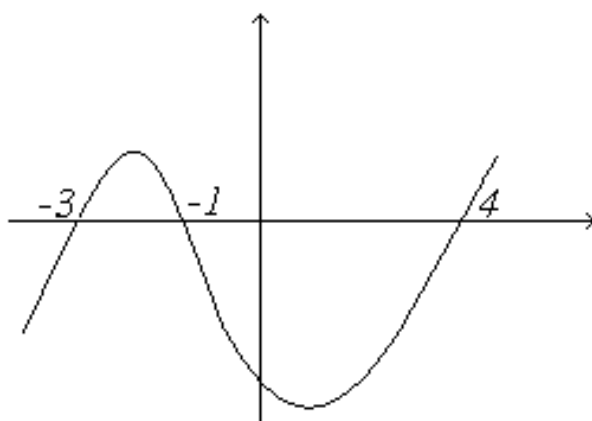


Observación. Estudiemos el polinomio $P(X) = (X+3)(X+1)(X-4)$ y su función polinómica asociada.

Solución. Tenemos que

$$\lim_{x \rightarrow +\infty} \bar{p}(x) = +\infty \quad y \quad \lim_{x \rightarrow -\infty} \bar{p}(x) = -\infty$$

Luego al menos una vez interseca el eje X , es decir, tiene al menos una raíz real. En efecto tiene tres raíces reales, a saber: $-3, -1, 4$. La curva interseca el eje X en los puntos: $(-3, 0), (-1, 0), (4, 0)$. Su gráfico es:

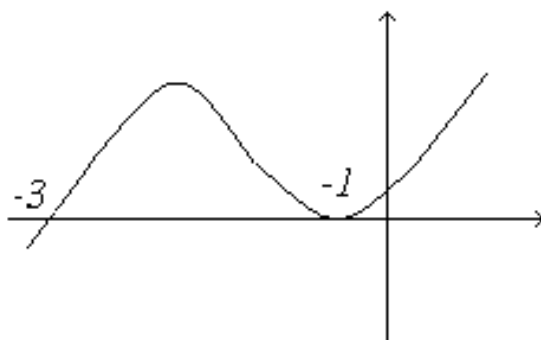


Observación. Estudiemos el polinomio $P(X) = (X+3)(X+1)^2$ y su función polinómica asociada.

Solución.

$$\lim_{x \rightarrow +\infty} \bar{p}(x) = +\infty \quad y \quad \lim_{x \rightarrow -\infty} \bar{p}(x) = -\infty$$

Las raíces reales son sólo dos: -3 que es una raíz simple y -1 que tiene multiplicidad 2. La raíz de multiplicidad 2 corresponde a un punto de tangencia de la curva con el eje X . Su gráfico es:



Observación. ¿Puede haber un polinomio real de grado 3 que no tenga raíz real alguna?

Solución. Sea $P(X) = aX^3 + bX^2 + cX + d$

Caso (i): $a > 0$, entonces

$$\lim_{x \rightarrow +\infty} \bar{p}(x) = +\infty \quad y \quad \lim_{x \rightarrow -\infty} \bar{p}(x) = -\infty$$

Y puesto que es una función continua, la curva no puede dar saltos, luego obligatoriamente atraviesa el eje X . Algebraicamente esto significa que tiene al menos una raíz real.

Caso (ii): $a < 0$. Análogo al caso anterior.

8.3 Divisibilidad en el conjunto de polinomios

Repaso: Divisibilidad en \mathbb{Z}

Tenemos que $6 = 2 \cdot 3$. Decimos: 6 es divisible por 3, 6 es divisible por 2, 2 divide a 6, o bien, 3 divide a 6. Se escribe: $2|6$; $3|6$ (es una línea vertical). Además 5 no divide a 6. Se escribe: $5 \nmid 6$

Se tiene que 2 y 3 son divisores propios de 6, en cambio 1 y 6 son divisores triviales de 6.

5 no tiene divisores propios. Se dice que 5 es primo.

Los primeros números primos son: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \dots .
Los divisores propios de 555 son: 3, 5, 37.

Filosofía de las matemáticas

Puesto que en $K[X]$, la mayoría de los elementos no tienen inverso multiplicativo, se tiene una situación análoga a \mathbb{Z} . Entonces se desea llevar los conceptos definidos en \mathbb{Z} a $K[X]$. No podrá ser idéntico pues en \mathbb{Z} se tiene la propiedad de orden total, sin embargo $K[X]$ no tiene orden: Serán conceptos inspirados en \mathbb{Z}

Observaciones

1. $P(X) = X^2 - 1$ es divisible por $X - 1$ y por $X + 1$, pues

$$X^2 - 1 = (X - 1)(X + 1)$$

2. En $\mathbb{R}[X]$, el polinomio $P(X) = X^2 + 1$ no es divisible por ningún polinomio $Q(X)$. Es decir no existe $Q(X) \in \mathbb{R}[X]$, tal que

$$X^2 + 1 = Q(X) \cdot T(X)$$

con $\text{gr}(Q(X)) = 1$, algún $T(X) \in \mathbb{R}[X]$.

3. El polinomio $X^4 - 1$ es divisible por el polinomio $X^3 + X^2 + X + 1$ en $\mathbb{R}[X]$, pues

$$X^4 - 1 = (X - 1)(X^3 + X^2 + X + 1)$$

Definición 8.3.1 Sean $P(X)$ y $Q(X)$ dos polinomios en $K[X]$. El polinomio $P(X)$ se dice **divisible por $Q(X)$ en $K[X]$** , si existe un polinomio $R(X)$ en $K[X]$ tal que $P(X) = Q(X) \cdot R(X)$. También diremos que el polinomio $Q(X)$ **divide al polinomio $P(X)$** y que el polinomio $R(X)$ **divide al polinomio $P(X)$** .

Notación. $Q(X) | P(X)$ y $R(X) | P(X)$.

Definición 8.3.2 Si $P(X) \neq Q(X) \cdot S(X)$, $\forall S(X) \in K[X]$, $\text{gr}(S(X)) > 1$, entonces diremos que $Q(X)$ **no divide a $P(X)$** y lo denotaremos $Q(X) \nmid P(X)$.

Ejercicios Resueltos

1. Busquemos los divisores de $P(X) = X^3 - 1$ en $\mathbb{R}[X]$.

Solución.

$$X^3 - 1 = (X - 1)(X^2 + X + 1)$$

$$X^3 - 1 = (2X - 2)\left(\frac{1}{2}X^2 + \frac{1}{2}X + \frac{1}{2}\right)$$

$$X^3 - 1 = \left(\frac{1}{3}X - \frac{1}{3}\right)(3X^2 + 3X + 3)$$

Luego algunos divisores de $P(X) = X^3 - 1$ en $\mathbb{R}[X]$ tienen la forma

$$R_\lambda(X) = \lambda X - \lambda \quad \text{y} \quad Q_\mu(X) = \mu X^2 + \mu X + \mu \cdot 1$$

Se tiene que $P(X) = R_\lambda(X) \cdot Q_\mu(X)$, con $\lambda \cdot \mu = 1$. Queda pendiente la pregunta si habrá otros divisores.

2. Busquemos divisores del polinomio $P(X) = X^3 + 1$.

Solución.

$$P(X) = X^3 + 1 = (X + 1)(X^2 - X + 1)$$

Algunos divisores de $P(X)$ en $\mathbb{R}[X]$ tienen la forma:

$$R_\lambda(X) = \lambda X + \lambda \quad \text{y} \quad Q_\mu(X) = \mu X^2 - \mu X + \mu$$

Se tiene que:

$$P(X) = R_\lambda(X) \cdot Q_\mu(X), \text{ con } \lambda \cdot \mu = 1$$

Queda pendiente si habrá otros divisores.

Definición 8.3.3 Factorizar un polinomio *es transformarlo en un producto de polinomios.*

Nota. Buscar divisores de un polinomio es entonces equivalente a buscar diferentes factorizaciones del polinomio dado.

Ejercicio. Busquemos divisores del polinomio $P(X) = X^{12} - 1$.

Solución.

$$\begin{aligned} P(X) &= X^{12} - 1 \\ &= (X^6 + 1)(X^6 - 1) \\ &= ((X^2)^3 + 1)((X^3)^2 - 1) \\ &= (X^2 + 1)(X^4 - X^2 + 1)(X^3 - 1)(X^3 + 1) \\ &= (X^2 + 1)(X^4 - X^2 + 1)(X - 1)(X^2 + X + 1)(X + 1)(X^2 - X + 1) \end{aligned}$$

Cada factor es un divisor de $P(X)$. Todavía se pueden encontrar más divisores, pero este problema lo resolveremos más adelante.

Tarea. Encuentre los posibles valores para a de manera que :

1. $X^3 + aX^2 - 10X + a^2$ sea divisible por $X - 2$
2. $2X^4 - 3X^3 + aX^2 - 9X + 1$ sea divisible por $X - 3$

Definición 8.3.4 Sea $P(X) \in K[X]$, entonces los polinomios constantes y aquellos de la forma $\lambda P(X)$, con $\lambda \in K$, serán llamados **divisores triviales de $P(X)$** y aquellos que no son triviales serán llamados **divisores propios de $P(X)$** . Los divisores triviales también son llamados **divisores impropios**.

Demos otro paseo por el mundo de la aritmética.

Teorema 8.3.1 (Teorema fundamental de la aritmética) Si n es un número natural, entonces

$$n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$$

con p_1, p_2, \dots, p_k primos distintos de dos en dos, se escribe de manera única.

Nota. En el conjunto de los polinomios, se definen conceptos inspirados en estos conceptos aritméticos.

Definición 8.3.5 Un polinomio $P(X) \in K[X]$ de grado mayor o igual a 1, se llamará **polinomio irreducible o primo sobre K** , si todos sus divisores son triviales en $K[X]$. En caso contrario será llamado **reducible en $K[X]$** , es decir, $P(X)$ es reducible sobre $K[X]$ si $\exists P_1(X), P_2(X) \in K[X]$ tal que

$$P(X) = P_1(X) \cdot P_2(X)$$

con $0 < \text{gr}(P_1(X)), \text{gr}(P_2(X)) < \text{gr}(P(X))$

Ejercicio (tarea). Estudie la reductibilidad sobre \mathbb{Q} , \mathbb{R} , \mathbb{Z}_2 y sobre \mathbb{Z}_3 de los siguientes polinomios:

(i) $P(X) = X^2 - 2$, (ii) $P(X) = X^2 + 1$, (iii) $P(X) = X^3 + 6$

Nota. El Teorema siguiente es análogo al Teorema Fundamental de la Aritmética, en $K[X]$

8.3.1 Teorema de la descomposición única

En $K[X]$, todo polinomio de grado mayor o igual a 1, admite una descomposición o factorización única, salvo el orden de los factores, en un producto de polinomios mónicos irreducibles en $K[X]$ y un factor constante de K .

Demostración. Se hace por inducción sobre el grado del polinomio.

8.4 División Euclidiana

Repaso de aritmética

Dividir significa multiplicar por el inverso multiplicativo. Puesto que los números enteros no tienen inverso multiplicativo, salvo el 1 y -1 , no se puede hablar de división, se hablará de división euclidiana.

Si 7 lo dividimos por 2, se obtiene 3 en el cociente y resto 1. El resto es estrictamente menor que el divisor.

Recuerde que en \mathbb{Z} hay orden total.

Filosofía de las matemáticas

En $K[X]$, se tiene que sólo los polinomios constantes diferentes de cero, tienen inverso multiplicativo. Esto nos dice que en $K[X]$ no se puede hablar de división. ¿Será posible construir algo parecido a la división? ¿Una división como la división euclidiana definida sobre el conjunto de los enteros?

Un polinomio P lo dividimos por un polinomio D , obteniendo Q en el cociente y R en el resto, es decir $P = D \cdot Q + R$. Pero en este caso " $R < D$ " no tiene sentido.

Nuevamente nos encontramos con un problema, pues en $K[X]$ no hay orden. Entonces vamos a comparar los grados de los polinomios.

La respuesta a todas estas interrogantes se tienen en el Teorema siguiente:

8.4.1 Teorema de la División Euclidiana o Algoritmo de la División

Sean $P(X)$ y $D(X)$ dos polinomios en $K[X]$, con $D(X) \neq 0$, entonces existen dos únicos polinomios $Q(X)$ y $R(X)$ tales que:

$$P(X) = D(X) \cdot Q(X) + R(X), \text{ con } \text{gr}(R(X)) < \text{gr}(D(X)) \text{ o } R(X) = 0$$

Demostración. Se hace por inducción sobre el grado de $P(X)$.

Definición 8.4.1 $Q(X)$ es llamado el **cuociente** de la división de $P(X)$ por $D(X)$, $R(X)$ es llamado el **resto**, $P(X)$ es llamado el **dividendo** y $D(X)$ es llamado el **divisor**

Nota. Sea $P(X) = X^2 - 3X + 1$, $D(X) = X - 2$, entonces

$$X^2 - 3X + 1 = (X - 2)(X - 1) + (-1)$$

Esta división se hace de la siguiente manera:

$$\begin{array}{r} X^2 - 3X + 1 : X - 2 = X - 1 \\ \underline{\mp X^2 \pm 2X} \\ -X + 1 \\ \underline{\pm X \mp 2} \\ -1 \end{array}$$

Observación Sea $\bar{p} : \mathbb{R} \rightarrow \mathbb{R}$ la función polinómica asociada. Se tiene que $\bar{p}(2) = -1$, número que coincide con el resto de la división euclidiana de $P(X)$ por $D(X)$, pues $\bar{p}(2) = (2-2)(2-1) + (-1) = -1$. Se tiene el teorema siguiente:

Teorema 8.4.1 (Teorema del Resto) *El resto de la división euclidiana de un polinomio $P(X)$ por $D(X) = X - \alpha$ es el número $\bar{p}(\alpha)$*

Demostración. Por el algoritmo de la división se tiene

$$P(X) = D(X) \cdot Q(X) + R(X), \text{ con } \text{gr}(R(X)) < \text{gr}(D(X)) = 1$$

Luego $gr(R(X)) = 0$ o $R(X) = 0$, es decir, $R(X) = k$, k una constante.

Luego $\bar{p}(x) = (x - \alpha) \cdot \bar{q}(x) + k$, entonces $\bar{p}(\alpha) = (\alpha - \alpha) \cdot \bar{q}(\alpha) + k$, luego $\bar{p}(\alpha) = k$

Introducción al Teorema del Factor

Nota. El polinomio $P(X) = X^2 + 1$ no es divisible por $X - 2$ pues $\bar{p}(2) = 2^2 + 1 = 5 \neq 0$.

El polinomio $P(X) = X^2 - X - 2$ es divisible por $X + 1$, pues $P(X) = (X + 1)(X - 2)$.

Nota. El polinomio $P(X) = X^2 - 4 = (X - 2)(X + 2)$ y $\bar{p}(2) = \bar{p}(-2) = 0$. Es decir, $P(X)$ es divisible por $X - 2$ y también por $X + 2$.

Tenemos el Teorema siguiente:

Teorema 8.4.2 (Teorema del Factor) *Un elemento $\alpha \in K$ es una raíz o cero del polinomio $P(X) \in K[X]$ si y sólo si $X - \alpha$ es un factor de $P(X)$ en $K[X]$.*

Demostración. Sea $\alpha \in K$ una raíz de $P(X)$, entonces $\bar{p}(\alpha) = 0$. Por el Algoritmo de la División existe $Q(X) \in K[X]$ tal que

$$P(X) = (X - \alpha) \cdot Q(X) + \bar{p}(\alpha)$$

luego $P(X) = (X - \alpha) \cdot Q(X)$, es decir $X - \alpha$ es un factor de $P(X)$.

Por otra parte, si $X - \alpha$ es un factor de $P(X)$, entonces existe $Q(X) \in K[X]$ tal que

$$P(X) = (X - \alpha) \cdot Q(X)$$

Luego $\bar{p}(\alpha) = (\alpha - \alpha) \cdot \bar{q}(\alpha) = 0$. Luego α es una raíz del polinomio $P(X)$.

Teorema 8.4.3 (Teorema sobre el número máximo de raíces) *Un polinomio $P(X) \in K[X]$, $P(X) \neq 0$, con $gr(P(X)) = n$, posee a lo más n raíces en K*

Demostración. Por inducción sobre el grado de $P(X)$

1. Sea $gr(P(X)) = 1$, entonces

$$P(X) = a_0 + a_1X, \quad a_1 \neq 0$$

luego $\alpha_0 = -\frac{a_0}{a_1}$ es la única raíz de $P(X)$

2. Hipótesis de inducción: Supongamos que todo polinomio de grado $n - 1$ tiene a lo más $n - 1$ raíces.
3. Por demostrar para $gr(P(X)) = n$

Si $P(X)$ no tiene raíces, el teorema se cumple.

Si $P(X)$ tiene a lo menos una raíz: sea α una tal raíz. Por el teorema del factor se tiene:

$$P(X) = (X - \alpha) \cdot Q(X), \text{ con } gr(Q(X)) = n - 1$$

Por hipótesis de inducción $Q(X)$ tiene a lo más $n - 1$ raíces. Luego $P(X)$ tiene a lo más n raíces.

8.5 Descomposición en $\mathbb{C}[X]$

Definición 8.5.1 *Un cuerpo K se dirá algebraicamente cerrado si todo polinomio $P(X) = a_0 + a_1X + \cdots + a_nX^n$, con $n \geq 1$, tiene sus n raíces en K*

Nota. \mathbb{Q} , \mathbb{R} no son algebraicamente cerrados.

Contraejemplo: El polinomio $P(X) = X^2 + 2$ no tiene raíces ni en \mathbb{Q} ni en \mathbb{R} .

Pregunta. ¿Habrá un cuerpo algebraicamente cerrado? La respuesta la tenemos en el siguiente Teorema:

Teorema 8.5.1 (Teorema Fundamental del Algebra) *Todo polinomio en $\mathbb{C}[X]$ tiene todas sus raíces en \mathbb{C} .*

Otra forma de enunciar el teorema es la siguiente:

\mathbb{C} es algebraicamente cerrado.

O bien:

Para todo $P(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{C}[X]$, se tiene

$$P(X) = a_n(X - z_1)(X - z_2) \cdots (X - z_n); \text{ con } z_i \in \mathbb{C}$$

no necesariamente distintas todas sus raíces.

O bien:

Un polinomio complejo de grado n , tiene n raíces complejas, no necesariamente distintas.

La demostración de este teorema no la veremos en este curso.

Ejemplo. Descompongamos $P(X) = X^3 - 1$ en $\mathbb{C}[X]$

En efecto, sus raíces son: $\omega_0 = 1$, $\omega_1 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ y $\omega_2 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$.

Luego $P(X) = (X - 1)(X - \omega_1)(X - \omega_2)$

Es decir, $P(X) = (X - 1)(X - (-\frac{1}{2} + \frac{\sqrt{3}}{2}i))(X - (-\frac{1}{2} - \frac{\sqrt{3}}{2}i))$

Ejemplo. En $\mathbb{C}[X]$, descompongamos el polinomio $P(X) = X^6 - 1$

Sabemos que las raíces sextas de la unidad son:

$$\omega_0 = 1, \quad \omega_1 = \frac{1}{2} + \frac{\sqrt{3}}{2}i, \quad \omega_2 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$$

$$\omega_3 = -1, \quad \omega_4 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i, \quad \omega_5 = \frac{1}{2} - \frac{\sqrt{3}}{2}i$$

Luego $P(X) = (X - 1)(X - \omega_1)(X - \omega_2)(X + 1)(X - \omega_4)(X - \omega_5)$

8.6 Descomposición en $\mathbb{R}[X]$

Observación. En el ejercicio anterior observamos que $\overline{\omega_1} = \omega_5$ y $\overline{\omega_2} = \omega_4$.

Esto nos ayuda a descomponer $P(X)$ en polinomios irreducibles en $\mathbb{R}[X]$.

$$Q_1(X) = (X - \omega_1)(X - \overline{\omega_1}) = X^2 - (\omega_1 + \overline{\omega_1})X + \omega_1 \cdot \overline{\omega_1} \in \mathbb{R}[X]$$

$$Q_2(X) = (X - \omega_2)(X - \overline{\omega_2}) = X^2 - (\omega_2 + \overline{\omega_2})X + \omega_2 \cdot \overline{\omega_2} \in \mathbb{R}[X]$$

Tenemos que

$$\omega_1 + \overline{\omega_1} = 1; \quad \omega_1 \cdot \overline{\omega_1} = 1; \quad \omega_2 + \overline{\omega_2} = -1; \quad \omega_2 \cdot \overline{\omega_2} = 1$$

Luego $Q_1(X) = X^2 - X + 1$ y $Q_2(X) = X^2 + X + 1$. Ambos polinomios son reales.

Luego

$$X^6 - 1 = (X - 1)(X + 1)(X^2 - X + 1)(X^2 + X + 1)$$

Los cuatro polinomios son irreducibles en $\mathbb{R}[X]$

Observación. Si $z \in \mathbb{C}$, se tiene que

$$(X - z)(X - \overline{z}) = X^2 - (z + \overline{z})X + z \cdot \overline{z}$$

el cual es un polinomio real.

Entonces uno se hace la pregunta siguiente: ¿En qué caso se tiene la raíz compleja con su raíz conjugada? La respuesta la tenemos en la siguiente proposición

Proposición 8.6.1 Sea $P(X) \in \mathbb{R}[X]$. Si z es una raíz compleja no real, entonces \overline{z} también es una raíz de $P(X)$

Demostración. Sea $P(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{R}[X]$. Sea z una raíz compleja no real de $P(X)$, entonces:

$$\begin{aligned} 0 = \overline{P(z)} &= \overline{a_0 + a_1z + a_2z^2 + \cdots + a_nz^n} \\ &= \overline{a_0} + \overline{a_1z} + \overline{a_2z^2} + \cdots + \overline{a_nz^n} \\ &= a_0 + a_1\overline{z} + a_2\overline{z}^2 + \cdots + a_n\overline{z}^n \\ &= a_0 + a_1\overline{z} + a_2(\overline{z})^2 + \cdots + a_n(\overline{z})^n \\ &= \overline{P(\overline{z})} \end{aligned}$$

Luego $\bar{p}(\bar{z}) = 0$.

Se tiene entonces el siguiente Teorema:

Teorema 8.6.2 (Teorema de Descomposición en $\mathbb{R}[X]$.) *Sea $P(X) \in \mathbb{R}[X]$. $P(X)$ admite una descomposición única (salvo el orden de sus factores) en un producto de polinomios reales mónicos irreducibles de grado 1 o 2 y un factor constante.*

Demostración. Basta observar que al efectuar el producto de factores del tipo $(X - z)(X - \bar{z})$, se obtiene un polinomio real irreducible en $\mathbb{R}[X]$ de grado 2.

Ejemplos

$$P(X) = 2X^2 - 50 = 2 \cdot (X - 5) \cdot (X + 5)$$

$$Q(X) = 3X^3 - 27X^2 + 72X - 60 = 3 \cdot (X - 2)^2 \cdot (X - 5)$$

8.7 Descomposición en $\mathbb{Q}[X]$

Observación. Consideremos el polinomio

$$Q(X) = 8X^3 - 32X^2 + 8X + 3$$

Se tiene que $\frac{1}{2}$ es una raíz, pues:

$$\bar{q}(\frac{1}{2}) = 8(\frac{1}{2})^3 - 32(\frac{1}{2})^2 + 8(\frac{1}{2}) + 3 = 1 - 8 + 4 + 3 = 0.$$

Observamos que $\frac{p}{q} = \frac{1}{2}$ y $p = 1|3$ y $q = 2|8$. Es decir $p|a_0$ y $q|a_n$. El siguiente teorema nos entrega información sobre las posibles raíces racionales de un polinomio con coeficientes enteros.

Teorema 8.7.1 *Sea $P(X) = a_0 + a_1X + \cdots + a_nX^n$ un polinomio con coeficientes enteros, de grado $n \geq 1$. Si $\alpha = \frac{p}{q}$ es una raíz racional de $P(X)$, (p y q relativamente primos), entonces $p|a_0$ y $q|a_n$*

Demostración. Sea

$$P(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$$

Supongamos que $\alpha = \frac{p}{q}$ es una raíz de $P(X)$, entonces

$$\bar{p}\left(\frac{p}{q}\right) = a_0 + a_1\left(\frac{p}{q}\right) + \cdots + a_n\left(\frac{p}{q}\right)^n = 0$$

Luego multiplicando por q^n , tenemos:

$$a_0q^n + a_1q^{n-1}p + \cdots + a_{n-1}qp^{n-1} + a_np^n = 0$$

De donde:

$$a_1q^{n-1}p + \cdots + a_{n-1}qp^{n-1} + a_np^n = -a_0q^n$$

Luego $p|a_0q^n$ y como $(p, q) = 1$, entonces $p|a_0$.

Además $q|(a_1q^{n-1}p + \cdots + a_{n-1}qp^{n-1} + a_np^n)$. Luego $q|a_np^n$. De donde se concluye que $q|a_n$.

Ejemplo. Veamos si el polinomio $P(X) = -10 + 3X + 18X^2$ tiene raíces racionales.

En efecto, sea $\alpha = \frac{p}{q}$ una raíz. Entonces: $p|10$ y $q|18$. Luego las posibilidades para p y q son: $p : 1, 2, 5, 10$ y $q : 1, 2, 3, 6, 9, 18$

$$\bar{p}\left(\frac{1}{1}\right) = \bar{p}(1) = 11 \neq 0$$

$$\bar{p}\left(\frac{1}{3}\right) = -10 + 3 \cdot \frac{1}{3} + 18 \cdot \frac{1}{9} = -10 + 1 + 2 \neq 0$$

$$\bar{p}\left(\frac{1}{6}\right) = -10 + 3 \cdot \frac{1}{6} + 18 \cdot \frac{1}{36} = \frac{-20+1+1}{2} \neq 0$$

$$\bar{p}\left(\frac{2}{3}\right) = -10 + 3 \cdot \frac{2}{3} + 18 \cdot \frac{4}{9} = -10 + 2 + 8 = 0. \text{ Luego } \frac{2}{3} \text{ es una raíz.}$$

$$\bar{p}\left(\frac{-5}{6}\right) = -10 + 3 \cdot \left(\frac{-5}{6}\right) + 18 \cdot \frac{25}{36} = \frac{-20-5+25}{2} = 0. \text{ Luego } -\frac{5}{6} \text{ es la otra raíz.}$$

$$\text{Luego } P(X) = 18\left(X - \frac{2}{3}\right)\left(X + \frac{5}{6}\right)$$

Ejercicios Resueltos

1. Encuentre los valores de a , de manera que

$$P(X) = X^3 + aX^2 - 10X + a^2$$

sea divisible por $X - 2$.

Solución. Que sea divisible por $X - 2$, significa que al dividir $P(X)$ por $X - 2$, se obtiene resto 0. Por el Teorema del Resto, tenemos que la función polinómica asociada evaluada en 2, debe tener valor 0, es decir, $8 + 4a - 20 + a^2 = 0$, tenemos $(a - 2)(a + 6) = 0$. Luego $a = 2$ o $a = -6$. Los polinomios buscados son:

$$P_1(X) = X^3 + 2X^2 - 10X + 4$$

$$P_2(X) = X^3 - 6X^2 - 10X + 36$$

2. Encuentre los valores de a , de manera que el polinomio

$$P(X) = 4X^3 + aX^2 - 2X + 5$$

al dividirlo por $X - 1$, se obtenga resto 5.

Solución. Por el Teorema del Resto, se tiene que la función polinómica asociada a $P(X)$, evaluada en 1, se obtiene el valor 5. Luego $4 + a - 2 + 5 = 5$, de donde $a = -2$.

3. En $\mathbb{R}[X]$, descomponga en sus factores irreducibles mónicos los polinomios:

$$P_1(X) = X^2 + 1; \quad P_2(X) = X^3 - 1; \quad P_3(X) = X^3 + 1$$

Solución. Se tiene que $P_1(X)$ es irreducible en $\mathbb{R}[X]$. Los otros polinomios se descomponen de la manera siguiente:

$$P_2(X) = (X - 1)(X^2 + X + 1); \quad P_3(X) = (X + 1)(X^2 - X + 1)$$

4. Descomponga en sus factores irreducibles en $\mathbb{R}[X]$, el polinomio $P(X) = X^{12} - 1$.

Solución. Buscamos $z \in \mathbb{C}$, tal que $z^{12} - 1 = 0$, es decir $z^{12} = 1$, luego buscamos las raíces décimo segundas de la unidad. Comencemos por escribir la unidad en su forma polar. Tenemos

$$1 = 1(\cos 0 + i \sin 0)$$

Ahora busquemos las raíces décimo segundas de la unidad:

$$w_0 = 1\left(\cos \frac{0}{12} + i \sin \frac{0}{12}\right) = 1$$

Para obtener la segunda raíz debemos sumar $\frac{2\pi}{12} = \frac{\pi}{6}$ al argumento de w_0 . Tenemos:

$$w_1 = \cos \frac{\pi}{6} + \sin \frac{\pi}{6} = \frac{\sqrt{3}}{2} + \frac{1}{2}i$$

Nuevamente debemos sumar $\frac{\pi}{6}$ al argumento de w_1 , para obtener el argumento de w_2 y así sucesivamente, tenemos:

$$\begin{aligned} w_2 &= \cos \frac{\pi}{3} + \sin \frac{\pi}{3} = \frac{1}{2} + \frac{\sqrt{3}}{2}i \\ w_3 &= \cos \frac{\pi}{2} + \sin \frac{\pi}{2} = i \\ w_4 &= \cos \frac{2\pi}{3} + \sin \frac{2\pi}{3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i \\ w_5 &= \cos \frac{5\pi}{6} + \sin \frac{5\pi}{6} = -\frac{\sqrt{3}}{2} + \frac{1}{2}i \\ w_6 &= \cos \pi + \sin \pi = -1 \\ w_7 &= \cos \frac{7\pi}{6} + \sin \frac{7\pi}{6} = -\frac{\sqrt{3}}{2} - \frac{1}{2}i \\ w_8 &= \cos \frac{4\pi}{3} + \sin \frac{4\pi}{3} = -\frac{1}{2} - \frac{\sqrt{3}}{2}i \\ w_9 &= \cos \frac{3\pi}{2} + \sin \frac{3\pi}{2} = -i \\ w_{10} &= \cos \frac{5\pi}{3} + \sin \frac{5\pi}{3} = \frac{1}{2} - \frac{\sqrt{3}}{2}i \\ w_{11} &= \cos \frac{11\pi}{6} + \sin \frac{11\pi}{6} = \frac{\sqrt{3}}{2} - \frac{1}{2}i \end{aligned}$$

Ahora que tenemos las raíces de $P(X)$, podemos descomponerlo en sus factores irreducibles en $\mathbb{C}[X]$. Se tiene:

$$P(X) = (X - w_0)(X - w_1) \cdots (X - w_{11})$$

Para obtener la descomposición en $\mathbb{R}[X]$, debemos encontrar la raíz conjugada de cada w_i . Tenemos que $\overline{w_1} = w_{11}$, $\overline{w_2} = w_{10}$, $\overline{w_3} = w_9$, $\overline{w_4} = w_8$ y $\overline{w_5} = w_7$. Podemos entonces construir los factores irreducibles en $\mathbb{R}[X]$, de la siguiente manera:

$$\begin{aligned} P_1(X) &= (X - w_1)(X - w_{11}) = X^2 - \sqrt{3}X + 1 \\ P_2(X) &= (X - w_2)(X - w_{10}) = X^2 - X + 1 \\ P_3(X) &= (X - w_3)(X - w_9) = X^2 + 1 \\ P_4(X) &= (X - w_4)(X - w_8) = X^2 + X + 1 \\ P_5(X) &= (X - w_5)(X - w_7) = X^2 + \sqrt{3}X + 1 \end{aligned}$$

Luego

$$X^{12} - 1 = (X - 1) \cdot (X + 1) \cdot P_1(X) \cdot P_2(X) \cdot P_3(X) \cdot P_4(X) \cdot P_5(X)$$

Es la descomposición de $P(X) = X^{12} - 1$ en sus factores irreducibles en $\mathbb{R}[X]$

5. Determine un polinomio real de grado 3 que admita las raíces 0 y 2 y tal que los restos que se obtienen al dividirlo por $X - 1$ y por $X - 3$ sean iguales. Calcule la tercera raíz.

Solución. $P(X)$ se descompone de la manera siguiente:

$$P(X) = X(X - 2)(X - a)$$

Los restos de la división por $X - 1$ y por $X - 3$ son iguales, luego al evaluar la función polinómica en 1 y en 3, estos valores deben coincidir. Luego $\bar{p}(1) = \bar{p}(3)$. De donde:

$$1(1 - 2)(1 - a) = 3(3 - 2)(3 - a)$$

Luego $a = \frac{5}{2}$ y el polinomio buscado es

$$P(X) = X^3 - \frac{9}{2}X^2 + 5X$$

6. En $\mathbb{R}[X]$, encuentre el polinomio de menor grado que tenga por raíces:
- (a) 3, -2
 - (b) $1 + 3i$, 2
 - (c) $-2i$, $2 + i$

Solución.

(a) $P(X) = (X - 3)(X + 2) = X^2 - X - 6$

- (b) Si un polinomio real, tiene una raíz compleja, entonces debe tener también su raíz conjugada. Luego el polinomio buscado es:

$$\begin{aligned} P(X) &= (X - (1 + 3i))(X - (1 - 3i))(X - 2) \\ &= X^3 - 2X^2 + 10X - 2X^2 + 4X - 20 \\ &= X^3 - 4X^2 + 14X - 20 \end{aligned}$$

(c) El polinomio buscado es:

$$\begin{aligned} P(X) &= (X - 2i)(X + 2i)(X - (2 + i))(X - (2 - i)) \\ &= (X^2 + 4)(X^2 - 4X + 5) \\ &= X^4 - 4X^3 + 9X^2 - 16X + 20 \end{aligned}$$

7. Encuentre el polinomio real mónico que tiene por raíces: -1 , $1 - 2i$ y que deja resto 45 al ser dividido por $X - 2$

Solución. El polinomio $P(X)$ tiene la forma:

$$\begin{aligned} P(X) &= (X + 1) \cdot (X - (1 - 2i)) \cdot (X - (1 + 2i)) \cdot (X - a) \\ &= (X + 1) \cdot (X^2 - 2X + 5) \cdot (X - a) \\ \bar{p}(2) &= (2 + 1) \cdot (4 - 4 + 5) \cdot (2 - a) \\ &= 45 \end{aligned}$$

Luego $a = -1$. De donde, el polinomio pedido es

$$\begin{aligned} P(X) &= (X + 1) \cdot (X^2 - 2X + 5) \cdot (X + 1) \\ &= (X^2 + 2X + 1)(X^2 - 2X + 5) \\ &= X^4 + 2X^2 + 8X + 5 \end{aligned}$$

8. Considere el polinomio $P(X) = X^3 + pX + q$, donde q es un número real fijo. Determine m y p , en función de q , de modo que dicho polinomio sea divisible por $Q(X) = X^2 + mX - 1$.

Solución. Comencemos por hacer la División Euclidiana. Tenemos:

$$\begin{array}{r} X^3 + pX + q : X^2 + mX - 1 = X - m \\ \underline{\mp X^3 \mp mX^2 \pm X} \\ -mX^2 + (p + 1)X + q \\ \underline{\pm mX^2 \pm m^2X \mp m} \\ (1 + p + m^2)X + (q - m) = 0 \end{array}$$

Luego tenemos:

$$\left| \begin{array}{rcl} 1 + p + m^2 & = & 0 \\ q - m & = & 0 \end{array} \right|$$

Se concluye entonces que $m = q$ y $p = -1 - q^2$

9. Dado el polinomio

$$P(X) = X^3 + 6X^2 - 63X - 392$$

Busquemos sus raíces, sabiendo que una de ellas es de multiplicidad 2.

Solución. La descomposición de $P(X)$, tiene la forma:

$$P(X) = (X - a)^2(X - b) = (X^2 - 2aX + a^2)(X - b)$$

Luego

$$X^3 + 6X^2 - 63X - 392 = X^3 + (-b - 2a)X^2 + (2ab + a^2)X - a^2b$$

Luego por definición de igualdad de polinomios, tenemos:

$$\begin{array}{rcl} X^2 & : & 6 = -2a - b \\ X & : & -63 = 2ab + a^2 \\ Cte & : & -392 = -a^2b \end{array}$$

De donde se obtiene $a_1 = -7$ y $a_2 = 3$

Luego, $b_1 = 8$ y $b_2 = -12$

Es fácil verificar que el par (a_2, b_2) no satisface la tercera ecuación.

Luego la única solución es (a_1, b_1) , es decir

$$P(X) = (X + 7)^2 \cdot (X - 8)$$

8.8 Fracciones Racionales

Definición 8.8.1 Sean $P(X), Q(X) \in K[X]$.

Diremos que $\frac{P(X)}{Q(X)}$, $Q(X) \neq 0$, es una fracción racional.

Definición 8.8.2 Diremos que dos fracciones racionales son iguales si:

$$\frac{P(X)}{Q(X)} = \frac{P'(X)}{Q'(X)} \text{ ssi } P(X) \cdot Q'(X) = Q(X) \cdot P'(X)$$

Definición 8.8.3 El conjunto formado por todas las fracciones racionales con coeficientes en K , será denotado $K(X)$, es decir

$$K(X) = \left\{ \frac{P(X)}{Q(X)}; Q(X) \neq 0; P(X), Q(X) \in K[X] \right\}$$

Definición 8.8.4 En $K(X)$ se define una **suma**, denotada por $+$, y dada por:

$$\frac{P(X)}{H(X)} + \frac{Q(X)}{G(X)} = \frac{P(X)G(X) + Q(X)H(X)}{H(X)G(X)}$$

Definición 8.8.5 Se define la **multiplicación** de la siguiente manera:

$$\frac{P(X)}{H(X)} \cdot \frac{Q(X)}{G(X)} = \frac{P(X)Q(X)}{H(X)G(X)}$$

Definición 8.8.6 A toda fracción racional $F(X) = \frac{P(X)}{Q(X)}$ se le asocia una **función racional**

$$\bar{f} : K \longrightarrow K; \bar{f}(z) = \frac{\bar{p}(z)}{\bar{q}(z)}, \text{ con } \bar{q}(z) \neq 0$$

Proposición 8.8.1 Sean $P(X)$ y $D(X)$ dos polinomios en $K[X]$ con $gr(P(X)) \geq gr(D(X))$, entonces existen $Q(X)$ y $R(X)$ tales que

$$\frac{P(X)}{D(X)} = Q(X) + \frac{R(X)}{D(X)}; gr(R(X)) < gr(D(X)) \text{ o } R(X) = 0$$

Demostración. Por el Algoritmo de la división se tiene que existen $Q(X)$ y $R(X)$ tales que

$$P(X) = Q(X)D(X) + R(X); \text{gr}(R(X)) < \text{gr}(D(X)) \text{ o } R(X) = 0$$

Luego

$$\frac{P(X)}{D(X)} = \frac{Q(X)D(X) + R(X)}{D(X)} = Q(X) + \frac{R(X)}{D(X)}$$

Nota. Diremos que la función racional ha sido descompuesta en fracciones parciales.

Ejemplo. Descompongamos la fracción racional

$$\frac{X^2 - X + 1}{X + 1}$$

En efecto:

$$\begin{array}{r} X^2 - X + 1 : X + 1 = X - 2 \\ \underline{\pm X^2 \pm X} \\ -2X + 1 \\ \underline{\pm 2X \pm 2} \\ 3 \end{array}$$

Luego

$$X^2 - X + 1 = (X + 1)(X - 2) + 3$$

De donde:

$$\frac{X^2 - X + 1}{X + 1} = X - 2 + \frac{3}{X + 1}$$

Teorema 8.8.2 Sean $F(X)$, $G(X)$ y $H(X)$ polinomios en $K[X]$ tales que:

1. $G(X)$ y $H(X)$ son primos relativos
2. $a = \text{gr}(G(X))$, $b = \text{gr}(H(X))$ y $\text{gr}(F(X)) < a + b$

Entonces existe una representación lineal

$$F(X) = P(X)G(X) + Q(X)H(X), \text{ ciertos } P(X), Q(X) \in K[X]$$

con $\text{gr}(P(X)) < b$ y $\text{gr}(Q(X)) < a$. Es decir, en $K(X)$, tenemos:

$$\frac{F(X)}{G(X)H(X)} = \frac{P(X)}{H(X)} + \frac{Q(X)}{G(X)}$$

Ejemplo. Descompongamos en fracciones parciales, la fracción:

$$\frac{6X - 2}{(X - 3)(X + 5)}$$

En efecto, la forma de la descomposición es la siguiente:

$$\frac{6X - 2}{(X - 3)(X + 5)} = \frac{a}{X - 3} + \frac{b}{X + 5}$$

Su representación lineal es:

$$6X - 2 = a(X + 5) + b(X - 3)$$

Luego:

$$6X - 2 = (a + b)X + (5a - 3b)$$

Por la definición de igualdad de polinomios, tenemos:

$$\left. \begin{array}{rcl} a + b & = & 6 \\ 5a - 3b & = & -2 \end{array} \right|$$

De donde $b = 4$ y $a = 2$

Luego:

$$\frac{6X - 2}{(X - 3)(X + 5)} = \frac{2}{X - 3} + \frac{4}{X + 5}$$

Proposición 8.8.3 *Se tiene la descomposición en suma de fracciones parciales siguiente:*

$$\frac{P(X)}{(X - \alpha)^n} = \frac{a_1}{X - \alpha} + \frac{a_2}{(X - \alpha)^2} + \cdots + \frac{a_n}{(X - \alpha)^n}$$

Donde $\text{gr}(P(X)) \leq n - 1$

Ejemplo. Descompongamos la fracción racional siguiente:

$$\frac{X^2 + 5X + 2}{(X + 3)^3}$$

En efecto, la forma de la descomposición es la siguiente:

$$\frac{X^2 + 5X + 2}{(X + 1)^3} = \frac{a}{X + 1} + \frac{b}{(X + 1)^2} + \frac{c}{(X + 1)^3}$$

Su representación lineal es:

$$X^2 + 5X + 2 = a(X + 1)^2 + b(X + 1) + c$$

Luego

$$X^2 + 5X + 2 = aX^2 + 2aX + a + bX + b + c$$

Por la definición de igualdad de polinomios tenemos:

$$\left. \begin{array}{rcl} a & = & 1 \\ 2a + b & = & 5 \\ a + b + c & = & 2 \end{array} \right|$$

Luego $a = 1$, $b = 3$ y $c = -2$ La descomposición buscada es entonces:

$$\frac{X^2 + 5X + 2}{(X + 1)^3} = \frac{1}{X + 1} + \frac{3}{(X + 1)^2} + \frac{-2}{(X + 1)^3}$$

Proposición 8.8.4 *Se tiene la descomposición en suma de fracciones parciales siguiente:*

$$\begin{aligned} \frac{P(X)}{(aX^2 + bX + c)^n} &= \frac{Q_1(X)}{aX^2 + bX + c} + \frac{Q_2(X)}{(aX^2 + bX + c)^2} + \cdots + \\ &+ \frac{Q_n(X)}{(aX^2 + bX + c)^n} \end{aligned}$$

Con $gr(P(X)) < 2n$ y $gr(Q_1), gr(Q_2), \dots, gr(Q_n) \leq 1$

Ejemplo. Descompongamos la fracción racional siguiente:

$$\frac{2X^3 + 3X^2 + 6X}{(X^2 + X + 1)^2}$$

En efecto, la descomposición tiene la forma siguiente:

$$\frac{2X^3 + 3X^2 + 6X}{(X^2 + X + 1)^2} = \frac{aX + b}{X^2 + X + 1} + \frac{cX + d}{(X^2 + X + 1)^2}$$

Luego su representación lineal es la siguiente:

$$2X^3 + 3X^2 + 6X = (aX + b)(X^2 + X + 1) + cX + d$$

De donde:

$$2X^3 + 3X^2 + 6X = aX^3 + aX^2 + aX + bX^2 + bX + b + cX + d$$

Usando la definición de igualdad de polinomios tenemos:

$$\left. \begin{array}{rcl} a & = & 2 \\ a + b & = & 3 \\ a + b + c & = & 6 \\ b + d & = & 0 \end{array} \right\}$$

De donde $a = 2$, $b = 1$, $c = 3$ y $d = -1$

La descomposición buscada es entonces:

$$\frac{2X^3 + 3X^2 + 6X}{(X^2 + X + 1)^2} = \frac{2X + 1}{X^2 + X + 1} + \frac{3X - 1}{(X^2 + X + 1)^2}$$

Ejemplo. Busquemos la forma de la descomposición de:

$$\frac{P(X)}{(X - 2)^2(X^2 + X + 1)^3}; \text{ con } \text{gr}(P(X)) < 8$$

En efecto, la descomposición buscada tiene la forma siguiente:

$$\begin{aligned} \frac{P(X)}{(X - 2)^2(X^2 + X + 1)^3} &= \frac{a}{X - 2} + \frac{b}{(X - 2)^2} + \frac{cX + d}{X^2 + X + 1} + \\ &+ \frac{eX + f}{(X^2 + X + 1)^2} + \frac{gX + h}{(X^2 + X + 1)^3} \end{aligned}$$

8.9 Ejercicios Propuestos

1. En $\mathbb{R}[X]$, descomponga en 6 factores, el polinomio

$$P(X) = X^{12} - 1$$

2. El polinomio $P(X) = X^4 - 1$, descompóngalo en:

- (a) Un factor de grado 1 y un factor grado 3
- (b) En dos factores de grado 2
- (c) En sus factores irreducible en $\mathbb{C}[X]$
- (d) Encuentre sus factores propios mónicos en $\mathbb{R}[X]$

3. Dado $a \in \mathbb{R}$, descomponga $X^6 - a^6$ como producto de factores irreducibles en $\mathbb{C}[X]$

4. Descomponga en sus factores irreducibles el polinomio $P(X) = X^8 - 1$
i) en $\mathbb{R}[X]$; ii) en $\mathbb{Q}[X]$

5. El polinomio $P(X) = X^6 + 1$, descompóngalo en $\mathbb{R}[X]$ en un factor de grado 2 y un factor de grado 4.

6. Demuestre que el polinomio

$$P(X) = (2a - b)X^2 + 4a^2(b - X) + b^2(X - 2a)$$

es divisible por $D_1(X) = X - 2a$ y $D_2(X) = X - b$.

7. Calcule el producto $P(X) = (X^3 + X^2 - 1)(X^2 - X + 1)$. Diga en que se convierte este desarrollo si cambiamos X por $-X$. Deduzca la descomposición de $R(X) = X^5 + X + 1$ en un producto de dos factores.

8. Encuentre un polinomio $P(X)$ con coeficientes enteros, del menor grado posible, tal que $P(\sqrt{2} + \sqrt{3}) = 0$

9. Determinar el cociente y el resto al dividir el polinomio :
- i) $2X^4 - 3X^3 + 4X^2 - 5X + 6$ por $X^2 - 3X + 1$
 - ii) $X^5 - X^4 + 1$ por $2X^3 - 2X$
 - iii) $-4X^3 + X^2$ por $X + \frac{1}{2}$
10. Al dividir el polinomio $aX^4 - 2X^3 + bX^2 - 18X + a$ por $X - 1$, el resto es 3 y el cociente es un polinomio que toma el valor 33 para $X = 2$. Calcular a y b .
11. En $\mathbb{R}[X]$ encuentre:
- (a) Un polinomio de grado 3 que tenga por raíces $1 + i, 1 - i, 2$
 - (b) Un polinomio que tenga por raíces $1, 0, 1 - 2i$
 - (c) Un polinomio que tenga por raíces 2 y 3 y que deje resto 4 al ser dividido por $R(X) = X - 4$
12. Sabiendo que $2i$ es raíz del polinomio
- $$P(X) = X^5 - 3X^4 + 2X^3 - 6X^2 - 8X + 24$$
- encuentre las otras raíces.
13. Encuentre las condiciones que deben cumplir a y b para que
- $$P(X) = X^3 + 3aX + b$$
- tenga:
- (a) Una raíz de multiplicidad dos
 - (b) Una raíz triple
14. Dos de las raíces de $P(X) = X^4 - 2(a^2 + b^2)X^2 + (a^2 - b^2)^2$ son $(a + b)$ y $(a - b)$. Encuentre las otras dos
15. Dado $a \in \mathbb{R}$, demuestre que $P(X) = X^4 + aX^2 + 1$ no puede tener una raíz triple.
16. Encuentre un polinomio $P(X)$ en $\mathbb{C}[X]$, $\mathbb{R}[X]$ o $\mathbb{Q}[X]$, de grado 3, cuyas raíces sean $\alpha, \alpha + 1$ y 2α y tal que el coeficiente de X^2 sea 3. Además determine α .

17. Encuentre todas las raíces en \mathbb{C} del polinomio $X^6 + X^4 + X^2 + 1$.
18. Factorice en $\mathbb{R}[X]$ y en $\mathbb{C}[X]$ los polinomios
- (a) $P(X) = X^4 + 2X^2 - 8$
 - (b) $Q(X) = X^4 + X^3 + X^2 + X$
 - (c) $R(X) = X^3 - X^2 - 7X + 15$, sabiendo que admite a $2 + i$ como raíz).
19. Expresé en la forma $a + bi$ las raíces de $P(X) = X^4 + 4$ y de $Q(X) = X^2 + i$
20. Considere los polinomios $P(X) = X^2 - 4X + 5$ y $Q(X) = X^3 - (1 + 2i)X^2 - 3X + 2i - 1$
- (a) Encuentre los números complejos que son raíces del polinomio $P(X)$
 - (b) Pruebe que el polinomio $Q(X)$ tiene una raíz común α con el polinomio $P(X)$. Determine α
 - (c) Divida $Q(X)$ por $D(X) = X - \alpha$
 - (d) Descomponga $Q(X)$ en factores de grado 1
 - (e) Determine $R(X) \in \mathbb{C}[X]$, de grado minimal que sea múltiplo común de $P(X)$ y del polinomio $S(X) = X^3 - (1 + 2i)X^2 - 3X + a$. Discuta los valores de a . Es único este polinomio $R(X)$?
21. Descomponga en $\mathbb{C}[X]$, los siguientes polinomios a) $X^6 - 1$; b) $X^4 + 16$; c) $X^4 - 2$; d) $X^8 - 1$; e) $X^{12} + 1$
22. Determine los valores de λ para que las ecuaciones siguientes tengan al menos una raíz doble :
- (a) $x^3 - 3x + \lambda = 0$
 - (b) $x^3 - 8x^2 + (13 - \lambda)x - 62\lambda = 0$
 - (c) $x^4 - 4x^3 + (2 - \lambda)x^2 + 2x - 2 = 0$
- y resuelva cada una de estas ecuaciones con las condiciones encontradas

23. Resuelva la ecuación $24x^3 - 14x^2 - 63x + 45 = 0$, sabiendo que una raíz es el doble de la otra
24. Resuelva la ecuación $x^4 - 16x^3 + 86x^2 - 176x + 105 = 0$, sabiendo que 1 y 7 son raíces
25. Resuelva la ecuación $4x^3 + 16x^2 - 9x - 36 = 0$, sabiendo que la suma de dos de sus raíces es cero.
26. Resuelva la ecuación $4x^3 + 20x^2 - 23x + 6 = 0$, sabiendo que tiene dos raíces iguales
27. Descomponer en fracciones parciales, las siguientes funciones racionales

a) $\frac{2z^3 + z + 1}{z - 1};$	b) $\frac{2z + 1}{(z - 1)(z + 2)}$
c) $\frac{z^2 + 1}{(z - 1)^3}$	d) $\frac{z^2 - z + 2}{z^4 - 5z^2 + 4}$
e) $\frac{z^2}{(z^2 + 1)}$	g) $\frac{3z^3 + 4}{z^2 + 3z + 2}$
h) $\frac{1}{z^2 + 1}$	i) $\frac{1}{(z^2 + 1)}$
j) $\frac{1}{z^2 + 4}$	k) $\frac{4z^3 - 2z^2 + z + 1}{(z - 2)(z + 1)^3}$
l) $\frac{z^2 - z + 4}{(z - 1)(z^2 + 2z + 2)^2}$	m) $\frac{7z^3 + 20x^2 + 35z - 13}{z^2(z^2 - 4z + 1)}$

Bibliografía

- [1] **Edgard De Alencar**, *Relações y Funções*, Livraria Nobel (Brasil). 1968
- [2] **Raúl Benavides Gallardo**, *Ejercicios resueltos de lgebra*, Universidad de La Frontera, 1994
- [3] **Enzo Gentile**, *Estructuras Algebraicas*, Monografía N 3, Serie Matemática, OEA, 1967
- [4] **Eric Goles**, *Algebra*, Dolmen. 1993
- [5] **Alamiro Robledo.**, *Lecciones de Algebra Elemental Moderna*. Editorial Universitaria. 1973
- [6] **Armando O. Rojo**, *Algebra*, Ed. El Ateneo, Buenos Aires, 1992
- [7] **Elbridge Vance**, *Algebra superior moderna*, 1965

Índice de términos

- Algebraicamente cerrado, 278
- Anillo, 213
- Antisimetría, 130
- Aritmética, 223
- Asociatividad, 199
- Axioma, 14
- Axioma de Inducción, 76

- Binomio de Newton, 87

- Cancelable, 207
- Cardinal de un conjunto, 39
- Clase de equivalencia, 146
- Codominio de una función, 166
- Codominio de una relación, 118
- Coficiente supremo, 262
- Complejos conjugados, 235
- Complemento, 45
- Composición de funciones, 175
- Congruencias en \mathbb{Z} , 151
- Congruencias módulo n , 152
- Conjunto cociente, 147
- Conjunto ordenado, 161
- Conjunto potencia, 49
- Conjunto universal, 38
- Conjunto vacío, 39
- Conmutatividad, 199
- Construcción de \mathbb{Q} , 155
- Construcción de \mathbb{Z} , 154

- Construcción de los números complejos, 229
- Construcción de los naturales según Peano, 75
- Contradicción, 13
- Contraejemplo, 44
- Cuantificadores, 40
- Cuerpo, 214
- Cuociente, 276

- Desarrollo del binomio, 101
- Descomposición en $\mathbb{C}[X]$, 278
- Descomposición en $\mathbb{Q}[X]$, 281
- Descomposición en $\mathbb{R}[X]$, 279, 281
- Distancia, 240
- Distancia entre números complejos, 236
- Distributividad, 200
- dividendo, 276
- División Euclidiana, 275, 276
- Divisibilidad de polinomios, 271
- divisor, 276
- Divisor de cero, 213
- Divisores propios, 274
- Dominio de una función, 166
- Dominio de una relación, 117

- Elemento absorbente, 202
- Elemento cancelable, 207

- Elemento idempotente, 202
 Elemento inverso, 203
 Elemento neutro, 200
 Elevación a potencia de un número complejo, 243
 Estructura algebraica, 197, 198
 Estructura algebraica de los números complejos, 232
 Estructura de \mathbb{Z}_n , 217
 Estructura de S_n , 218
 Extensión de una función, 173
 Extracción de raíces, 246
 Fórmula de De Moivre, 248
 Factorial, 87
 Factorización de un polinomio, 273
 Forma exponencial de un número complejo, 250
 Forma polar de un número complejo, 241
 Forma trigonométrica de un número complejo, 241
 Fracciones racionales, 287
 Función biyectiva, 175
 Función epiyectiva, 175
 función identidad, 174
 Función inversa, 176, 177
 Función inyectiva, 174
 Función polinómica, 265, 266
 Función racional, 288
 Funciones, 165
 Funciones entre conjuntos finitos, 185, 188
 Funciones entre conjuntos no finitos, 189
 Grado de un polinomio, 261
 Grafo de una relación, 120
 Grupo, 210
 Idempotente, 202
 Igualdad de conjuntos, 38
 Igualdad de funciones, 170
 Igualdad de números complejos, 230
 Igualdad de pares ordenados, 113
 Igualdad de polinomios, 261
 Imagen de una función, 166
 Imagen de una relación, 118
 Imagen recíproca, 172
 Indeterminada, 260
 Inverso, 203
 Ley de composición interna, 197, 198
 Multiplicación de números complejos, 242
 Multiplicidad de una raíz, 266
 Número combinatorio, 89
 Número combinatorio, 91
 Número factorial, 87
 Números complejos, 229
 Números naturales, 75
 Par ordenado, 113
 Paradojas, 8
 Parte imaginaria, 230
 Parte real, 230
 Partición, 149
 Permutaciones, 181, 182
 Polinomio complejo, 260
 Polinomio constante, 262
 Polinomio irreducible, 274

- Polinomio mónico, 262
- Polinomio racional, 260
- Polinomio real, 260
- Polinomio sobre K , 260
- Polinomios, 259
- Postulados de Peano, 75
- Predicado, 39
- Producto cartesiano, 113, 114
- Progresión aritmética, 70
- Progresión geométrica, 72
- Proposición Lógica, 7
- Proposiciones equivalentes, 9
- Raíces de un polinomio, 266
- Reducción de circuitos, 30
- Reflexividad, 122
- Relación de equivalencia, 141
- Relación de orden parcial, 162
- Relación de orden total, 162
- Relaciones binarias, 113, 122
- Relaciones de equivalencia, 140
- Relaciones de orden, 160
- Relaciones entre conjunto, 116
- Resto, 276
- Restricción, 173
- Simetría, 125
- Subconjunto, 44
- Subestructuras, 208
- Subgrupo, 214
- Subgrupo propio, 215
- Suma de cuadrados, 67, 74, 76
- Suma de cubos, 77
- Suma de los múltiplos de 4, 79
- Suma de los números impares, 78
- Suma de los números pares, 78
- Suma de polinomios, 263
- Sumatoria, 61
- Sumatoria propiedades, 62
- Tautología, 13
- Teo. Fund. sobre rel. de equiv., 149
- Teorema, 14
- Teorema de Cayley, 218
- Teorema de descomposición única, 275
- Teorema de Descomposición en $\mathbb{R}[X]$, 281
- Teorema del Binomio, 102
- Teorema del Factor, 277
- Teorema del Resto, 276
- Teorema Fundamental del Álgebra, 279
- Transitividad, 129
- Triángulo de Pascal, 92, 104
- Valor absoluto, 236
- Valor de verdad, 10