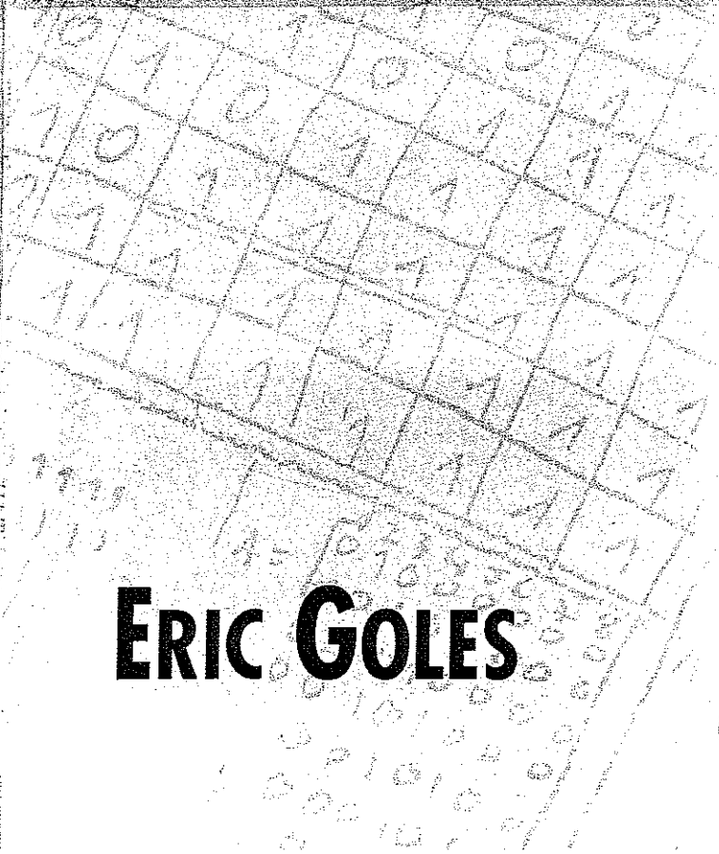
lgebra" es un libro que obedece a la voluntad de entusiasmar al lector, mostrándole, a través de desarrollos simples y motivantes, la vigencia naravilla de las matemáticas y su aplicación a problemas de muy variada índole.

s andes tópicos cubiertos son: lógica, conjuntos, inducción matemática, aciones, funciones y estructuras algebraicas. En el contexto de estructuras se udian las propiedades básicas de complejos, polinomios y matrices. Además, pecto de las matrices, se estudia la solución de sistemas lineales a través de al...amiento y, en el caso cuadrado, del algoritmo de Gauss.

los los capítulos y temas vienen acompañados de ejercicios y soluciones en gran te ae ellos.

EDICIONES DOLMEN

ALGEBRA



ERIC GOLES

Inscripción Nº 87.679

EDICIONES PEDAGOGICAS CHILENAS S.A.
EDICIONES DOLMEN
SANTA MAGDALENA 187, SANTIAGO

Esta primera edición se terminó de imprimir en octubre de 1993, en los Talleres Gráficos de Editorial Universitaria.

Dirección : Jaime Cordero
Cubierta : Marian Salamovich
Daniça Goles

I.S.B.N. 956-201-189-5
D-LNB- 213

PRINTED IN CHILE / IMPRESO EN CHILE

ERIC GOLES CHACC

ALGEBRA

EDICIONES DOLMEN

INDICE

Introducción	13
Capítulo I, Lógica y Conjuntos	19
1.1. Algebra proposicional	19
1.1.1. Tautologías o teoremas lógicos	22
1.2. Conjuntos	25
1.2.1. Igualdad entre conjuntos	27
1.2.2. Inclusión de conjuntos	29
1.2.3. Diferencia y complemento	30
1.2.4. Unión e intersección de conjuntos	32
1.2.5. Diagramas de Venn	33
1.2.6. Algebra de conjuntos	34
1.2.7. Diferencia simétrica	35
1.2.8. Conjuntos finitos e infinitos	36
1.3. Cuantificadores lógicos	37
1.3.1. Negación de cuantificadores	38
1.4. Indices, familias de conjuntos y particiones	40
Ejercicios Capítulo I	44
Temas Capítulo I	49
1. Circuitos lógicos	51
Ejercicios circuitos lógicos	57
2. De como el barbero no tiene quien lo afeite	59
Paradoja de Rusell	59
Ejercicios lógicos	60
Capítulo II, Inducción Matemática	63
2.1. Principio de inducción	63
2.2. Usos y abusos inductivos	66
2.3. Recurrencias	68
2.4. Progresiones	74
2.4.1. Progresiones aritméticas	74
2.4.2. Progresiones geométricas	75
2.5. Coeficientes binomiales	76
2.5.1. Triángulo de Pascal	78
2.5.2. Binomio de Newton	80
2.6. Interpretación combinatorial de los coeficientes binomiales	82
2.7. Sumatorias múltiples	84
Ejercicios Capítulo II	87
Temas Capítulo II	93
1. Tallarines con salsa y/o tren al sur	95

2. Partición de la Atlántida 96
3. Fractal=Pascal 105
4. Más recurrencias 107
4.1. Torre de Hanoi 107
4.2. Variaciones sobre trozos de pizza 112
Ejercicios pizzas 115
4.3. Números de Fibonacci 116
Embaldosados $2 \times n$ 117
Ejercicios Fibonacci 118
Capítulo III, Relaciones 121
3.1. Pares ordenados y n-tuplas 121
3.2. Productos cartesianos 123
3.3. Relaciones binarias 126
3.4. Representaciones de una relación 128
3.5. Clasificación de relaciones 133
3.6. Relaciones de orden 141
3.7. Teoría de números 143
3.7.1. Algoritmo de la división 143
3.7.2. Algoritmo de Euclides 144
3.8. Relaciones de equivalencia 150
3.9. Clases de congruencia módulo p 154
Ejercicios Capítulo III 157
Temas Capítulo III 163
1. Parentesco en la gran pradera 165
Ejercicios en la pradera 167
2. Sobre bases, Euclides y otras hierbas 168
2.1. Expresión de un número en base b 168
2.2. Complejidad Euclideana 170
Ejercicios Euclideanos 172
3. Congruencias lineales 173
Ejercicios congruencias 177
4. Grafos y matrices 178
Ejercicios grafos 184
5. Agencia matrimonial "La Solución" 186
Ejercicios matrimoniales 194
6. Ordenes son órdenes 195
Capítulo IV, Funciones 205
4.1. Introducción 205
4.2. Funciones y conjuntos 206
4.2.1. Propiedades del conjunto imagen y pre-imagen 207
4.2.2. Restricción y extensión de funciones 210
4.3. Clasificación y zoología funcionaria: epiyecciones, inyecciones, biyecciones 211
4.4. Funciones sobre conjuntos finitos 214
4.5. Identidades combinatoriales 216
4.5.1. Número de funciones entre dos conjuntos finitos 216
4.5.2. Número de funciones inyectivas 216
4.5.3. Número de inyecciones con distinta imagen 218
4.6. Función inversa 218
4.7. Composición de funciones 219
4.8. Permutaciones 223
4.8.1. Propiedades generales de permutaciones en S_n 225
Ejercicios Capítulo IV 227
Temas Capítulo IV 231
1. Cantor, cardinalidad y otros resbaladeros 233
Ejercicios Cantorianos 239
2. Sobre parentela, casorios y tribus 240
Ejercicios antropológicos 244
Capítulo V, Estructuras Algebraicas 247
5.1. Introducción 247
5.2. Ley de composición interna 252
5.3. Propiedades de estructuras 255
5.4. Subestructuras 258
5.5. Estructura de congruencias 259
5.6. Clasificación de estructuras 262
5.7. Morfismos 263
5.8. Grupos 267
5.8.1. Propiedades elementales de un grupo 268
5.8.2. Subgrupos 270
5.8.3. Representación de Cayley 272
5.8.4. Grupo de matrices isomorfo a (S_n, o) 275
5.8.5. Teorema de Lagrange 282
5.8.6. Grupos cíclicos 284
5.9. Anillos 288
5.9.1. Propiedades elementales de un anillo 291
5.10. Cuerpos 293
Ejercicios Capítulo V 296
Temas Capítulo V 301
1. Torres 303
2. Variaciones sobre el triángulo de Las Bermudas 308
Ejercicios en Bermudas 312

3. La Pascalina reproductora 314
4. Funciones indicatrices 317
Ejercicios indicatrices 321
Capítulo VI, Complejos y Polinomios 323
6.1. El Cuerpo de los complejos 323
6.1.1. Conjugados 325
6.1.2. Interpretación geométrica de $\mathbb{C}$ 326
6.1.3. Forma polar de un número complejo 330
6.1.4. Potencias complejas 332
6.1.5. Raíces n-ésimas de un complejo 333
6.2. El anillo de los polinomios 336
6.2.1. División de polinomios 340
6.2.2. Máximo común divisor de dos polinomios 344
6.2.3. Raíces de polinomios 345
6.2.4. Polinomios irreductibles 350
6.2.5. Relación entre raíces y coeficientes polinomiales 353
Ejercicios Capítulo VI 356
Temas Capítulo VI 361
1. Raíces 363
2. Descomposición de fracciones racionales 367
Ejercicios racionales 369
Capítulo VII, Algebra Matricial 371
7.1. Matrices particulares 376
7.2. Potencias, traspuestas, inversas 379
7.3. Matrices elementales 382
7.4. Sistemas lineales y escalonamiento de matrices 386
7.5. Solución general de sistemas lineales 391
7.6. Sistemas cuadrados y algoritmo de Gauss 394
7.7. Cálculo de inversas y sistemas con varios lados derechos 397
7.8. Factorización LU 400
7.9. Complejidad del algoritmo de Gauss 402
Ejercicios Capítulo VII 403
Temas Capítulo VII 411
1. La melancolía 413
1.1. Matrices mágicas 413
1.2. Matrices mágicas simétricas 415
Ejercicios mágicos 416
2. Del maquiavelismo matricial a la Strassen 417
Ejercicios Maquiavélicos 421
Solucionario 423
Soluciones Capítulo I 423
Soluciones Capítulo II 423
Soluciones Capítulo III 425
Soluciones Capítulo IV 426
Soluciones Capítulo V 427
Soluciones Capítulo VI 429
Soluciones Capítulo VII 430
Referencias 433
Glosario 437

INTRODUCCION

Este libro cubre el programa semestral de un curso de álgebra, dedicado preferentemente a estudiantes de carreras técnicas y de ingeniería. El libro está estructurado en capítulos y temas. Los capítulos tienen por objetivo introducir las nociones, herramientas y resultados esenciales. Los temas obedecen a la voluntad de mostrar al lector, a través de desarrollos simples y motivantes, que la matemática es algo vivo y en continua evolución, siendo capaz de atacar problemas de muy variada índole. Estos corresponden, en su gran mayoría, a aplicaciones recientes relacionadas con el material entregado en los capítulos, entre otras: concepción de circuitos, determinación de listas de preferencia, modelamiento de relaciones de parentesco y complejidad de algoritmos. También, mediante algunos temas, se complementa el material del capítulo desarrollando resultados clásicos, a nuestro juicio importantes, por ejemplo: la paradoja de Rusell en el capítulo I y el teorema de Cantor en el capítulo IV. En todos estos temas la puerta queda abierta (a través de preguntas y ejercicios propuestos), de manera que los lectores puedan investigar y, en ocasiones, realizar experimentos computacionales.

En varias oportunidades he sacrificado la rigurosidad de la presentación en beneficio de una buena comprensión intuitiva. Esto a través de ejemplos introductorios o verificando casos particulares y, a veces, dejando de lado detalles técnicos. Es mi experiencia que esta óptica ha sido muy beneficiosa para los alumnos que han seguido el texto.

El material de base del libro está contenido, casi en su totalidad, en los capítulos. Por ello el lector deberá leerlos en orden secuencial. Es recomendable desarrollar algunos de los ejercicios propuestos así como al menos un tema de cada capítulo. Esto último ayudará a una mejor comprensión de las nociones del capítulo, así como al desarrollo de la iniciativa e imaginación del lector.

Para el profesor de un curso semestral que utilice este texto, recomiendo tratar los capítulos en forma secuencial, incluir en clase de cátedra al menos tres temas y, de manera ineludible, el de cardinalidad. Sería también conveniente desarrollar en clase auxiliar algunos de los ejercicios propuestos con un asterisco (de mayor dificultad) y al menos cinco temas. Me parecen insoslayables, en el marco de una escuela de ingeniería, los temas sobre matrimonios estables, recurrencias y el algoritmo de Strassen para multiplicar matrices.

A continuación detallo el contenido del libro:

El primer capítulo trata de las operaciones lógicas usuales, cuantificadores lógicos, álgebra y familias de conjuntos. Se desarrollan dos temas: los Circuitos Lógicos y la Paradoja de Rusell. Además, se proponen ejercicios de diversa dificultad.

El capítulo dos corresponde a Inducción Matemática y Recursividad. Implícitamente se insiste reiteradamente en la noción de proceso iterativo y por ende algorítmico. En cuanto al principio inductivo, el énfasis no está en la prueba por inducción de una fórmula ya establecida sino en el problema global: dada una expresión, por ejemplo una sumatoria, tratar de conjeturar, mediante ensayos, cual es su fórmula cerrada y posteriormente probarla por inducción. Se presenta una gran cantidad de ejemplos, algunos mostrando cómo no hay que utilizar la inducción, y otros poniendo en evidencia una fructífera estrategia de la algorítmica actual: "dividir para conquistar". Posteriormente se desarrollan las definiciones recursivas usuales (sumatorias, factoriales, coeficientes binomiales y triángulo de Pascal) y se presentan, a través de ejemplos, algunas de sus aplicaciones. En cuanto a los temas; todos corresponden a aplicaciones del principio de inducción y de la recursividad. Figura aquí una demostración, muy gráfica, del teorema de los cinco colores, la complejidad del puzzle conocido como la torre de Hanoi, las diversas maneras de cortar una pizza y la clásica, y sin embargo tan actual, sucesión de Fibonacci, presentada ésta en un contexto geométrico (enumeración de embaldosados de un tablero de $2 \times n$). En un contexto más estético se presenta una visualización computacional del triángulo de Pascal, relacionada con los recientes desarrollos en autómatas celulares (paradigma del cálculo paralelo) y los denominados "objetos fractales".

El capítulo tres está dedicado a la noción de Relación; en él se definen los pares ordenados, producto cartesiano, las propiedades más importantes de relaciones y sus representaciones más usuales. En particular se introduce la noción de matriz binaria (elementos 0 y 1) aplicada a la caracterización de una relación. Se pone énfasis en relaciones de orden y equivalencia. En cuanto a las primeras, se estudia, con cierta profundidad, la relación de divisibilidad, introduciendo el tatarabuelo de todos los algoritmos, Euclides, y los rudimentos de teoría de números. Por otra parte, las relaciones de equivalencia se desarrollan en torno a las congruencias. En los temas se presenta una curiosa estructuración de las relaciones de parentesco en una tribu indígena, la noción de base entera y su relación con la convergencia del algoritmo de Euclides, el teorema de caracterización de soluciones para congruencias lineales, el teorema que relaciona la potencia de una matriz binaria (con operaciones booleanas) con la representación gráfica de una relación, el algoritmo de elección de parejas entre listas ordenadas de preferencias y una

relación de orden, actualmente utilizada en física para modelar la dinámica de avalanchas.

El capítulo cuatro está dedicado a la noción de función y el tratamiento algebraico de las mismas mediante imágenes, pre-imágenes y la operación de composición. También se desarrollan las interpretaciones combinatoriales mediante funciones sobre conjuntos finitos, de números factoriales y coeficientes binomiales. Se termina el capítulo con la noción de permutación y su estructuración mediante la operación composición, preparando así el terreno para las estructuras algebraicas. Los temas que se desarrollan en este capítulo son dos. El primero, a mi juicio imprescindible, se refiere a los rudimentos de la teoría de cardinalidad, presentando el teorema de Cantor. El otro tema tiene que ver con el modelamiento, mediante permutaciones de las relaciones de parentesco en una tribu amazónica.

En el capítulo cinco se estudian las Estructuras Algebraicas. La noción de estructrura se introduce mediante tres ejemplos, de naturaleza aparentemente distinta, que obedecen a un mismo principio: una operación idéntica descrita por una tabla de doble entrada. Esto permite presentar intuitivamente la noción de estructura como la relación entre objetos mediante una operación. Además, prepara ya la noción de morfismo: tablas iguales cuando se hace abstracción de los elementos (en el sentido de conjuntos), como manera de comparar estructuras. Posteriormente, se introduce la noción de ley de composición interna y sus propiedades. En este contexto, se define formalmente la noción de morfismo y se presentan las estructuras de grupo, anillo y cuerpo, haciendo énfasis en la de grupo, para mostrar que, a partir de axiomas bastante elementales, es posible obtener profundos resultados algebraicos. En particular, se demuestra que un grupo finito es isomorfo a un grupo de permutaciones (teorema de Cayley), y por ende a un grupo de matrices de permutación. También se desarrolla el teorema de Lagrange y el concepto de grupo cíclico.

En cuanto a Anillos y Cuerpos, se presentan diversos ejemplos, en particular las estructuras de congruencia. Se termina el capítulo demostrando que la estructura de congruencias módulo p es un cuerpo si y sólo si p es un número primo.

Los temas corresponden a una interpretación geométrica (en un tablero de ajedrez) del grupo de Klein, el estudio de la circulación vehicular en torno a una plaza (introduciendo de paso el análisis de un lenguaje formal vía la noción de "palabras equivalentes" en un alfabeto finito) y el estudio algebraico de un autómata celular evolucionando en una línea mediante una función suma módulo p.

El capítulo seis está dedicado a dos estructuras algebraicas de gran utilidad: los números complejos y los polinomios. Se presenta aquí el álgebra usual de los complejos, su interpretación geométrica y el cálculo de raíces enésimas, en particular de la unidad. En cuanto a los polinomios, éstos se introducen como objeto formal en una indeterminada x para, más adelante, ver sus relaciones con la función asociada. Se estudia la divisibilidad, el algoritmo de división, la reductibilidad y el mínimo común denominador de polinomios. Posteriormente se estudian las raíces de un polinomio y el número de las mismas. Mediante el enunciado del teorema fundamental (obviamente sin demostración) se determina la factorización de un polinomio en factores lineales sobre los complejos y en factores lineales y cuadráticos irreductibles sobre los números reales. Se termina el capítulo presentando la relación entre los coeficientes de un polinomio y sus raíces.

Los temas en este caso son dos: el primero trata sobre la existencia de raíces de un polinomio real de grado impar, y el segundo muestra la factorización de fracciones racionales mediante la descomposición del denominador en factores irreductibles.

El séptimo y último capítulo está dedicado al álgebra de matrices. Se presenta dicha estructura con las operaciones de suma y multiplicación, introduciendo las nociones de matriz inversa, traspuesta, triangular y diagonal. Posteriormente son definidas las matrices elementales para, mediante ellas, escalonar matrices arbitarias y estudiar la resolución general de sistemas lineales. En el caso particular de matrices cuadradas se desarrolla el algoritmo de Gauss, probando que una matriz es invertible si y sólo si el producto de los pivotes de la matriz triangular generada por Gauss no es nulo. Se finaliza el capítulo con la descomposición LU y el cálculo del número de operaciones (multiplicaciones y divisiones) necesarias para triangularizar una matriz cuadrada.

Desarrollamos dos temas, el primero dedicado a las matrices mágicas (suma por filas, columnas y diagonales constante) y su escritura, en el caso 3×3, en función de dos matrices particulares. El segundo tema presenta el algoritmo de Strassen para multiplicar matrices de 2×2 en 7 multiplicaciones en lugar de 8. A continuación, mediante el principio recursivo de "dividir para conquistar", se demuestra que, las 7 multiplicaciones de Strassen, lejos de ser un ejercicio ocioso, permiten un sustancial ahorro en la multiplicación de matrices arbitrarias.

Al final del texto se entregan las referencias correspondientes a las principales fuentes utilizadas en la concepción de capítulos y temas, un solucionario parcial de los ejercicios y un glosario.

La realización de este libro no hubiese sido posible sin la participación de profesores y estudiantes de la Facultad de Ciencias Físicas y Matemáticas de la Universidad de Chile que buscaron en él, con saña y entusiasmo, chambonadas y ejercicios imposibles. Muy en particular agradezco a los profesores Pablo Dartnell, Antun Domic Bezic, José Henríquez y Jaime San Martín por sus valiosos aportes. Es también mi convicción que este trabajo es una consecuencia natural del particular ambiente intelectual y de camaradería que se vive cotidianamente en el Departamento de Ingeniería Matemática de nuestra Facultad. Con respecto a la materialización del texto debo agradecer a todas las secretarias del departamento, muy en particular a Regina Mateluna por su excelente trabajo en TEX y la paciencia para soportar estoicamente los continuos cambios en la redacción del texto.

No podría concluir estas líneas sin agradecer a mi familia, muy en particular a Haydée: paciencia y comprensión por el que se es en un oficio que todo lo inunda, sin el menor respeto por lo cotidiano.

Eric Goles Chacc

En Santiago, Junio de 1993.

CAPITULO I

Los cuatro puntos cardinales
son tres: el Norte y el Sur.
Vicente Huidobro

LOGICA Y CONJUNTOS

1.1 Algebra Proposicional.

La lógica ocupa un lugar de primera importancia en el quehacer humano y en particular en matemáticas. Mucho se ha escrito al respecto y aún hoy en día se discuten sus fundamentos. En el marco de este curso de introducción al lenguaje algebraico, estudiaremos las operaciones más usuales en lógica proposicional.

Una proposición lógica la entenderemos como una sentencia sujeta a dos valores constantes: "*verdadero*" (V) o "*falso*" (F), denominados *valores de verdad*. Denotaremos una proposición mediante letras minúsculas, $p, q, r, s, ...$ etcétera. Por ejemplo:

p : "murió el roto Quezada"

q : "estoy en medio de un triángulo"

son proposiciones que denominamos simples por no contener dentro de sí mismas otra proposición.

A partir de proposiciones simples podemos construir otras, llamadas compuestas, mediante operaciones denominadas *conectivos lógicos*. Estas son la negación, conjunción, disyunción, implicación y equivalencia. Las cuales definimos a través de *tablas de verdad*.

Sean p y q dos proposiciones; sus valores de verdad son V y F y las posibles combinaciones de estos valores son:

p	q
F	F
F	V
V	F
V	V

Para cada par de valores de verdad, según sea la operación definida entre p y q, obtendremos un resultado (V o F).

Negación. Dada una proposición p, su *negación*, que denotaremos $\bar{p}$, toma el valor de verdad contrario a p. Su tabla de verdad es la siguiente:

p	$\bar{p}$
F	V
V	F

A modo de ejemplo, la negación de "murió el roto Quezada" es "no murió el roto Quezada".

Disyunción. Dadas dos proposiciones p y q, definimos la proposición compuesta $p \vee q$, denominada la *disyunción* ("o lógico") entre p y q como aquella que es falsa sólo si p y q son falsas. Su tabla de verdad es la siguiente:

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

Dadas las proposiciones simples "murió el roto Quezada" y "estoy en medio de un triángulo", su disyunción es la proposición compuesta "murió el roto Quezada o estoy en medio de un triángulo".

Conjunción. Dadas las proposiciones p y q, definimos $p \wedge q$, denominada la *conjunción* ("y lógico") entre p y q como aquella que es verdadera sólo si p y q son verdaderas. Su tabla de verdad es la siguiente:

p	q	$p \wedge q$
F	F	F
F	V	F
V	F	F
V	V	V

Tomando las mismas proposiciones simples del ejemplo anterior, su conjunción sería "murió el roto Quezada y estoy en medio de un triángulo".

Implicación. Dadas las proposiciones p y q, definimos la *implicación*, $p \Rightarrow q$, que se lee "si p entonces q" (o bien p implica q), como la proposición condicional que es falsa sólo si p es verdadera y q falsa. Dicho de otra manera, una proposición verdadera no puede implicar una proposición falsa (es falso que una proposición verdadera implique una falsa). Su tabla de verdad es la siguiente:

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

Para las proposiciones del ejemplo anterior, la implicación sería "si murió el roto Quezada entonces estoy en medio de un triángulo".

Este tipo de proposición condicional es muy útil en la concepción de lenguajes computacionales. En la mayoría de ellos existe una instrucción del tipo "si p entonces q". Por ejemplo: "si x es un número par entonces vaya a la instrucción 666".

Doble implicación o equivalencia. Dadas las proposiciones p y q, definimos la *equivalencia*, $p \Leftrightarrow q$, como la proposición bicondicional que se lee "p si y sólo si q" (o bien "p es equivalente a q") y que es verdadera sólo si p y q tienen asignado el mismo valor de verdad. Su tabla es la siguiente:

p	q	$p \Leftrightarrow q$
F	F	V
F	V	F
V	F	F
V	V	V

Considerando las proposiciones anteriores, la equivalencia sería "murió el roto Quezada si y sólo si estoy en medio de un triángulo".

Mediante las operaciones que hemos definido, podemos construir otras proposiciones más complejas y evaluarlas mediante tablas de verdad. Para ello es a menudo conveniente agrupar proposiciones entre paréntesis: $(\overline{p \wedge q})$, $(p \Rightarrow q) \vee r$, etcétera. Entenderemos que los conectivos lógicos aplicados a una proposición entre paréntesis operan sobre toda la proposición al interior de los paréntesis. Por ejemplo, $(\overline{p \wedge q})$ debe leerse "no es cierto que $p \wedge q$".

Desarrollemos, a modo de ejemplo, la tabla de verdad de la siguiente proposición compuesta: $(p \vee \bar{q}) \wedge \bar{p}$. Para simplificar los cálculos es conveniente determinar los valores de verdad de las proposiciones simples que en ella figuran y posteriormente calcular las compuestas, combinando los valores de verdad ya calculados.

1	2	3	4	5	6
p	q	$\bar{p}$	$\bar{q}$	$p \vee \bar{q}$	$(p \vee \bar{q}) \wedge \bar{p}$
F	F	V	V	V	V
F	V	V	F	F	F
V	F	F	V	V	F
V	V	F	F	V	F

El cálculo anterior se desglosa de la siguiente manera:

1. Se calculan los valores de verdad de $\bar{p}$ y $\bar{q}$, según la definición de la negación, directamente de las columnas 1 y 2.
2. Se calcula el valor de verdad de $p \vee \bar{q}$ (columna 5) aplicando la definición de la disyunción a las columnas 1 y 4.
3. Se calcula el valor de verdad final (columna 6) aplicando la definición de la conjunción a las columnas 5 y 3.

Mediante la proposición lógica bicondicional de equivalencia es posible "comparar" dos proposiciones. Por ejemplo, consideremos las tablas de verdad de las proposiciones $p \vee q$ *y* $q \vee p$:

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

Vemos que $p \vee q$ y $q \vee p$ tienen la misma tabla de verdad como aparece en la quinta columna, luego la proposición $(p \vee q) \iff (q \vee p)$ es siempre verdadera. En lo sucesivo, dos proposiciones p y q se dirán *equivalentes* si tienen los mismos valores de verdad. En tal caso notaremos $p \iff q$.

Denominaremos *tautología* o *teorema lógico* a una proposición siempre verdadera.

1.1.1 Tautologías o teoremas lógicos.

Dadas las proposiciones p, q, s :

Asociatividad:

$$p \vee (q \vee s) \iff (p \vee q) \vee s \tag{1.1}$$

$$p \wedge (q \wedge s) \iff (p \wedge q) \wedge s.$$

Conmutatividad:

$$p \vee q \iff q \vee p, \quad p \wedge q \iff q \wedge p. \tag{1.2}$$

Distributividad:

$$p \wedge (q \vee s) \iff (p \wedge q) \vee (p \wedge s) \qquad (\wedge \text{ con respecto a } \vee) \tag{1.3}$$
$$p \vee (q \wedge s) \iff (p \vee q) \wedge (p \vee s) \qquad (\vee \text{ con respecto a } \wedge).$$

Doble negación:

$$\bar{\bar{p}} \iff p. \tag{1.4}$$

Principio de contradicción:

$$\overline{(p \wedge \bar{p})} \iff V \text{ (siempre verdadero).} \tag{1.5}$$

Principio del tercero excluido:

$$p \vee \bar{p} \iff V. \tag{1.6}$$

Leyes de Complementación o de De Morgan:

$$\overline{(p \vee q)} \iff \bar{p} \wedge \bar{q}, \quad \overline{(p \wedge q)} \iff \bar{p} \vee \bar{q}. \tag{1.7}$$

Contrarrecíproca:

$$(p \Rightarrow q) \iff (\bar{q} \Rightarrow \bar{p}). \tag{1.8}$$

Otros teoremas relacionan diferentes conectivos lógicos entre sí:

Equivalencia y doble implicación:

$$(p \iff q) \iff ((p \Longrightarrow q) \wedge (q \Longrightarrow p)). \tag{1.9}$$

Reducción de la implicación y la equivalencia a los conectivos $\vee, \wedge, -$:

$$(p \Longrightarrow q) \iff (\bar{p} \vee q) \tag{1.10}$$
$$(p \iff q) \iff ((\bar{p} \wedge \bar{q}) \vee (p \wedge q)). \tag{1.11}$$

Demostremos algunos de estos teoremas:

El principio de contradicción, (1.5), se demuestra directamente de la tabla de verdad

p	$\bar{p}$	$p \wedge \bar{p}$	$\overline{(p \wedge \bar{p})}$
F	V	F	V
V	F	F	V

■

Demostremos una de las leyes de De Morgan, (1.7):

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

p	q	$\bar{p}$	$\bar{q}$	$p \vee q$	$\overline{(p \vee q)}$	$\bar{p} \wedge \bar{q}$	$\overline{(p \vee q)} \Longleftrightarrow \bar{p} \wedge \bar{q}$
F	F	V	V	F	V	V	V
F	V	V	F	V	F	F	V
V	F	F	V	V	F	F	V
V	V	F	F	V	F	F	V

■

También es posible realizar demostraciones de manera algebraica mediante el reemplazo por tautologías conocidas. Demostremos de este modo el teorema (1.11):

De la tautología (1.9):

$$(p \Longleftrightarrow q) \Longleftrightarrow (p \Longrightarrow q) \wedge (q \Longrightarrow p),$$

de la tautología (1.10):

$$\Longleftrightarrow (\bar{p} \vee q) \wedge (\bar{q} \vee p),$$

de la propiedad distributiva:

$$\Longleftrightarrow [(\bar{p} \vee q) \wedge \bar{q}] \vee [(\bar{p} \vee q) \wedge p]$$

$$\Longleftrightarrow [(\bar{p} \wedge \bar{q}) \vee (q \wedge \bar{q})] \vee [(\bar{p} \wedge p) \vee (q \wedge p)].$$

Es directo ver, del principio de contradicción (teorema (1.5)), que $q \wedge \bar{q} \Longleftrightarrow F$ y que $\bar{p} \wedge p \Longleftrightarrow F$, de donde:

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

por conmutatividad:

$$\Longleftrightarrow (\bar{p} \wedge \bar{q}) \vee (p \wedge q) \quad ■$$

Veamos, como ejercicio, un último desarrollo proposicional, utilizando reemplazos. Demostremos la tautología:

$$u \Leftrightarrow (\bar{p} \wedge \bar{q}) \vee (p \wedge \bar{q}) \vee (\bar{p} \wedge q) \vee (p \wedge q) \Leftrightarrow V.$$

Utilizando la conmutatividad y la asociatividad:

$$u \Leftrightarrow [(\bar{p} \wedge \bar{q}) \vee (\bar{p} \wedge q)] \vee [(p \wedge \bar{q}) \vee (p \wedge q)].$$

Utilizando la distributividad de $\wedge$ con respecto a $\vee$:

$$u \Leftrightarrow [\bar{p} \wedge (\bar{q} \vee q)] \vee [p \wedge (\bar{q} \vee q)].$$

Pero $\bar{q} \vee q \Leftrightarrow V$ (principio tercero excluído, teorema (1.6)), de donde:

$$u \Leftrightarrow [\bar{p} \wedge V] \vee [p \wedge V].$$

Es directo que $\bar{p} \wedge V \Leftrightarrow \bar{p}$ y, además, $p \wedge V \Leftrightarrow p$ (verifique), concluyendo $u \Leftrightarrow \bar{p} \vee p \Leftrightarrow V$ ■

Para terminar esta sección, señalemos que la lógica estará presente en todo el libro, ya sea a través de la definición de conceptos (por ejemplo, las operaciones de conjuntos) como también en las diversas demostraciones que presentaremos.

1.2 Conjuntos.

A menudo hemos coleccionado objetos: cuadros, mariposas, etc. En álgebra y en matemáticas para hablar de colecciones nos referimos a conjuntos. Un conjunto es una colección de objetos arbitrarios.

De una colección sólo podemos saber (por ejemplo, por inspección exhaustiva, aunque no siempre es posible) si un objeto está o no está en la colección. Formalmente diremos que el objeto *pertenece* o *no pertenece* al conjunto. Y nada más ... salvo quizás enumerar la colección ... lo cual suele ser difícil o ... en algunos casos y sentidos, imposible.

Representaremos un *conjunto* por las letras mayúsculas del abecedario:

$$A, B, C, ..., S, ..., Z.$$

Sus *elementos* por letras minúsculas

$$a, b, c, ..., z.$$

Si un elemento, (digamos x), está en el conjunto C notaremos:

$$x \in C$$

y diremos que *el elemento x pertenece al conjunto C.*

Si no está, notaremos:

$$x \notin C$$

y diremos que *x no pertenece a C.*

Hacer el inventario de un conjunto consiste en explicitar sus elementos. Por ejemplo, si el conjunto C está formado por los elementos a, b, c se escribirá:

$$C = \{a, b, c\}.$$

Como sólo nos interesa si un elemento está o no está en un conjunto dado, es natural que el orden en que inventariamos los elementos sea irrelevante:

$$\begin{aligned} C &= \{a, b, c\} = \{a, c, b\} = \{b, a, c\} \\ &= \{b, c, a\} = \{c, a, b\} = \{c, b, a\}. \end{aligned}$$

También, por el mismo argumento anterior, se tiene:

$$\begin{aligned} C &= \{a, b, c\} = \{a, a, a, b, b, c, c\} \\ &= \{c, a, a, b, b\} = ... = etc. \end{aligned}$$

¡Las repeticiones no interesan!

Como no nos preocupa ninguna eventual relación que pudiese existir entre los elementos de un conjunto, aparte de la pertenecencia, podemos decir que un conjunto es "amorfo".

Algunos conjuntos importantes son los siguientes:

- El conjunto de los enteros no-negativos o números *naturales*: $\mathbb{N} = \{0, 1, 2, 3, ...\}$
- El conjunto de los *enteros*, $\mathbb{Z} = \{... - 2, -1, 0, 1, 2, ...\}$
- El conjunto de los *racionales* o números que se escriben de la forma p/q, donde $p, q \in \mathbb{Z}, q \neq 0$. Este conjunto se nota Q.
- El conjunto de los *irracionales* o números que no se pueden escribir de la forma p/q (por ejemplo, $\sqrt{2}$ como veremos más adelante). Este conjunto se nota **I**.
- El conjunto de todos los números *reales*, $-1, 0, 3.14, \pi, \sqrt{2}, ...$ que notamos $\mathbb{R}$.

- El conjunto *vacío*, que notamos ϕ, que es el que no contiene ningún elemento o bien aquel para el cual la proposición $(x \notin \phi)$ es siempre verdadera y $(x \in \phi)$ es siempre falsa.
- El conjunto *universo*, U, que contiene todos los elementos de un cierto contexto o bien aquel para el cual la proposición $(x \in U)$ es siempre verdadera.
- Conjuntos *singleton*, que son aquellos que contienen un elemento. Por ejemplo $\{a\}, \{1\}, \{q\}$, etcétera.

De los conjuntos anteriores vemos que algunos (por ejemplo, $\mathbb{N}, \mathbb{Z}, \{a\}$) se definen explicitando o enumerando sus elementos, pero otros (como $\mathbb{R}$) no pueden definirse de esta manera. En el primer caso hablamos de una definición por *extensión* y en el segundo por *comprensión*. Tomemos por ejemplo el conjunto S, de todos los números reales inferiores o iguales a 3.5. La definición por comprensión es la única posible y está dada por:

$$S = \{x \in \mathbb{R} / x \leq 3.5\}.$$

En general un conjunto definido por comprensión, se caracteriza por una propiedad del mismo dada por una proposición $p(x)$:

$$S = \{x \in U / p(x)\}$$

que se lee *x pertenece a S si y sólo si la proposición $p(x)$ es verdadera.*

En el ejemplo anterior, $p(x)$ es la proposición $(x \leq 3.5)$ y se tiene:

$$x \in S \Longleftrightarrow p(x) \wedge (x \in \mathbb{R})$$

1.2.1 Igualdad entre conjuntos.

Diremos que dos conjuntos A y B son *iguales* si y sólo si contienen exactamente los mismos elementos:

$$(A = B) \Longleftrightarrow (x \in A \Longleftrightarrow x \in B) \tag{1.12}$$

En caso contrario, diremos que A es distinto de B y lo notaremos $A \neq B$. De la definición de igualdad es fácil verificar que:

$$A = A \text{ (reflexibidad)} \tag{1.13}$$

$$A = B \Longleftrightarrow B = A \text{ (simetría)} \tag{1.14}$$

$$(A = B) \wedge (B = C) \Longrightarrow A = C \quad \text{(transitividad)}. \tag{1.15}$$

Menos fácil, aunque intuitivamente directo es:

$$A \neq B \iff \text{Existe algún elemento } x \text{ tal que}$$

$$(x \in A \wedge x \notin B) \vee (x \notin A \wedge x \in B). \tag{1.16}$$

Demostremos esta última propiedad:

$$(A \neq B) \iff (\overline{A = B}) \iff \text{"La proposición } (A = B) \text{ es falsa"}$$

como

$$(A = B) \iff (x \in A \iff x \in B),$$

entonces

$$(A \neq B) \iff (\overline{A = B}) \iff \overline{(x \in A \iff x \in B)},$$

pero sabemos que:

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

es un teorema lógico o tautología (Teorema 1.11). Luego, definiendo las proposiciones:

$$p = (x \in A), \quad q = (x \in B),$$

se tiene

$$\bar{p} = (x \notin A), \quad \bar{q} = (x \notin B),$$

de donde:

$$(A \neq B) \iff \overline{(p \iff q)} \iff \overline{((\bar{p} \wedge \bar{q}) \vee (p \wedge q))}.$$

Por las leyes de De Morgan (teorema (1.17)):

$$\iff \overline{(\bar{p} \wedge \bar{q})} \wedge \overline{(p \wedge q)}$$

$$\iff (p \vee q) \wedge (\bar{p} \vee \bar{q}).$$

Por las leyes de distributividad:

$$\iff [(p \vee q) \wedge \bar{p}] \vee [(p \vee q) \wedge \bar{q}]$$

$$\iff [(p \wedge \bar{p}) \vee (q \wedge \bar{p})] \vee [(p \wedge \bar{q}) \vee (q \wedge \bar{q})],$$

pero, por el principio de contradicción (teorema (1.5)):

$$p \wedge \bar{p} \iff F \iff q \wedge \bar{q},$$

además, dada cualquier proposición r se tiene la tautología $r \vee F \iff r$, de donde:

$$\iff (q \wedge \bar{p}) \vee (p \wedge \bar{q}),$$

reemplazando $q, p, \bar{p}, \bar{q}$:

$$(A \neq B) \iff (x \in B \wedge x \notin A) \vee (x \in A \wedge x \notin B),$$

por conmutatividad de $\wedge$:

$(A \neq B) \iff$ Existe algún x tal que $(x \in A \wedge x \notin B) \vee (x \notin A \wedge x \in B)$ ■

Constatamos entonces que la demostración rigurosa (aunque ésta no lo es del todo por la frase "*existe algún x tal que*", que cayó un poco del cielo) es mucho más ardua que la intuición que podría tenerse sobre el problema.

1.2.2 Inclusión de conjuntos.

Dados los conjuntos

$$B = \{a, c, z, 1\}, \qquad C = \{a, c, z, b\}, \qquad A = \{a, z, 1\},$$

es trivial verificar que A es una subcolección de B : cada elemento de A está en B.

Además C, aunque contiene tres elementos comunes con B, no es una subcolección y finalmente los tres conjuntos son distintos.

En este contexto, diremos que un conjunto A está *contenido o incluido* en B o es un *subconjunto* de B, si cada elemento perteneciente al conjunto A también pertenece a B. En tal caso notaremos $A \subseteq B$. Formalmente:

$$A \subseteq B \iff (x \in A \Longrightarrow x \in B). \tag{1.17}$$

Por ejemplo:

$$\{0\} \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq Q \subseteq \mathbb{R}$$

$$\{0, 3.15\} \not\subseteq \mathbb{N} \qquad (\not\subseteq : \textit{no está contenido en}).$$

De la definición es fácil verificar que, dados dos conjuntos A, B arbitrarios:

$$A \subseteq A \tag{1.18}$$

$$\phi \subseteq A \tag{1.19}$$

$$(A \subseteq B) \wedge (B \subseteq A) \Longleftrightarrow A = B \tag{1.20}$$

$$(A \subseteq B) \wedge (B \subseteq C) \Longrightarrow A \subseteq C. \tag{1.21}$$

La propiedad (1.20) es importante ya que nos entrega un camino alternativo para verificar la igualdad entre dos conjuntos. Demostrémosla:

$$[(A \subseteq B) \wedge (B \subseteq A)] \Longleftrightarrow [(x \in A \Longrightarrow x \in B) \wedge (x \in B \Longrightarrow x \in A)],$$

denominando $p \Longleftrightarrow (x \in A)$, $q \Longleftrightarrow (x \in B)$:

$$[(A \subseteq B) \wedge (B \subseteq A)] \Longleftrightarrow [(p \Longrightarrow q) \wedge (q \Longrightarrow p)].$$

Finalmente, utilizando el teorema lógico (1.9) obtenemos (1.20):

$$[(A \subseteq B) \wedge (B \subseteq A)] \Longleftrightarrow (x \in A \Longleftrightarrow x \in B) \Longleftrightarrow A = B \quad \blacksquare$$

Dado un conjunto A, sabemos que $\phi \subseteq A \subseteq A$. En este contexto, ϕ, A se denominan los subconjuntos triviales de A. Un conjunto B estrictamente contenido en A, es decir que exista al menos un elemento de A que no pertenece a B, se dirá un *subconjunto propio*:

$$B \subset A \Longleftrightarrow (B \subseteq A) \wedge (B \neq A). \tag{1.22}$$

A partir de la noción de *inclusión* (1.17) y dado un conjunto A, definimos el conjunto de las *partes* de A, que notamos $\mathcal{P}(A)$, como el *conjunto de todos los subconjuntos* de A :

$$\mathcal{P}(A) = \{X / X \subseteq A\}. \tag{1.23}$$

Es importante notar que $\mathcal{P}(A)$ es un conjunto cuyos elementos son conjuntos: una colección de colecciones. Por ejemplo si $A = \{a, b, c\}$

$$\mathcal{P}(A) = \{\phi, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c, \}\}.$$

1.2.3. Diferencia y complemento.

Dado un problema específico de álgebra, usualmente es necesario definir el conjunto más grande que sirva de marco al problema. En tal sentido

notamos U como el conjunto *universo*, de manera que cualquier conjunto A que utilicemos esté contenido en U (ver también página 27). Si, por ejemplo, estamos trabajando con conjuntos de números enteros, $U = \mathbb{Z}$. Con conjuntos de letras, U será el abecedario, etcétera.

Otra relación natural entre conjuntos es la *diferencia*. Sean, por ejemplo, los conjuntos $A = \{a, b, c, d\}$, $B = \{a, b, e\}$. Si al conjunto A le "sacamos" los elementos comunes con B se obtiene el conjunto $\{c, d\}$. Si a B le "sacamos" los elementos comunes con A obtenemos el conjunto $\{e\}$. De manera formal, dados dos conjuntos A, B se define su *diferencia* como sigue:

$$A \setminus B = \{x \in U / x \in A \wedge x \notin B\}, \tag{1.24}$$

o bien

$$x \in A \setminus B \Longleftrightarrow (x \in A \wedge x \notin B).$$

Tomando un universo U, la diferencia de un conjunto con respecto a U se denomina *complemento*: Dado A, $U \setminus A$ se define como el *complemento* de A con respecto a U y se nota:

$$C_U(A) = U \setminus A. \tag{1.25}$$

Luego $C_U(A)$ contiene los elementos que pertenecen a U y que no pertenecen a A. Si convenimos que U es el universo suele notarse:

$$x \in C_U(A) \Longleftrightarrow x \notin A,$$

subentendiendo que los elementos $x \notin A$ son elementos de $U \setminus A$.

Por ejemplo: dado $U = \{a, b, ..., z\}$, $A = \{a, e, i, o, u\}$, $C_U(A)$ es el conjunto de letras consonantes. Dado $U = \mathbb{N}$, y el conjunto de números pares, $I\!P = \{x \in \mathbb{N} / x = 2n,\ n \in \mathbb{N}\}$:

$$C_U(I\!P) = \{x \in \mathbb{N} / x = 2n + 1,\ n \in \mathbb{N}\},$$

que es el conjunto de los números impares.

Dos propiedades de base de la operación complemento son:

$$C_U(U) = \phi, \quad C_U(\phi) = U \tag{1.26}$$

$$C_U((C_U(A)) = A. \tag{1.27}$$

Demostremos (1.27)

$$x \in C_U(C_U(A)) \Longleftrightarrow x \notin C_U(A) \Longleftrightarrow \overline{(x \in U \wedge x \notin A)}$$

$$\Longleftrightarrow ((x \notin U) \vee (x \in A)) \Longleftrightarrow x \in A.$$

Luego, de la definición (1.12), de igualdad de conjuntos, se obtiene la propiedad ■

1.2.4 Unión e intersección de conjuntos.

Entre conjuntos, tal como entre proposiciones, es posible definir dos operaciones, la *unión* y la *intersección* de conjuntos. Sean por ejemplo $A = \{a, b, c, d\}, B = \{a, b, y, z\}$.

Constatamos que $\{a, b\}$ es exactamente el conjunto de los elementos comunes entre A y B. Por otra parte $\{a, b, c, d, y, z\}$ es el conjunto que contiene los elementos de A y también los de B.

Formalmente, dados los conjuntos A, B definimos su *intersección* como el conjunto de los elementos comunes a A y B que notamos $A \cap B$:

$$A \cap B = \{x / x \in A \wedge x \in B\}, \tag{1.28}$$

o bien

$$x \in A \cap B \Longleftrightarrow (x \in A) \wedge (x \in B).$$

Diremos que dos conjuntos son *disjuntos* si y sólo si su intersección es el conjunto vacío.

Definimos la *unión* de A y B, como el conjunto que contiene los elementos de A y de B, que notamos $A \cup B$:

$$A \cup B = \{x / x \in A \vee x \in B\}, \tag{2.29}$$

o bien

$$x \in A \cup B \Longleftrightarrow (x \in A) \vee (x \in B).$$

A modo de ejemplo, dados los conjuntos

$$A = \{1, x, z\}, B = \{2, x, y\}, C = \{1, a, z\},$$

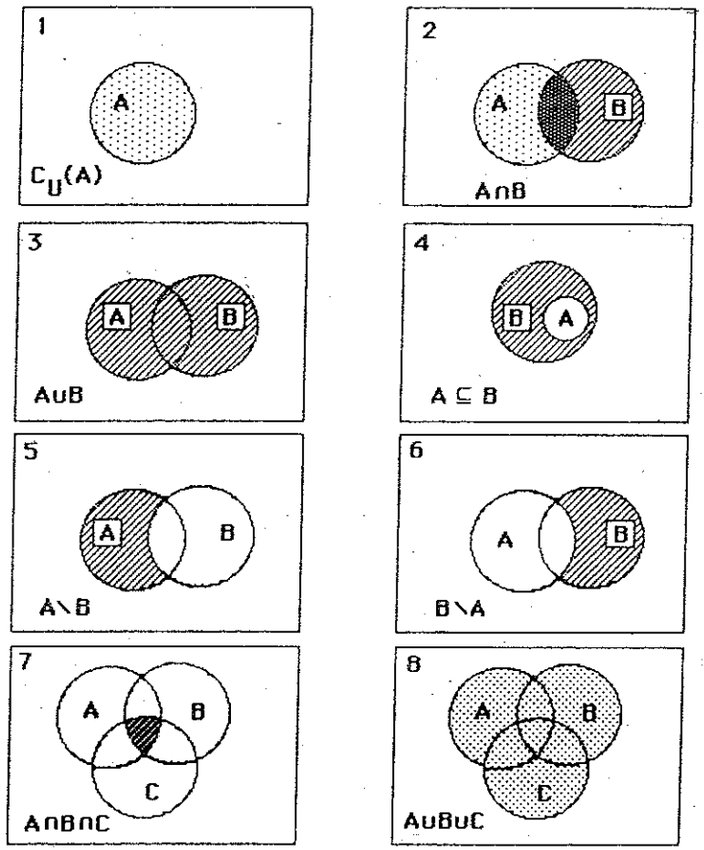
se tiene:

$$A \cap B = \{x\}, A \cap C = \{1, z\}, B \cap C = \phi, (A \cap B) \cap C = \phi$$
$$A \cup B = \{1, 2, x, y, z\}; A \cup C = \{1, a, x, z\}$$
$$B \cup C = \{1, 2, a, x, y, z\}, (A \cup B) \cup C = \{1, 2, a, x, y, z\}$$

$$(A \cap B) \cup C = \{1, a, x, z\}, (A \cap C) \cup B = \{1, 2, x, y, z\}$$
$$(A \cup B) \cap C = \{1, z\}, (A \cup C) \cap B = \{x\}$$
$$(B \cup C) \cap A = A = \{1, x, z\}$$
$$(A \cup B) \cap (A \cup C) = \{1, x, z\}.$$

1.2.5 Diagramas de Venn.

Dado un conjunto universo U, representado por un rectángulo, podemos visualizar un conjunto $A \subseteq U$ como una circunsferencia o elipse contenida en el rectángulo. Mediante esta iconografía podemos representar las operaciones entre conjuntos, en la medida que no se involucren demasiados conjuntos. Obviamente el dibujo sólo constituye una ayuda gráfica y en ningún caso una demostración de las propiedades que en él se observan. Algunos ejemplos de diagramas de Venn son los siguientes:



1.2.6 Algebra de conjuntos.

Algunas propiedades de las operaciones complemento, intersección y unión son las siguientes:

Conmutatividad.

$$A \cup B = B \cup A, \quad A \cap B = B \cap A. \tag{1.30}$$

Asociatividad.

$$\begin{aligned} A \cup (B \cup C) &= (A \cup B) \cup C \\ A \cap (B \cap C) &= (A \cap B) \cap C. \end{aligned} \tag{1.31}$$

Distributividad.

$$\begin{aligned} A \cup (B \cap C) &= (A \cup B) \cap (A \cup C) \\ A \cap (B \cup C) &= (A \cap B) \cup (A \cap C). \end{aligned} \tag{1.32}$$

Leyes de Complementación de De Morgan:

$$\begin{aligned} C_U(A \cup B) &= C_U(A) \cap C_U(B) \\ C_U(A \cap B) &= C_U(A) \cup C_U(B). \end{aligned} \tag{1.33}$$

$$\begin{aligned} A \subseteq A \cup B \quad &\wedge \quad B \subseteq A \cup B \\ A \supseteq A \cap B \quad &\wedge \quad B \supseteq A \cap B. \end{aligned} \tag{1.34}$$

Demostremos la propiedad (1.33): $C_U(A \cup B) = C_U(A) \cap C_U(B)$.

$$x \in C_U(A \cup B) \Longleftrightarrow x \notin A \cup B \Longleftrightarrow \overline{(x \in (A \cup B))},$$

de la definición de $A \cup B$ (ver (1.29)):

$$\Longleftrightarrow \overline{(x \in A \vee x \in B)},$$

de De Morgan para proposiciones lógicas (teorema lógico (1.7)):

$$\Longleftrightarrow \overline{(x \in A)} \wedge \overline{(x \in B)} \Longleftrightarrow (x \notin A) \wedge (x \notin B)$$

$$\Longleftrightarrow (x \in C_U(A)) \wedge (x \in C_U(B)),$$

de la definición de intersección, (1.28):

$$\Longleftrightarrow x \in C_U(A) \cap C_U(B) \quad \blacksquare$$

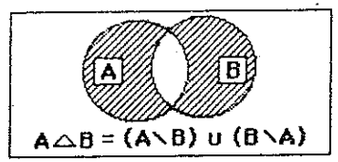
1.2.7 Diferencia simétrica.

Otra operación útil entre conjuntos es la siguiente: dados dos conjuntos A, B definimos su *diferencia simétrica*, que notamos $A \triangle B$, como el conjunto de los elementos que pertenecen a $A \setminus B$ ó $B \setminus A$:

$$A \triangle B = (A \setminus B) \cup (B \setminus A), \tag{1.35}$$

o bien

$$(x \in A \triangle B) \Leftrightarrow [(x \in A \setminus B) \vee (x \in B \setminus A)].$$



Del diagrama de Venn constatamos que:

$$A \triangle B = (A \cup B) \setminus (A \cap B), \tag{1.36}$$

pero esto no constituye una demostración. Verifiquemos rigurosamente esta identidad:

$x \in (A \cup B) \setminus (A \cap B) \Leftrightarrow (x \in A \cup B) \wedge (x \notin A \cap B)$

$\Leftrightarrow (x \in A \vee x \in B) \wedge (x \notin A \cap B)$,

distribuyendo

$\Leftrightarrow (x \in A \wedge x \notin A \cap B) \vee (x \in B \wedge x \notin A \cap B)$

$\Leftrightarrow [x \in A \wedge (x \notin A \vee x \notin B)] \vee [x \in B \wedge (x \notin A \vee x \notin B)]$,

distribuyendo

$\Leftrightarrow [(x \in A \wedge x \notin A) \vee (x \in A \wedge x \notin B)] \vee [(x \in B \wedge x \notin A) \vee (x \in B \wedge x \notin B)]$,

por el principio de contradicción (Teorema lógico (1.5)

$\Leftrightarrow [F \vee (x \in A \wedge x \notin B)] \vee [(x \in B \wedge x \notin A) \vee F]$

pero, para cualquier proposición $p, F \vee p \Leftrightarrow p$, luego,

$\Leftrightarrow (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)$

$\Leftrightarrow (x \in A \setminus B) \vee (x \in B \setminus A) \Leftrightarrow x \in (A \setminus B) \cup (B \setminus A) \Leftrightarrow x \in A \triangle B$ $\blacksquare$

Otras propiedades de la diferencia simétrica aparecen en los ejercicios del capítulo.

1.2.8. Conjuntos finitos e infinitos.

El conjunto $A = \{a, b, c, d\}$ tiene 4 elementos y es *finito*. $\mathbb{N} = \{0, 1, 2, 3, ...\}$ es un conjunto ***infinito***. El conjunto de los números reales, $\mathbb{R}$, también es infinito y no es posible describirlo por extensión.

Dado un conjunto finito (número finito de elementos) A, definimos el *cardinal* como el número de elementos de A. Esto lo notamos:

$$|A| = \text{ número de elementos de } A. \tag{1.37}$$

En algunos textos también se utiliza la notación $card(A)$.

Por ejemplo, sea $A = \{a, b, c\}$, luego $|A| = 3$. Además, dado que el conjunto de las partes es el siguiente:

$$\mathcal{P}(A) = \{\phi, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}.$$

$|\mathcal{P}(A)| = 8 = 2^3 = 2^{|A|}$. Demostraremos más adelante que esta propiedad se verifica para todo conjunto finito. También es directo de la definición que $|\phi| = 0$.

Una propiedad no trivial es la siguiente:

Dados dos conjuntos finitos A y B:

$$|A \cup B| = |A| + |B| - |A \cap B|. \tag{1.38}$$

Basta observar que en $|A| + |B|$ se consideran dos veces el número de elementos de $A \cap B$.

Una demostración formal, que utiliza subíndices para distinguir los elementos de los conjuntos A, B y $A \cap B$, es la siguiente:

Sea $A \cap B = \{c_1, ..., c_p\}$, luego los elementos comunes de A y B son $c_1, ..., c_p$. Supongamos que, aparte de estos elementos, A y B poseen otros:

$$A = \{a_1, ..., a_m, c_1, ..., c_p\}$$
$$B = \{b_1, ..., b_n, c_1, ..., c_p\},$$

donde:

$$(a_i \in A) \wedge (a_i \notin B) \qquad 1 \leq i \leq m$$
$$(b_j \in B) \wedge (b_j \notin A) \qquad 1 \leq j \leq n.$$

Tenemos entonces:

$$A \cup B = \{a_1, ..., a_m, b_1, ...b_n, c_1, ..., c_p\},$$

de donde

$$\begin{aligned} |A \cup B| &= m + n + p \\ &= (m + p) + (n + p) - 2p + p = (m + p) + (n + p) - p \\ &= |A| + |B| - |A \cap B| \quad \blacksquare \end{aligned}$$

Observemos que si $A \cap B = \phi$, entonces $|A \cup B| = |A| + |B|$.

Para el caso infinito la noción de cardinalidad se complica ya que hay "infinitos" de distinta naturaleza. Es claro que $\mathbb{R}$ tiene *más* elementos que $\mathbb{N}$, pero no es nada claro que, en algún sentido, los elementos de $\mathbb{N}$ y $\mathbb{Z}$ pueden asociarse uno a uno. Situaciones como ésta nos llevarán a exponer los rudimentos de una teoría que nos permita entender distintos tipos de infinito. Trataremos esto en el tema *Cantor, cardinalidad y otros resbaladeros* del capítulo IV.

1.3 Cuantificadores lógicos.

En alguna de las demostraciones anteriores aparecen frases del tipo "existe algún x en A tal que ..." o bien "para todo x en A...". Para formalizar esto notaremos:

$$\text{(Existe algún elemento } x \text{ en el conjunto } A) \Longleftrightarrow \exists x \in A$$

$$\text{(Para todo } x \text{ en el conjunto } A) \iff \forall x \in A.$$

En el primer caso, la existencia de algún elemento x en A no implica que éste sea único. En algunas situaciones es conveniente resaltar su unicidad:

$$\text{"existe un único elemento } x \text{ en } A\text{"} \iff \exists! x \in A.$$

Tomemos una proposición $p(x)$ donde x es elemento de un conjunto universo U. Diremos que U es el *dominio* de esta proposición. Claramente $p(x)$ puede ser verdadera o falsa, de acuerdo al elemento particular de U en que sea evaluada. Por ejemplo, dada la proposición $p(x) = (x - 1 = 0)$ en $\mathbb{N}$, $p(1)$ es verdadera y $p(0)$ es falsa.

Formalmente, definimos los cuantificadores lógicos, sobre proposiciones, como sigue: dada una proposición p, con dominio U, le asociamos el subconjunto de U donde p es verdadera:

$$A = \{x \in U / p(x)\}$$

Se definen entonces las proposiciones:

$$(\forall x \in U)p(x) \Leftrightarrow (A = U) \tag{1.39}$$
$$(\exists x \in U)p(x) \Leftrightarrow (A \neq \phi) \tag{1.40}$$
$$(\exists! x \in U)p(x) \Leftrightarrow (A = \{u\})(u \in U). \tag{1.41}$$

La equivalencia (1.39) dice que la proposición $(\forall x \in U)p(x)$ es verdadera si y sólo si el conjunto de valores donde p es verdadera coincide con el dominio, U. Análogamente, la proposición $(\exists x \in U)p(x)$ es verdadera si y sólo si el conjunto de valores donde p es verdadera es no vacío. Obviamente, las proposiciones (1.39), (1.40),(1.41) pueden ser verdaderas o falsas, de acuerdo a las características del conjunto A.

Consideremos, como ejemplo, el universo $U = \mathbb{N}$ y la proposición $p(n) \Leftrightarrow (n$ es par). Así, $A = \{p \in \mathbb{N}/p = 2n, n \in \mathbb{N}\}$, es el conjunto de los números pares. Luego, de acuerdo a (1.39), (1.40) y (1.41):

$$(\forall n \in \mathbb{N})p(n) \Leftrightarrow F$$
$$(\exists n \in \mathbb{N})p(n) \Leftrightarrow V$$
$$(\exists! n \in \mathbb{N})p(n) \Leftrightarrow F.$$

Otros ejemplos son los siguientes:

$(\exists x \in \mathbb{N})(x$ es divisible por 2) es verdadera.
$(\forall x \in \mathbb{N})(x$ es divisible por 2) es falsa.
$(\forall x \in \mathbb{R})(x^2 + x = 0)$ es falsa.
$(\exists x \in \mathbb{R})(x^2 + x = 0)$ es verdadera.
$(\exists! x \in \mathbb{R})(x^2 + x = 0)$ es falsa.
$(\exists x \in \mathbb{Z})(x^2 + x^3 = 0)$ es verdadera.

1.3.1 Negación de cuantificadores.

Dada una proposición p con dominio U, las negaciones de $(\forall x \in U)p(x)$ y $(\exists x \in U)p(x)$ son las siguientes:

$$\overline{[(\forall x \in U)p(x)]} \Longleftrightarrow (\exists x \in U)\bar{p}(x) \tag{1.42}$$

$$\overline{[(\exists x \in U)p(x)]} \Longleftrightarrow (\forall x \in U)\bar{p}(x). \tag{1.43}$$

Demostremos (1.42).

De la definición (1.39):

$$(\forall x \in U)p(x) \Longleftrightarrow (A = U),$$

luego

$$(\overline{(\forall x \in U)p(x)}) \Longleftrightarrow \overline{(A = U)} \Longleftrightarrow (A \neq U),$$

de la definición de igualdad entre conjuntos (identidad (1.12)) y como $A \subseteq U$:

$$\Longleftrightarrow (\exists x)(x \in U \wedge x \notin A)$$
$$\Longleftrightarrow (\exists x \notin A)$$
$$\Longleftrightarrow (\exists x \in U)\bar{p}(x) \quad \blacksquare$$

A modo de ejemplo, neguemos la proposición:

$$v(\varepsilon, \delta) \Leftrightarrow (\forall \varepsilon > 0)(\exists \delta > 0)(|x - x_0| < \delta \Rightarrow |y - y_0| < \varepsilon).$$

Para ello, consideremos la proposición

$$p(\varepsilon) \Leftrightarrow (\exists \delta > 0)(|x - x_0| < \delta \Rightarrow |y - y_0| < \varepsilon).$$

Notemos, además, que $(\forall \varepsilon > 0) \Leftrightarrow (\forall \varepsilon \in \mathbb{R}_+)$, donde $\mathbb{R}_+$ es el conjunto de números reales positivos. Tenemos entonces directamente de (1.42):

$$\bar{v}(\varepsilon, \delta) \Leftrightarrow \overline{(\forall \varepsilon > 0)p(\varepsilon)} \Leftrightarrow \overline{(\forall \varepsilon \in \mathbb{R}_+)p(\varepsilon)} \Leftrightarrow (\exists \varepsilon \in \mathbb{R}_+)\bar{p}(\varepsilon). \tag{1.44}$$

Desarrollemos ahora $\bar{p}(\varepsilon)$:

$$\bar{p}(\varepsilon) \Leftrightarrow \overline{(\exists \delta > 0)(|x - x_0| < \delta \Rightarrow |y - y_0| < \varepsilon)}$$

$$\Leftrightarrow \overline{(\exists \delta \in \mathbb{R}_+)(|x - x_0| < \delta \Rightarrow |y - y_0| < \varepsilon)}$$

$$\Leftrightarrow (\forall \delta \in \mathbb{R}_+)\overline{(|x - x_0| < \delta \Rightarrow |y - y_0| < \varepsilon)}. \tag{1.45}$$

Para determinar la negación de $(|x - x_0| < \delta \Rightarrow |y - y_0| < \varepsilon)$, definamos las proposiciones:

$$q(\delta) \Leftrightarrow (|x - x_0| < \delta)$$
$$r(\varepsilon) \Leftrightarrow (|y - y_0| < \varepsilon).$$

Se tiene entonces:

$$(q(\delta) \Rightarrow r(\varepsilon)) \Leftrightarrow [(|x - x_0| < \delta) \Rightarrow (|y - y_0| < \varepsilon)].$$

Pero, utilizando el teorema lógico (1.10), escribimos la implicación:

$$(q(\delta) \Rightarrow r(\varepsilon)) \Leftrightarrow (\bar{q}(\delta) \vee r(\varepsilon)).$$

Luego:

$$\overline{(|x - x_0| < \delta \Rightarrow |y - y_0| < \varepsilon)} \Leftrightarrow \overline{(\bar{q}(\delta) \vee r(\varepsilon))},$$

del teorema lógico (1.7), de De Morgan:

$$\Leftrightarrow (q(\delta) \wedge \bar{r}(\varepsilon)).$$

Además, $\bar{r}(\varepsilon) \Leftrightarrow \overline{(|y - y_0| < \varepsilon)} \Leftrightarrow (|y - y_0| \geq \varepsilon)$, obteniendo

$$\overline{(|x - x_0| < \delta \Rightarrow |y - y_0| < \varepsilon)} \Leftrightarrow [(|x - x_0| < \delta) \wedge (|y - y_0| \geq \varepsilon)].$$

Reemplazando en (1.45):

$$\bar{p}(\varepsilon) \Leftrightarrow (\forall \delta \in \mathbb{R}_+)[(|x - x_0| < \delta) \wedge (|y - y_0| \geq \varepsilon)].$$

Reemplazando en (1.44):

$$\begin{aligned} \bar{v}(\varepsilon, \delta) &\Leftrightarrow (\exists \varepsilon \in \mathbb{R}_+)(\forall \delta \in \mathbb{R}_+)[(|x - x_0| < \delta) \wedge (|y - y_0| \geq \varepsilon)] \\ &\Leftrightarrow (\exists \varepsilon > 0)(\forall \delta > 0)[(|x - x_0| < \delta) \wedge (|y - y_0| \geq \varepsilon)], \end{aligned}$$

que corresponde a la negación de $v(\varepsilon, \delta)$ ■

1.4 Indices, familias de conjuntos y particiones.

Supongamos una colección de conjuntos $A_1, A_2, ..., A_n$. Esta colección la podemos agrupar en otro conjunto, denominado *familia de conjuntos*, $\{A_1, A_2, ..., A_n\}$ o simplemente $\{A_i\}_{i=1}^n$ o bien, $\{A_i\}_{i \in I}$, donde $I = \{1, 2, ..., n\}$ es un conjunto llamado de *índices*.

También podría tratarse de una familia infinita; por ejemplo si el conjunto de índices es:

$$I = I\!P = \{0, 2, 4, 8, ...\}, \quad I = I\!N, \text{ etcétera,}$$

en ambos casos notamos la familia $\{A_i\}_{i \in I}$.

Por ejemplo, $\{A_i\}_{i \in I\!P} = \{A_0, A_2, .., A_{2n}, ..\}, \{A_i\}_{i \in I\!N} = \{A_0, A_1, ..., A_n, ..\}$.

Dada una familia de conjuntos, $\{A_i\}_{i \in I}$, definimos su *unión* e *intersección* de la manera siguiente:

$$x \in \bigcup_{i \in I} A_i \Longleftrightarrow (\exists i \in I) \quad (x \in A_i) \tag{1.46}$$

$$x \in \bigcap_{i \in I} A_i \Longleftrightarrow (\forall i \in I) \quad (x \in A_i). \tag{1.47}$$

Dado un conjunto A, diremos que la familia $\{A_i\}_{i \in I}$ es una *partición* de A si y sólo si verifica:

$$(A_i \neq \phi)(\forall i \in I) \tag{1.48}$$

$$A = \bigcup_{i \in I} A_i \tag{1.49}$$

$$(\forall i, j \in I) \quad (i \neq j \Longrightarrow A_i \cap A_j = \phi). \tag{1.50}$$

Por ejemplo, si $A = I\!N$, una partición estaría formada por los conjuntos de números pares e impares: $A_1 = \{0, 2, 4, ...,\}$ y $A_2 = \{1, 3, 5, ...\}$.

Para familiarizarnos con "familias" (¡valga la redundancia!), consideremos $\mathcal{C} = \{A_i\}_{i \in I\!N^*}$, $(I\!N^* = I\!N \setminus \{0\})$ tal que $U = \bigcup_{i \in I\!N^*} A_i$ y $(A_i \neq \phi)(\forall i \in I\!N^*)$. Es decir, la familia $\mathcal{C}$ cubre el conjunto U, pero no es necesariamente una partición. Sin embargo, podemos construir una partición de U, a partir de $\mathcal{C}$, utilizando el procedimiento siguiente:

Construyamos la familia $\mathcal{C}' = \{B_i\}_{i \in I\!N^*}$, definida como sigue:

$$\begin{aligned} B_1 &= A_1 \\ B_2 &= A_2 \setminus A_1 \\ B_3 &= A_3 \setminus (A_1 \cup A_2)... \end{aligned}$$

En general:

$$B_n = A_n \setminus \bigcup_{i=1}^{n-1} A_i, \; n \geq 2.$$

Intuitivamente, al construir B_n le "quitamos" al conjunto A_n todos los elementos que han aparecido previamente.

Demostremos que la nueva familia, $\mathcal{C}''$, compuesta por los conjuntos no vacíos de C', es una partición de U. Antes de esto, veamos un ejemplo:

Supongamos que se tienen siete conjuntos $\{A_i\}_{i=1}^{7}$:

$A_1=\{1,4,6,7,10,12\}$, $A_2=\{1,2,5,6,\}$, $A_3=\{2,4,5,7,10\}$, $A_4=\{1,3,10\}$, $A_5=\{2,3,4,9,10\}, A_6=\{4,5,6,7,8,9,11,12\}, A_7=\{1,3,5,7,10,11,12\}$,

contenidos en un universo $U=\{i\}_{i=1}^{12}$. Luego,

$$B_1 = A_1 = \{1,4,6,7,10,12\}$$
$$B_2 = A_2 \setminus A_1 = \{2,5\}$$
$$B_3 = A_3 \setminus (A_1 \cup A_2) = \phi$$
$$B_4 = \{3\}, B_5 = \{9\}, B_6 = \{8,11\}, B_k = \phi \quad \forall k \geq 7.$$

La partición del conjunto U es $\mathcal{C}'' = \{B_1, B_2, B_4, B_5, B_6\}$.

Desarrollemos ahora una prueba formal de la propiedad. Sin pérdida de generalidad supongamos que $\mathcal{C}'' = \{B_i\}_{i\in I}, I \subseteq \mathbb{N}^*$, es la familia de conjuntos no vacíos. Se debe demostrar que estos conjuntos son dos a dos disjuntos y que su unión corresponde al conjunto U.

Verifiquemos primero que los conjuntos son dos a dos disjuntos. Tomemos dos índices $n, m \in I^*, n > m$. De la definición:

$$x \in B_n \Leftrightarrow (x \in A_n) \wedge (x \notin \bigcup_{i=1}^{n-1} A_i),$$

como $n > m$, se tiene $B_m \subseteq A_m \subseteq \bigcup_{i=1}^{n-1} A_i$. Así, $x \notin B_m$ y entonces $x \notin B_n \cap B_m$.

De donde es directo concluir:

$$B_n \cap B_m = \phi \quad \forall n, m \in I, n \neq m.$$

Veamos, finalmente, qué sucede con la unión:

$$x \in \bigcup_{i\in I} B_i \Leftrightarrow (\exists n \in I, x \in B_n)$$
$$\Leftrightarrow (\exists n \in I, x \in A_n \setminus \bigcup_{j=1}^{n-1} A_j)$$
$$\Rightarrow (\exists n \in I, x \in A_n) \Leftrightarrow x \in \bigcup_{i\in I} A_i.$$

Luego, $\bigcup_{i\in I} B_i \subseteq \bigcup_{i\in\mathbb{N}^*} A_i = U$.

En el otro sentido, $x \in \bigcup_{i\in\mathbb{N}^*} A_i \Leftrightarrow \exists i \in \mathbb{N}^*, x \in A_i$. Sea n el número natural más pequeño tal que $x \in A_n$. Es decir, $\forall j < n, x \notin A_j$. Luego:

$$(x \in A_n) \wedge (x \notin A_j) \quad (\forall j \leq n-1)$$
$$\Leftrightarrow x \in A_n \setminus \bigcup_{j=1}^{n-1} A_j = B_n$$
$$\Rightarrow x \in \bigcup_{i\in I} B_i$$

De donde, $\bigcup_{i\in I} B_i = \bigcup_{i\in\mathbb{N}^*} A_i = U$.

Hemos demostrado entonces que la familia $\{B_i\}_{i\in I^*}$ es una partición del conjunto U ■

Ejercicios.

Algebra proposicional.

1. Demuestre las tautologías (1.1) - (1.10), dadas en el capítulo, mediante tablas de verdad.
2. Demuestre las tautologías o teoremas lógicos:
   (a) $p \vee p \iff p$; $\quad p \wedge p \iff p$.
   (b) $p \wedge V \iff p$.
   (c) $p \vee V \iff V$.
   (d) $p \Longrightarrow (p \vee q)$.
   (e) $(p \wedge q) \Longrightarrow p; (p \wedge q) \Longrightarrow q$.
   (f) $(p \iff q) \wedge (q \iff r) \Longrightarrow (p \iff r)$.
   (g) $(p \wedge (p \Longrightarrow q)) \Longrightarrow q$.
   (h) $(\bar{p} \Longrightarrow p) \Longrightarrow p$.
   (i) $(p \wedge \bar{q} \Longrightarrow q) \Longrightarrow (p \Longrightarrow q)$.
   (j) $(p \wedge q) \Rightarrow [(p \vee q) \Leftrightarrow (p \Leftrightarrow q)]$.
3. Demuestre, sin utilizar tablas de verdad (mediante reemplazos):
   (a) $\overline{(p \iff q)} \iff (p \iff \bar{q})$.
   (b) $\overline{(p \wedge \bar{q}) \vee (\bar{p} \wedge q)} \iff (p \iff q)$.
4. Dé una expresión lógica que sólo contenga a los conectivos $-, \wedge, \vee$ de las expresiones:
   (a) $[(p \wedge q) \Rightarrow (p \vee q)] \Leftrightarrow (p \Leftrightarrow q)$.
   (b) $(\bar{p} \iff q) \Longrightarrow (p \wedge q)$.
   (c) $(p \iff q \iff r)$.
   (d) $((p \Longrightarrow q) \wedge (q \Longrightarrow s)) \Longrightarrow (p \Longrightarrow s)$.
5. Determine todas las proposiciones lógicas simples que pueden formarse con p y q (todas las tablas de verdad y sus expresiones lógicas).
6. Discuta si, para cualquier valor de verdad de p, q y r, son siempre verdaderas las siguientes proposiciones:
   (a) $\overline{(p \Leftrightarrow q)} \Leftrightarrow (\bar{p} \Leftrightarrow \bar{q})$.
   (b) $[(p \wedge q) \Rightarrow (p \vee q)] \Leftrightarrow (p \Leftrightarrow q)$.
7. Niegue y simplifique: (es decir exprese la proposición de la manera más simple posible).
   (a) $p \wedge (q \vee r) \wedge (\bar{p} \vee \bar{q} \vee r)$.
   (b) $p \wedge q \Longrightarrow r$.
   (c) $p \Longrightarrow \bar{q} \wedge r$.
8. Se define la operación *"o" exclusivo* como: $(p \underline{\vee} q) \Leftrightarrow (p \vee q) \wedge \overline{(p \wedge q)}$
   (a) Encuentre la tabla de verdad del operador $\underline{\vee}$.
   Pruebe las tautologías:

   (b) $[p \wedge (q \underline{\vee} r)] \Leftrightarrow [(p \wedge q) \underline{\vee} (p \wedge r)]$, (o sea $\wedge$ distribuye cada una a $\underline{\vee}$).
   (c) $\overline{(p \underline{\vee} q)} \Leftrightarrow (p \Leftrightarrow q)$, (o sea, "dos proposiciones equivalentes no pueden ser excluyentes").
9. Dadas las tablas siguientes:

p	q	r	red
V	V	V	F
V	V	F	F
V	F	V	F
V	F	F	V
F	V	V	V
F	V	F	V
F	F	V	F
F	F	F	V

p	q	r	luz
V	V	V	V
V	V	F	V
V	F	V	F
V	F	F	V
F	V	V	F
F	V	F	F
F	F	V	F
F	F	F	V

   Encuentre las expresiones más simples para las proposiciones *red* y *luz*.
10. Resuelva este problema y construya otros análogos:
    Hay dos puertas, una conduce al cielo, la otra al averno. Hay dos guardias que sólo responden "verdadero" o "falso" a las preguntas de las almas que por allí transitan.
    Además uno de los guardias siempre dice la verdad y el otro siempre miente.
    Determine una única pregunta tal que, independientemente del guardia al cual se interrogue, permita tomar el camino al cielo.
    Indicación: Formalice el problema en términos de proposiciones lógicas.

Conjuntos.

11. Demuestre todas las propiedades enunciadas en el texto.
12. Demuestre $C_U(A) = \phi \iff A = U$. $C_U(A) = U \iff A = \phi$.
13. Demuestre:
    (a) $((A \subseteq C) \wedge (B \subseteq C)) \Longrightarrow (A \cup B) \subseteq C$.
    (b) $((C \subseteq A) \wedge (C \subseteq B)) \Longrightarrow C \subseteq A \cap B$.
    De (a) y (b) concluya que:
    (c) La unión entre A y B es el conjunto más pequeño (según la inclusión) que contiene A y B.
    (d) La intersección entre A y B es el mayor conjunto común (según la inclusión) que está contenido tanto en A como B.
14. (a) Demuestre que $[(A \cup X = A \cup Y) \wedge (A \cap X = A \cap Y)] \Leftrightarrow X = Y$.
    (b) Demuestre:
    $X \subseteq Y \Leftrightarrow A \cap [X \cup (B \setminus (A \setminus X))] \subseteq (A \cap Y) \cup [(A \cap B) \setminus (A \setminus Y)]$.
15. Demuestre que $\{A \setminus (B \cup C), B, C \setminus B\}$ es una partición de $E = A \cup B \cup C$.

16. Demuestre:
    (a) $(A \setminus B) \setminus C = A \setminus (B \cup C)$.
    (b) $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$.
    (c) $A \cup (B \setminus C) = (A \cup B) \setminus (C \setminus A)$.
    (d) $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$.
17. Demuestre que si A, B, C son conjuntos de un universo U, se cumple que:
    $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$.
18. Sean A, B conjuntos arbitrarios. Demuestre:
    (a) $A \triangle B = B \triangle A$.
    (b) $A \triangle (B \triangle C) = (A \triangle B) \triangle C$.
    (c) $A \triangle \phi = A$.
    (d) $A \triangle A = \phi$.
    (e) $A \triangle B = C \iff A \triangle C = B$.
19. Demuestre
    (a) $A \subseteq B \Longrightarrow \mathcal{P}(A) \subseteq \mathcal{P}(B)$.
    (b) $\mathcal{P}(A \cup B) \supseteq \mathcal{P}(A) \cup \mathcal{P}(B)$ (¿es verdad la inclusión inversa?).
    (c) $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.
    (d) $\mathcal{P}(A) = \mathcal{P}(B) \Longrightarrow A = B$.
20. Sea A en un universo U.
    (a) Defina adecuadamente $C[\mathcal{P}(A)]$.
    (b) Encuentre una relación (inclusión, igualdad, etc.) entre $\mathcal{P}(C_U(A))$ y $C[\mathcal{P}(A)]$.
21. ¿Qué sucede si en lugar de representar conjuntos mediante círculos (en los diagramas de Venn) se representan con cuadrados?, ¿o triángulos? Discuta.

Cuantificadores Lógicos.

22. Determine si son verdaderas o falsas las proposiciones:
    (a) $(\exists x \in \mathbb{R}), \quad (x^3 = 1)$.
    (b) $(\forall x \in \mathbb{R}), \quad (x^2 = 0)$.
    (c) $(\exists! x \in \mathbb{R}), \quad (x - 1 = 0)$.
23. Discuta los valores de verdad de:
    (a) $(\forall \alpha \in \{a, b, c, ...x, y, z\})(\alpha = x)$.
    (b) $(\forall \alpha \in \{a, b, c, ..., x, y, z\})(\alpha \neq x)$.
    (c) $(\exists \alpha \in \{a, b, c, ..., x, y, z\})(\alpha \neq x)$.
    (d) $(\exists \alpha \in \{a, b, c, ..., x, y, z, \})(\alpha = x)$.
    (e) $(\exists \alpha \in \{a, b, ..., x, y, z\})(\alpha = u)$.
    (f) $(\exists! \alpha \in \{a, b, ..., x, y, z\})(\alpha = a)$.

24. Niegue las proposiciones
    (a) $(\forall a \in \mathbb{N})(\forall b \in \mathbb{N})(\exists p \in \mathbb{Z})(\exists y \in \mathbb{Z})(ax + by = 1)$.
    (b) $(\forall \beta > 0)(\exists m \in \mathbb{R})[(\forall x < \beta,\ m > x) \wedge (\forall x > \beta,\ m \leq x)]$.
25. (a) ¿Cuál es la negación de $(\exists! x \in U)p(x)$?
    (b) Niegue la proposición: $(\forall y \in \mathbb{R}^+)(\exists! x \in \mathbb{R}^+)(x^2 = y)$.

Familias de Conjuntos.

26. Sea la familia $\{A_n\}_{n \in \mathbb{N}^*}; \mathbb{N}^* = \mathbb{N} \setminus \{0\}; \quad A_n = [-2n, 3n]$, intervalo de números reales. Determine $\bigcup_{i \in \mathbb{N}^*} A_n, \quad \bigcap_{i \in \mathbb{N}^*} A_n$.
27. Dada la familia $\{A_i\}_{i \in I}$; pruebe que, dado un conjunto A:
    $A \cap (\bigcup_{i \in I} A_i) = \bigcup_{i \in I} (A \cap A_i)$
    $A \cup (\bigcap_{i \in I} A_i) = \bigcap_{i \in I} (A \cup A_i)$.
28. Enuncie y demuestre las Leyes de De Morgan para el complemento en el caso de unión e intersección de familias arbitrarias de conjuntos.
* 29. Sea la familia de índices $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$ y la familia $F = \{A_k\}_{k \in \mathbb{N}^*}$.

$$\text{Se definen } LI(F) = \bigcup_{n \in \mathbb{N}^*} \left(\bigcap_{k \geq n} A_k \right) \text{ y } LS(F) = \bigcap_{n \in \mathbb{N}^*} \left(\bigcup_{k \geq n} A_k \right)$$

    (a) Demuestre que $LI(F) \subseteq LS(F)$.
    Si se tiene que $LI(F) = LS(F)$, se define

$$LI(F) = LS(F) = L(F).$$

    (b) Demuestre que si $A_k \subseteq A_{k+1} \quad \forall k \in \mathbb{N}^*$, entonces existe $L(F)$ y además:

$$L(F) = \bigcup_{n \in \mathbb{N}^*} A_n.$$

    (c) Demuestre que si $A_k \supseteq A_{k+1}\ \forall k \in \mathbb{N}^*$, entonces existe $L(F)$ y $L(F) = \bigcap_{n \in \mathbb{N}^*} A_n$.

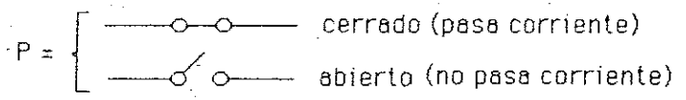
TEMAS CAPITULO I

1. Circuitos lógicos.

2. De cómo el barbero no tiene quién lo afeite,
el cartero no tiene quién le entregue su correspondecia
y Rusell construye su paradoja.

1. Circuitos lógicos.

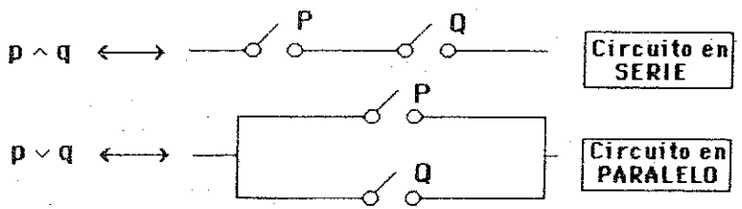
Definamos un interruptor P, de la manera siguiente:



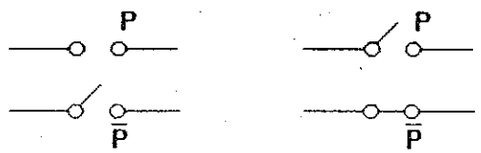
Dada una proposición lógica p, hacemos la identificación:

p	P
F	abierto
V	cerrado.

Podemos interpretar la conjunción y disyunción lógica como sigue:



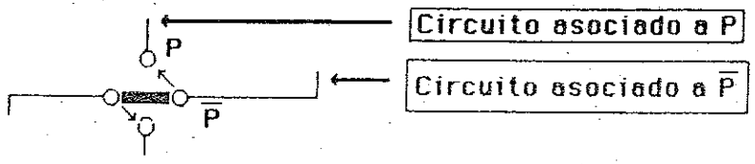
Dado un interruptor P designamos $\bar{P}$ como otro interruptor que está abierto si y sólo si P está cerrado:



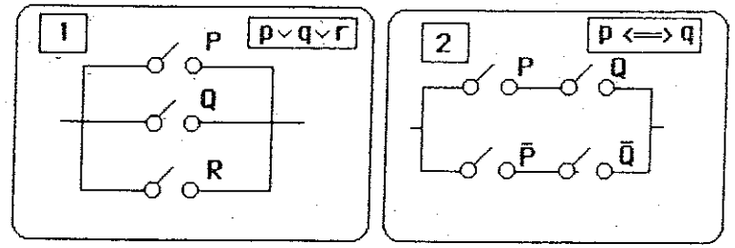
Obviamente un interruptor $\bar{P}$ modela la negación de una proposición lógica:

$$\bar{p} \longleftrightarrow \bar{P}.$$

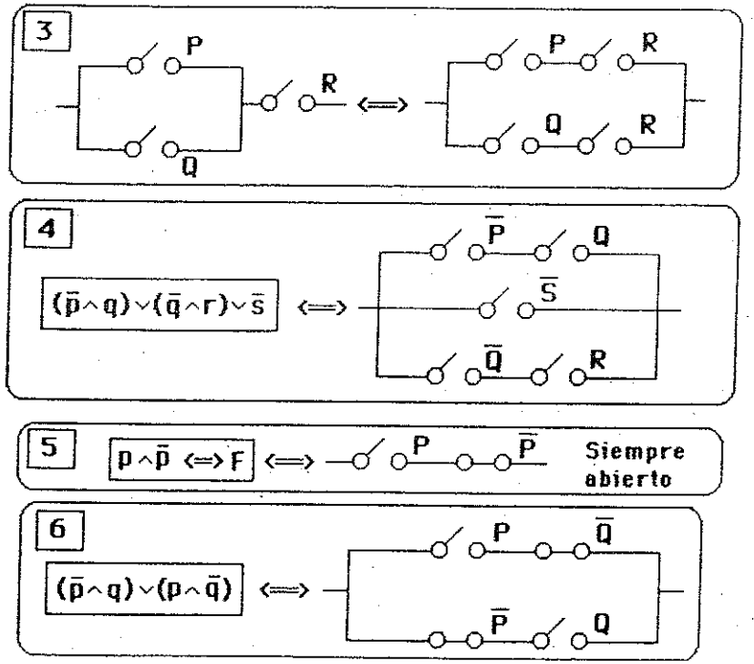
Una manera física de construir un interruptor $\bar{P}$ es la siguiente:



Ejemplos



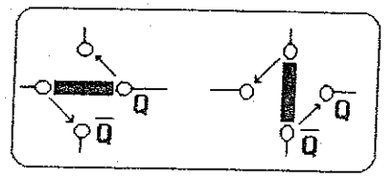
De la tautología $(p \vee q) \wedge r \Longleftrightarrow (p \wedge r) \vee (q \wedge r)$ se obtiene:

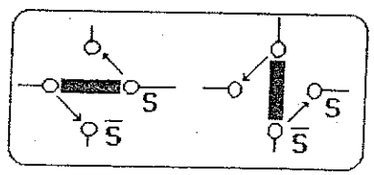


En el circuito del ejemplo 6 la corriente pasa si y sólo si P está abierto y Q cerrado o P está cerrado y Q está abierto. Esto es fácil de verificar pues este circuito es equivalente a la proposición $(p \wedge \bar{q}) \vee (\bar{p} \wedge q)$, correspondiente al "o exclusivo".

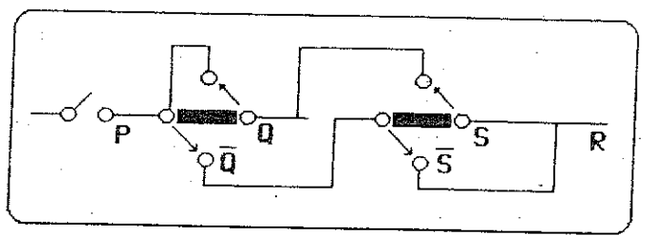
Realicemos mediante un circuito la proposición: $r \Longleftrightarrow (p \wedge \bar{q} \wedge s) \vee (p \wedge q \wedge \bar{s})$ Construyendo ahora "físicamente" los interruptores $\bar{S}$ y $\bar{Q}$:

Interruptores para la Negación:





Circuito asociado a la proposición r:



Desarrollemos la aplicación siguiente:

Se pide construir un circuito para un dormitorio que tiene sólo una lámpara que requiere de dos interruptores: uno en la puerta de entrada y otro cerca de la cama. El circuito debe funcionar de modo que cada interruptor, independientemente de la posición del otro, apague (si está prendida) o prenda (si está apagada) la luz.

Sean P y Q los contactos correspondientes a los dos interruptores.

Tratemos de resolver el problema mediante una proposición lógica r de manera que si ella es "verdadera", al cambiar p o q sea falsa o viceversa. Sea la tabla:

p	q	r
F	F	V
F	V	F
V	F	F
V	V	V

Vemos que, en lenguaje informal, si $p = q = F (r = V)$, al cambiar $p = V$ se obtiene $r = F$. Análogamente si $p = q = V (r = V)$, al cambiar p o q se obtiene $r = F$.

Por otra parte, si el valor de verdad de p y q es distinto (es decir $r = F$), $((p = F \wedge q = V)$ o $(p = V \wedge q = F))$, al cambiar p o q se obtiene $r = V$

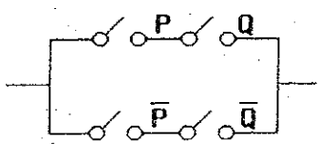
Luego la proposición r asociada es:

$$r \iff (p \iff q).$$

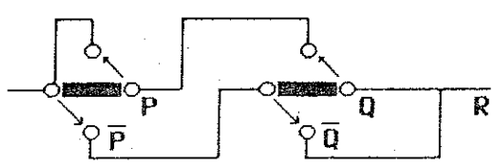
Del teorema 1.11 del Capítulo se obtiene:

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

En términos de circuito:



O bien, construyendo los interruptores $\bar{P}$ y $\bar{Q}$:



Extendamos el ejemplo anterior al caso en que deseamos encender o apagar la ampolleta con tres interruptores independientes. De manera análoga al caso de dos interruptores, asociemos al circuito deseado una proposición s, de manera que si ella es verdadera, al cambiar p, q o r (las proposiciones

asociadas e interruptores P, Q y R) sea falsa o viceversa. La tabla de verdad es la siguiente:

p	q	r	s
V	V	V	V
V	V	F	F
V	F	V	F
V	F	F	V
F	V	V	F
F	V	F	V
F	F	V	V
F	F	F	F

Es directo verificar que la proposición asociada es

$$s \Leftrightarrow (p \Leftrightarrow q) \Leftrightarrow r.$$

En efecto, si p y q tienen distintos valores de verdad, entonces, el valor de verdad de $(p \Leftrightarrow q)$ es F. Luego, en este caso:

$$s \Leftrightarrow (F \Leftrightarrow r).$$

Esto significa que s cambia su valor de verdad de acuerdo al valor de la proposición $\bar{r}$: si r es falsa, s es verdadera. Si r es verdadera entonces s es falsa.

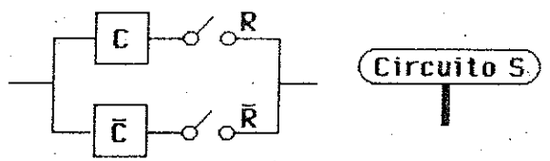
Si p y q tienen el mismo valor de verdad, entonces $(p \Leftrightarrow q)$ es verdadera y se tiene, en esta situación:

$$s \Leftrightarrow (V \Leftrightarrow r).$$

Sea $c \Leftrightarrow (p \Leftrightarrow q)$. Luego la proposición que nos interesa tiene la forma:

$$s \Leftrightarrow (c \Leftrightarrow r).$$

Denominaremos C el circuito asociado a c y $\bar{C}$ el asociado a $\bar{c}$. En este contexto, y de acuerdo al circuito asociado a una equivalencia (ver ejemplo 2), el circuito S, asociado a s, es el siguiente:



Como C es el circuito asociado a $(p \Leftrightarrow q)$, del ejemplo 2 se tiene:

Tratemos de resolver el problema mediante una proposición lógica r de manera que si ella es "verdadera", al cambiar p o q sea falsa o viceversa. Sea la tabla:

p	q	r
F	F	V
F	V	F
V	F	F
V	V	V

Vemos que, en lenguaje informal, si $p = q = F (r = V)$, al cambiar $p = V$ se obtiene $r = F$. Análogamente si $p = q = V (r = V)$, al cambiar p o q se obtiene $r = F$.

Por otra parte, si el valor de verdad de p y q es distinto (es decir $r = F$), $((p = F \wedge q = V)$ o $(p = V \wedge q = F))$, al cambiar p o q se obtiene $r = V$

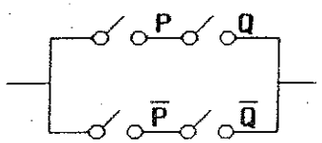
Luego la proposición r asociada es:

$$r \Longleftrightarrow (p \Longleftrightarrow q).$$

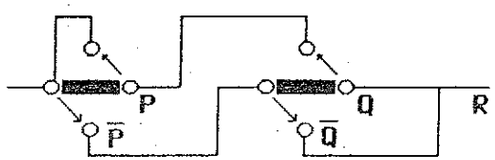
Del teorema 1.11 del Capítulo se obtiene:

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

En términos de circuito:



O bien, construyendo los interruptores $\bar{P}$ y $\bar{Q}$:



Extendamos el ejemplo anterior al caso en que deseamos encender o apagar la ampolleta con tres interruptores independientes. De manera análoga al caso de dos interruptores, asociemos al circuito deseado una proposición s, de manera que si ella es verdadera, al cambiar p, q o r (las proposiciones

asociadas e interruptores P, Q y R) sea falsa o viceversa. La tabla de verdad es la siguiente:

p	q	r	s
V	V	V	V
V	V	F	F
V	F	V	F
V	F	F	V
F	V	V	F
F	V	F	V
F	F	V	V
F	F	F	F

Es directo verificar que la proposición asociada es

$$s \Leftrightarrow (p \Leftrightarrow q) \Leftrightarrow r.$$

En efecto, si p y q tienen distintos valores de verdad, entonces, el valor de verdad de $(p \Leftrightarrow q)$ es F. Luego, en este caso:

$$s \Leftrightarrow (F \Leftrightarrow r).$$

Esto significa que s cambia su valor de verdad de acuerdo al valor de la proposición $\bar{r}$: si r es falsa, s es verdadera. Si r es verdadera entonces s es falsa.

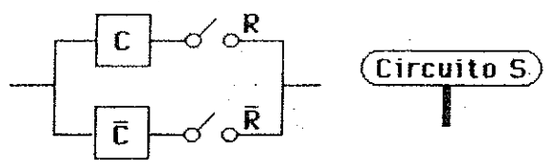
Si p y q tienen el mismo valor de verdad, entonces $(p \Leftrightarrow q)$ es verdadera y se tiene, en esta situación:

$$s \Leftrightarrow (V \Leftrightarrow r).$$

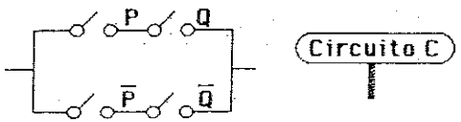
Sea $c \Leftrightarrow (p \Leftrightarrow q)$. Luego la proposición que nos interesa tiene la forma:

$$s \Leftrightarrow (c \Leftrightarrow r).$$

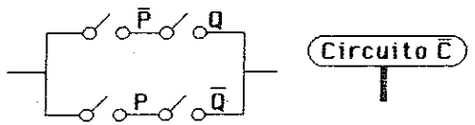
Denominaremos C el circuito asociado a c y $\bar{C}$ el asociado a $\bar{c}$. En este contexto, y de acuerdo al circuito asociado a una equivalencia (ver ejemplo 2), el circuito S, asociado a s, es el siguiente:



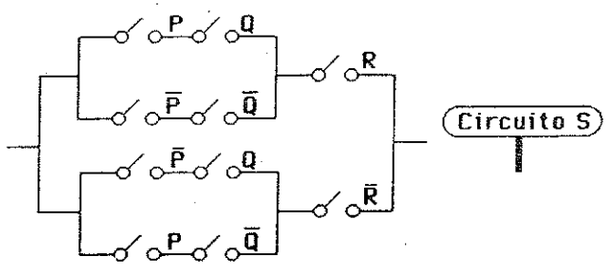
Como C es el circuito asociado a $(p \Leftrightarrow q)$, del ejemplo 2 se tiene:



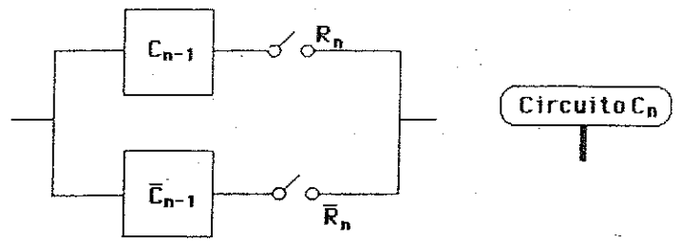
Por otra parte, como $\bar{c} \Leftrightarrow \overline{(p \Leftrightarrow q)} \Leftrightarrow (\bar{p} \Leftrightarrow q)$ (verifique), obtenemos, del ejemplo 2:



Concluímos entonces que el circuito solicitado es



La construcción previa puede extenderse de manera natural al caso de n interruptores. Si hemos logrado construir un circuito que apague o encienda una ampolleta con $n-1$ interruptores independientes (denominemos C_{n-1} este circuito), al agregar uno más, el interruptor R_n, tendremos el circuito:



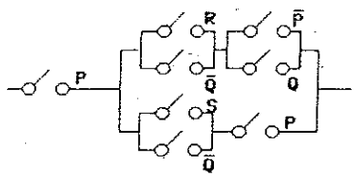
Esta idea, denominada construcción recursiva, se formalizará en el próximo capítulo.

Ejercicios.

1. Verifique las tautologías del capítulo utilizando circuitos .
2. Construya un circuito R con los interruptores P, Q, U, V tal que:
   (a) R esté cerrado (pasa corriente) si todos los interruptores están cerrados o ninguno está cerrado.
   (b) El circuito R estará cerrado cuando algunos, pero no todos, los contactos P, Q, U, V estén cerrados.
3. Un comité de tres personas requiere un circuito que indique el resultado de sus votaciones. Para votar, cada miembro del comité presiona un botón. La ampolleta del circuito debe prenderse si y sólo si la proposición elegida es mayoritaria.
4. Construir un circuito análogo para un comité compuesto por un presidente y cinco miembros: la ampolleta debe alumbrarse si y sólo si la

proposición elegida tiene la mayoría o bien sólo la mitad incluyendo, en este último caso, al presidente.

5. Reduzca (simplifique) el circuito:



6. (a) ¿Cuántos cables necesita para construir físicamente el circuito que apaga o enciende una ampolleta con dos interruptores independientes?
   (b) ¿Cuántos cables se requieren en el caso de 3 interruptores independientes?
   (c) ¿Cuántos cables se requieren en el caso de n interruptores independientes? (¿Será esto posible de construir físicamente?). Atrévase, especule.

2. De cómo el barbero no tiene quién lo afeite, el cartero no tiene quién le entregue la correspondencia y Russell construye su paradoja.

En el pueblo de Tamegroute (10 millas al este de Zagora) el alcalde ha dictado dos extrañas leyes:

1) El único cartero del poblado sólo puede llevar la correspondencia a aquellos que no la retiran por sí mismos de Correos.
2) De manera análoga, el único barbero sólo puede afeitar a aquellos que no pueden afeitarse a sí mismos.

Mientras el barbero afeita al cartero se produce el diálogo siguiente:

Barbero: Tengo un grave problema. Bien sabe usted que sólo puedo afeitar a aquellos habitantes que no se afeitan a sí mismos. Pero, ¿cómo me afeito yo? ¿A qué parte de los habitantes pertenezco?, pues si me afeito, entonces soy del bando de los que se afeitan por sí mismos luego, de acuerdo a la disposición municipal, no puedo afeitarme.

Por otra parte, si no me afeito, entonces estoy en el conjunto de los que no se afeitan a sí mismos, luego puedo afeitarme pero si me afeito ...

Cartero: Mi situación es tan angustiante como la suya, pues, ¿qué puedo hacer con mi correspondencia? etcétera, etcétera...

Paradoja de Russell.

Sea el conjunto que comprende a todos los conjuntos que no se contienen a sí mismos como elementos. Por ejemplo, el conjunto de todas las mujeres no es una mujer, luego éste no se contiene a sí mismo.

Podríamos decir que este tipo de conjuntos son aquellos que no poseen las propiedades características de los elementos que contienen.

También existen conjuntos que se contienen a sí mismos como elementos: el conjunto de todos los conjuntos, "el conjunto de objetos caracterizados por ocho palabras" se contiene a sí mismo ya que está caracterizado por 8 palabras.

Denominemos *Normales* aquellos conjuntos que no se contienen a sí mismos y *Patológicos* aquellos que se contienen a sí mismos.

Sea $\mathcal{N}$ "el conjunto de todos los conjuntos normales".

Tratemos de ver a cuál clase de conjuntos pertenece $\mathcal{N}$, a la normal o la patológica.

Supongamos que $\mathcal{N}$ es normal, es decir, que no se contiene a sí mismo como elemento, luego $\mathcal{N}$ pertenece al conjunto $\mathcal{N}$ de los conjuntos normales

ya que, por definición $\mathcal{N}$ contiene a todos los conjuntos normales. Pero si $\mathcal{N}$ pertenece a $\mathcal{N}$ entonces $\mathcal{N}$ no es normal.

Supongamos ahora que $\mathcal{N}$ es patológico, es decir $\mathcal{N}$ se contiene a sí mismo como elemento. Luego el conjunto $\mathcal{N}$ contiene un conjunto patológico que es él mismo.

Formalmente, el conjunto de todos los conjuntos normales puede escribirse:

$$\mathcal{N} = \{x | x \notin x\},$$

de donde:

$$(\mathcal{N} \in \mathcal{N} \Rightarrow \mathcal{N} \notin \mathcal{N}) \wedge (\mathcal{N} \notin \mathcal{N} \Rightarrow \mathcal{N} \in \mathcal{N}) \quad \blacksquare$$

Esta paradoja, junto con otras, contribuyó a sembrar la desconfianza en el mundo matemático y finalmente llevó a un reestudio de sus fundamentos, estudio que continúa hasta hoy en día.

Ejercicios.

1. Desarrolle el razonamiento del cartero.

2. Construya ejemplos de conjuntos normales y patológicos.

3. Suponga que en el pueblo en cuestión hay un único profesor de Matemáticas y el alcalde le exige que sólo puede resolver los problemas de Matemáticas de aquellas personas que no saben Matemáticas. El profesor tiene un problema matemático que desea resolver. Discuta y formalice el planteamiento del problema, si el profesor tiene solución o no para su dilema, etcétera.

4. Establezca un diálogo filosófico entre cartero, barbero y profesor.

5. En la puerta del cementerio municipal de Castro aparece la siguiente advertencia: "prohibida la entrada de vendedores ambulantes". ¿Qué puede concluir, en el espíritu Ruselliano o Parriano de la afirmación precedente? Desarrolle (problema "encontrado" en artículo "homenaje a N. Parra", revista APSI, diciembre 1991.)

6. Analice, discuta del punto de vista lógico, reemplace, en lo posible, por proposiciones y construya otros ejemplos:

   (a) : "Se dice que no hay regla sin excepción ¿Es esto cierto? Yo no me atrevería a asegurarlo. En todo caso, si esta afirmación contiene

verdad, será una verdad de hecho, que no satisface plenamente la razón. Toda excepción -se añade- confirma la regla. Esto no parece tan obvio y es, sin embargo, más aceptable lógicamente. Porque si toda excepción lo es de una regla, donde hay excepción hay regla, y quien piensa la excepción piensa la regla. Esto es ya una verdad de razón, es decir, de Perogrullo, mera tautología, que nada nos enseña. No podemos conformarnos con ella. Sutilicemos, añadamos algo que no se le pueda ocurrir a Perogrullo.

1. Si toda excepción confirma la regla, una regla sin excepción sería un regla sin confirmar, de ningún modo una no-regla.
2. Una regla con excepciones, será siempre más firme que una regla sin excepciones, a la cual faltaría la excepción que la confirmase.
3. Tanto más regla será una regla cuanto más abunde en excepciones.
4. La regla ideal sólo contiene excepciones.

Continuad por razonamientos encadenados hasta alcanzar el ápice o el vórtice de vuestro ingenio. Y cuando os hiervan los sesos, etcétera, etcétera."

(b) Sobre la dialéctica.
Cuando el hombre -habla Mairena, iniciando un ejercicio de Retórica- vio su cuerpo desnudo en el espejo de las aguas, se dijo: "he aquí algo perfectamente bello que merece guardarse." E inventó el vestido. Porque, evidentemente... Continúe usted, señor Martínez, desarrollando el tema.

- Evidentemente -habla Martínez-, evidentemente...
- Adelante.
- Evidentemente, no hay vestido que no suponga una previa desnudez. ¿Voy bien?
- Prosiga.
- No hay, pues, vestido sin desnudo, aunque haya un desnudo anterior al vestido. Sirve el vestido, en primer lugar, para guardar y proteger la desnudez de nuestro cuerpo, y, en segundo, para asegurarnos, de la manera más firme, la posibilidad de desnudarnos. ¿Voy bien?
- Sin duda.
- Del mismo modo, o por razones análogas, se inventaron las jaulas para guardar y proteger la libertad de los pájaros, porque evidentemente...
- Adelante.
- No hay jaula pajarera, propiamente dicha, que no suponga una previa libertad de volar. ¿Que no fueron los pájaros los inventores de las jaulas? Sin duda. No es menos cierto que sin el libre vuelo

de los pájaros no existirían las jaulas pajareras.
Una voz.- ¡Claro!
– Es claro, en efecto, que, así como el vestido se debe a la nativa desnudez del cuerpo humano, se debe la jaula a la libertad de las aves para el vuelo. Claro es también que así como los amigos del vestido no son enemigos del desnudo, sino sus más fieles guardadores, los amigos de las jaulas no somos, ni mucho menos, enemigos de la libertad de los pájaros.
Una voz.- ¡Claro!
Otra voz.- ¡No tan claro!

(Juan de Mairena I, Antonio Machado, Ed. Losada, 1957)

7. Comente, discuta, construya otros argumentos y problemas análogos:

   (a) Argumentum Ornithologicum
   Cierro los ojos y veo una bandada de pájaros. La visión dura un segundo o acaso menos; no sé cuántos pájaros vi. ¿Era definido su número? El problema involucra el de la existencia de Dios. Si Dios existe, el número es definido, porque Dios sabe cuántos pájaros vi. Si Dios no existe, el número es indefinido, porque nadie pudo llevar la cuenta. En tal caso, vi menos de diez pájaros (digamos) y más de uno, pero no vi nueve, ocho, siete, seis, cinco, cuatro, tres o dos pájaros. Vi un número entre diez y uno, que no es nueve, ocho, siete, seis, cinco, etcétera. Ese número entero es inconcebible, *ergo* Dios existe.

   (El Hacedor, Jorge Luis Borges, Ed. EMECE, 1967) .

   (b) Supongamos un juego para dos personas que termina en un número finito de movidas, con la ineluctable victoria de uno de los jugadores, *ergo* si Dios existe es único.

CAPITULO II

Que seas todas las mujeres más una.

INDUCCION MATEMATICA

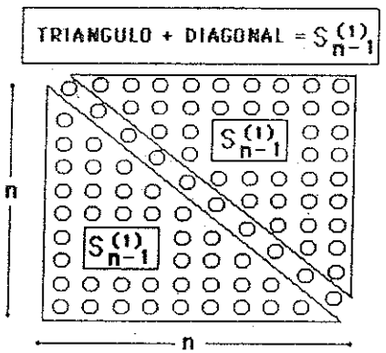
2.1. Principio de inducción.

En 1786 un profesor con deseos de leer el periódico propone a sus alumnos de 9 años sumar los 100 primeros números naturales. Frente al estupor del maestro uno de ellos da la respuesta en pocos minutos: 5050. El alumno se llamaba Gauss. Este razonó de la manera siguiente: si $S_n(1)$ es el valor de la suma de los n primeros números naturales, se tiene

$$\begin{array}{ccccccccc} 1 & + & 2 & +\ldots+ & n & = & S_n(1) \\ + & & + & & + & & + \\ n & + & n-1 & +\ldots+ & 1 & = & S_n(1) \\ \hline (n+1) & + & (n+1) & +\ldots+ & (n+1) & = & 2S_n(1) \end{array}$$

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

Una manera geométrica de enfocar el problema consiste en asociar a cada número natural k bolitas, luego la suma, $S_n(1)$, se visualiza:



Luego $n^2 = S_n(1) + S_{n-1}(1)$
de donde:

$$n^2 = S_{n-1}(1) + n + S_{n-1}(1)$$

$$2S_{n-1}(1) = n^2 - n \Longrightarrow \quad S_{n-1}(1) = \frac{n(n-1)}{2}.$$

Ahora bien: El problema también podría ser demostrar que $S_n(1) = \frac{n(n+1)}{2}$ $\forall n \geq 0$. En tal caso: verificamos para $n = 0$: $S_0(1) = 0$

$$n = 1, \quad S_1(1) = 0 + 1 = 1 \quad \text{y} \quad \frac{1(2)}{2} = 1$$

$$n = 2, \quad S_2(1) = 0 + 1 + 2 = 3 \quad \text{y} \quad \frac{2(3)}{2} = 3$$

$$n = 3, \quad S_3(1) = 0 + 1 + 2 + 3 = 6 \quad \text{y} \quad \frac{3(4)}{2} = 6, \textit{etc.}$$

Luego suponemos que es verdad para un valor n arbitrario:

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

y, a partir de esta hipótesis, se demuestra para $n + 1$:

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

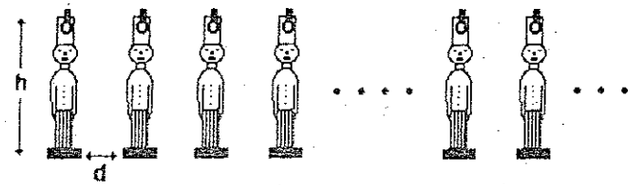
y de aquí concluimos que, como n es arbitrario, entonces es verdad para todo n ■

Observaciones:

1. Se verificó primero la propiedad para el primer número natural (0).
2. Se supuso verdadera la propiedad para n y se demostró para $n + 1$.
3. Se afirmó (de 1 y 2) que era verdad para un número natural, n arbitrario.

Otro ejemplo:

Supongamos un conjunto infinito de soldados de plomo de altura h y a una distancia d tal que $d < h$.



Claramente la experiencia nos dice que al empujar el primero (soldado 0), dado que $d < h$, caen todos los demás. Obviamente esta experiencia es imaginaria y sólo la podemos realizar para una fila finita (aunque) arbitraria de soldados. Cuando el número es infinito, entonces utilizamos el principio anterior:

1) El "soldado 0 cae cuando lo empujamos".
2) Supongamos que cae el $n-$ésimo: dado que $d < h$, éste empuja al $n + 1$, que también cae; luego:
3) todos los soldados caen.

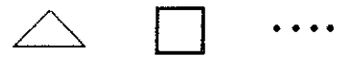
Basándonos en las "experiencias" adquiridas en los dos problemas anteriores, podemos enunciar el *Principio de Inducción:*

Principio de inducción matemática (primera forma).

Sea $P(n)$ una propiedad sobre los números naturales tal que verifica:
(I) $P(0)$ es verdadera

(II) $\forall n \in \mathbb{N}$, $P(n)$ verdadera $\Longrightarrow P(n+1)$ verdadera
entonces $\forall n \in \mathbb{N}$, $P(n)$ es verdadera.

Obviamente, el principio puede aplicarse a partir de un número natural no necesariamente 0. Así por ejemplo, si estamos hablando de alguna propiedad de un polígono de n lados, esto tiene significado sólo para $n \geq 3$:



En tal caso el principio de inducción debe aplicarse a partir de $n_0 = 3$.

Principio de inducción matemática (segunda forma).

(I) $P(n_0)$ *es verdadera*
(II) $\forall n \in \mathbb{N},\ n \geq n_0,\ P(n)$ *verdadera* $\Longrightarrow P(n+1)$ *verdadera*
entonces: $\forall n \in \mathbb{N},\ n \geq n_0\ P(n)$ *verdadera.*

2.2. Usos y abusos inductivos.

El uso del principio de inducción es delicado y debe aplicarse con precaución. Veamos, por ejemplo, el siguiente problema:

Tomemos 999 tarjetas iguales. Sobre las 111 primeras escribamos el número 1, sobre las 111 siguientes escribamos el número 2, y así sucesivamente hasta las últimas 111 marcadas con el número 9.

Mezclemos todas las tarjetas en una bolsa y tomemos n tarjetas al azar (n es un número arbitrario entre 1 y 100), luego veamos los números que se obtienen. Vamos a demostrar que los n dígitos son iguales, independientemente del número de veces que repitamos el experimento. Obviamente esto es falso, basta realizar la experiencia. De todas maneras vamos a dar una demostración (falsa) por inducción:

Sea la propiedad a demostrar P_n : Las n tarjetas, $1 \leq n \leq 100$, tienen el mismo dígito. (tenemos aquí 100 afirmaciones, $n = 1, ..., 100$).

Para $n = 1$, la afirmación es evidentemente verdadera. Si tomamos sólo una tarjeta, cualquiera sea su número el conjunto total (de 1 tarjeta) tiene el mismo dígito.

Tomemos ahora un número k de tarjetas, entre 1 y 99 y demostremos que si P_k es verdadera entonces lo es P_{k+1} :

Saquemos $k+1$ tarjetas de la bolsa y de éstas retiremos una arbitraria, A.

Dada la hipótesis de inducción, las k tarjetas que quedan tienen el mismo número. Luego las $k+1$ tienen el mismo número salvo, tal vez, la tarjeta A.

Reemplazemos ahora una tarjeta arbitraria (entre las k) por A. Nuevamente se tienen k tarjetas, luego por hipótesis de inducción éstas tienen igual número, por lo tanto A tiene el mismo dígito que las $k-1$ y como la $k-$ésima que sacamos es igual a las $k-1$ concluímos que todas, es decir las $k+1$, tienen igual dígito. Con lo cual hemos demostrado que $P(n)$ es verdadero $\forall n \geq 1$.

Reflexionemos, ¿ dónde está el error ? o ¿qué parte del principio de inducción hemos aplicado mal ?

La respuesta es el paso de $n = 1$ a $n = 2$. Si tenemos dos tarjetas α, β y tomamos una (por ejemplo α) nos queda sólo β. Pero al sacar β y poner α

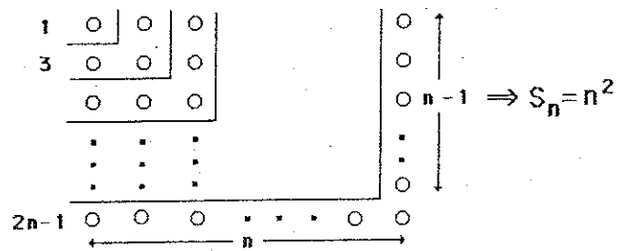
no tenemos una tercera tarjeta para comparar los dígitos de α y β luego esto no implica necesariamente $\alpha = \beta$ de dónde la propiedad es falsa para $k = 2$ luego cualquiera sea $k \geq 2$ el razonamiento es falso pues al poner subconjuntos de $k-1$ no podemos asegurar que tengan el mismo dígito.

Otra observación importante es que, en el primer ejemplo del capítulo, $S_n(1) = 1 + 2 + ... + n$, en realidad hay dos problemas:

1. Conjeturar cuál es el valor de $S_n(1)$.
2. Demostrar que efectivamente el valor conjeturado es el correcto.

Es decir, si no conocemos el valor de la suma no podemos aplicar el principio de inducción. Primero debo establecer la propiedad $P(n)$ y esto suele ser difícil.

Veamos por ejemplo, la suma de los n primeros números impares $S_n = 1+3+5+...+(2n-1)$. Un método astuto para conjeturar su valor es el siguiente: cada entero lo representamos por bolitas distribuidas como sigue



luego $S_n = n^2$. Verifiquemos por inducción:

$$\text{para} \qquad n = 1, \quad 2n - 1 = 1 \quad S_1 = 1^2 = 1.$$

Supongamos verdadero para n; $S_n = n^2$ y demostremos para $n+1$:

$$S_{n+1} = S_n + 2(n+1) - 1 = n^2 + 2n + 2 - 1 =$$
$$= n^2 + 2n + 1 = (n+1)^2 \quad \blacksquare$$

Más difícil sería:

$$S_n(2) = 1^2 + 2^2 + 3^2 + ... + n^2 = ?$$

la suma de los n primeros cuadrados. Develaremos esta incógnita y otras expresiones similares en el párrafo 2.3.

Estudiemos, como último ejemplo, la aplicación denominada *Dividir para Conquistar:*

Dado un conjunto A con 2^n elementos, ordenado de menor a mayor y un elemento $x \in \mathbb{R}$, construir un procedimiento (algoritmo) que mediante $n+1$ preguntas determine si x pertenece o no al conjunto A.

Hagámoslo por inducción sobre n. Para $n = 0$ $|A| = 2^0 = 1$, luego $A = \{a_0\}$ por lo tanto basta preguntar si $x = a_0$ (1 pregunta). Para $n = 1$ $|A| = 2^1 = 2$; $A = \{a_0, b_0\}$ obviamente bastan $2 = n+1$ preguntas:

$$x \leq a_0, \quad x \leq b_0.$$

Supongamos que conocemos un procedimiento para todo conjunto A, $|A| = 2^n$, y tal que involucre a lo más $n+1$ preguntas. Tomemos $n+1$, es decir, $A = \{a_0, ..., a_{2^n-1}, b_0, ..., b_{2^n-1}\}$ ($|A| = 2^{n+1}$) con:

$$a_0 < a_1 < ... < a_{2^n-1} < b_0 < b_1 < ... < b_{2^n-1}.$$

Podemos particionar:

$$A = \underbrace{\{a_0, ..., a_{2^n-1}\}}_{B} \cup \underbrace{\{b_0, ..., b_{2^n-1}\}}_{C}.$$

1. Preguntamos si $x \leq a_{2^n-1}$
2. Si $x \leq a_{2^n-1} \Longrightarrow x \notin C$ y bastan (hipótesis de inducción) $n+1$ pregunta para saber si está en B.
3. Si $x > a_{2^n-1}$, bastan $n+1$ preguntas para saber si está en C.

Luego, con $1 + (n+1) = n+2$ preguntas sabemos si x pertenece o no a A. Luego, hemos determinado un procedimiento para todo conjunto $|A| = 2^n$ para saber si un elemento x pertenece o no a él. El procedimiento anterior es muy utilizado en la elaboración de algoritmos y se conoce como la técnica de *dividir para conquistar*: un problema se divide en subproblemas más pequeños para los cuales se tiene ya un procedimiento para resolverlos.

2.3. Recurrencias.

En el párrafo anterior comenzamos con el cálculo de $S_n(1) = 1+2+...+n$. Claramente, $S_1(1) = 1$ y $S_n(1) = S_{n-1}(1) + n$. $\forall n \geq 2$. Esta ecuación que para ser evaluada depende de valores anteriores, la denominaremos *recursiva* o de *recurrencia*. Si disponemos de una calculadora electrónica o un computador, dado el valor $S_1(1)$, podemos ir calculando los valores sucesivos

de manera automática $S_1(1) = 1$, $S_2(1) = S_1(1) + 2 = 1 + 2 = 3, S_3(1) = S_2(1) + 3 = 6$,... etcétera.

Pero en matemáticas preferimos las *fórmulas cerradas*, es decir obtener de una vez y para siempre el valor de $S_n(1)$ en función de n, sin tener que calcular necesariamente los valores anteriores (además, esto es más económico del punto de vista de tiempo y cálculos en el computador). En el caso aludido la fórmula cerrada es $n(n+1)/2$, que para un valor n requiere sólo una multiplicación y una división en vez de muchísimas sumas cuando n es grande.

Antes de discutir algunas recurrencias interesantes vamos a dar una notación importante en matemáticas, la de *sumatoria*.

Sea $(a_i)_{i\geq 0} = \{a_0, a_1, a_2, ...\}$ un conjunto de números reales, también denominado una *sucesión*, y sea:

$$S_n = a_0 + a_1 + a_2 + ... + a_n$$

la suma de los $n+1$ primeros elementos de la sucesión que notaremos:

$$S_n = \sum_{i=0}^{n} a_i. \tag{2.1}$$

Claramente (2.1) es equivalente a la definición recursiva, o de recurrencia, siguiente:

$$\begin{aligned} S_0 &= a_0 \\ S_n &= S_{n-1} + a_n \qquad \forall n \geq 1 \end{aligned} \tag{2.2}$$

o bien, con la notación Σ :

$$\begin{aligned} \sum_{i=0}^{0} a_i &= a_0 \\ \sum_{i=0}^{n} a_i &= \sum_{i=0}^{n-1} a_i + a_n \qquad \forall n \geq 1 \end{aligned} \tag{2.3}$$

$\sum_{i=0}^{n} a_i$ se lee "sumatoria de $i = 0$ hasta $i = n$ de los valores a_i".

Es conveniente observar que en la definición de sumatoria los índices son "mudos", es decir

$$\sum_{i=0}^{n} a_i = \sum_{j=0}^{n} a_j = \sum_{k=0}^{n} a_k = \text{ etcétera,}$$

pero, ¡atención!

$$\sum_{i=0}^{n} a_i \neq \sum_{k=0}^{n} a_j;$$

en este último caso $j \neq k$.

A partir de la definición anterior podemos establecer sumatorias a partir de un índice no necesariamente 0. Definimos:

$$\begin{aligned} \sum_{i=k}^{n} a_i &= \sum_{i=0}^{n} a_i - \sum_{i=0}^{k-1} a_i \qquad \forall \quad 1 \leq k \leq n \\ &= (a_0 + a_1 + ... + a_n) - (a_0 + ... + a_{k-1}) \\ &= (a_k + a_{k+1} + ... + a_n). \end{aligned} \tag{2.4}$$

Leemos $\sum_{i=k}^{n} a_i$ como sumatoria de los valores a_i entre los índices k y n. De esto se desprende que podemos particionar una suma de manera arbitraria:

$$\sum_{i=0}^{n} a_i = \sum_{i=0}^{k-1} a_i + \sum_{i=k}^{n} a_i \qquad 0 \leq 1 < k \leq n,$$

y en particular:

$$\sum_{i=k}^{k} a_i = a_k,$$

también en este caso, es posible utilizar la definición recursiva:

$$\sum_{i=k}^{n+1} a_i = \sum_{i=k}^{n} a_i + a_{n+1} \qquad \begin{matrix} \forall n \geq k \\ \forall 0 \leq k \leq n; \end{matrix}$$

en efecto,

$$\begin{aligned} &\sum_{i=0}^{n+1} a_i - \sum_{i=0}^{k-1} a_i \\ &= \sum_{i=0}^{n} a_i + a_{n+1} - \sum_{i=0}^{k-1} a_i \\ &= \sum_{i=k}^{n} a_i + a_{n+1} \qquad \blacksquare \end{aligned}$$

Otras propiedades útiles, de demostración directa, son las siguientes:

$$\sum_{i=0}^{n} \lambda = \lambda(n+1), \qquad \forall \lambda \in \mathbb{R} \tag{2.5}$$

$$\sum_{i=0}^{n} \lambda a_i = \lambda \sum_{i=0}^{n} a_i, \qquad \forall \lambda \in \mathbb{R} \tag{2.6}$$

$$\sum_{i=0}^{n} (a_i + b_i) = \sum_{i=0}^{n} a_i + \sum_{i=0}^{n} b_i \tag{2.7}$$

$$\sum_{i=0}^{n} a_i = \sum_{i=s}^{n+s} a_{i-s} \text{ (cambio de variables).} \tag{2.8}$$

$$\sum_{i=1}^{n} (a_i - a_{i-1}) = a_n - a_0 \text{ (propiedad telescópica).} \tag{2.9}$$

De acuerdo a la expresión (2.4) podemos enunciar propiedades equivalentes para sumatorias que parten de un valor no necesariamente nulo ($\sum_{i=k}^{n}$).

Por ejemplo, la propiedad (2.5) sería:

$$\sum_{i=k}^{n} \lambda = \lambda(n-k+1) \quad \forall \lambda \in \mathbb{R}, \quad \forall 0 \leq k \leq n.$$

La propiedad (2.8) es muy útil y consiste solamente en un cambio de índices:

$$\begin{aligned} 0 &\rightarrow a_0 \qquad i = s \qquad \rightarrow a_{s-s} = a_0 \\ 1 &\rightarrow a_1 \qquad i = s+1 \rightarrow a_{s+1-s} = a_1 \\ &\vdots \qquad\quad \vdots \\ n &\rightarrow a_n \qquad i = s+n \rightarrow a_{s+n-s} = a_n, \end{aligned}$$

luego, las sumatorias tienen el mismo valor.

La demostración rigurosa de cada una de las propiedades se hace directamente de la definición recursiva y utilizando el principio de inducción (¡verificarlo!). Demostremos, por ejemplo, la propiedad (2.9):

Es cierto para $n = 1$

$$\sum_{i=1}^{1} (a_i - a_{i-1}) = a_1 - a_0;$$

supongamos que se verifica para n y demostremos para $n+1$:

$$\sum_{i=1}^{n+1}(a_i+a_{i-1})=\sum_{i=1}^{n}(a_i-a_{i-1})+a_{n+1}-a_n=a_n-a_0+a_{n+1}-a_n=a_{n+1}-a_0 \quad \blacksquare$$

La notación Σ nos da un marco cómodo para el cálculo de ciertas expresiones. En este contexto desarrollamos el ejemplo siguiente:

Conocida la sumatoria

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

La pregunta es ¿cuál es el valor de la sumatoria de los cuadrados?

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

Obviamente: $1^2 \leq n^2$, $2^2 \leq n^2, \ldots, n^2 \leq n^2$ de donde

$$S_n(2)=\sum_{i=1}^{n} i^2 \leq \sum_{i=1}^{n} n^2 = nn^2 = n^3.$$

Conjeturamos entonces que el valor, $S_n(2)$, es un polinomio cúbico en la variable n :

$$S_n(2)=a_0+a_1n+a_2n^2+a_3n^3,$$

donde, a_0, a_1, a_2, a_3 son coeficientes por determinar:

Si $n=0 \Longrightarrow a_0=0$, luego:

$$S_n(2)=a_1n+a_2n^2+a_3n^3.$$

Evaluando para $n=1, n=2$ y $n=3$ se obtiene el sistema de tres ecuaciones y tres incógnitas:

$$\begin{array}{rrrl} a_1+ & a_2+ & a_3 & =1 \\ 2a_1+ & 4a_2+ & 8a_3 & =5 \\ 3a_1+ & 9a_2+ & 27a_3 & =14, \end{array}$$

de donde

$$\begin{array}{rrrl} a_1+ & a_2+ & a_3= & 1 \\ & 2a_2+ & 6a_3= & 3 \\ & 6a_2+ & 24a_3= & 11 \end{array} \Longrightarrow \begin{array}{rrrl} a_1+ & a_2+ & a_3= & 1 \\ & 2a_2+ & 6a_3= & 3 \\ & & 6a_3= & 2 \end{array}$$

$$\Longrightarrow a_3=1/3 \Longrightarrow a_2=(3-6a_3)/2=1/2$$

$$\Longrightarrow a_1=1-a_2-a_3=1-\frac{1}{2}-\frac{1}{3}=\frac{6-3-2}{6}=\frac{1}{6}.$$

Reemplazando los coeficientes, $S_n(2)=\frac{1}{6}n+\frac{1}{2}n^2+\frac{1}{3}n^3$

$$=\frac{n+3n^2+2n^3}{6}.$$

Obtenemos entonces una fórmula cerrada para la suma de los n primeros cuadrados:

$$S_n(2)=\frac{n(n+1)(2n+1)}{6}. \tag{2.10}$$

Otra manera de calcular esta suma es "complicando" el problema. No sabemos calcular la suma de cuadrados, ¡utilicemos entonces la suma de los cubos!:

$$S_n(3)=\sum_{i=1}^{n} i^3$$

Se tiene que:

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

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

de donde:

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

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

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

Si aún no está convencido, puede verificar esto por inducción $\blacksquare$

2.4 Progresiones.

2.4.1. Progresiones aritméticas.

Dadas las sucesiones de números reales: $1, 3, 5, 7, X?$; $2, 0, -2, -4, -6, Y?$ Los números que se nos imponen como sus próximos elementos son $X = 9$ e $Y = -8$. Estas soluciones intuitivas corresponden a sucesiones de números construidos según la regla:

$$a_{n+1} = a_n + d, \text{ donde } d \text{ es una constante real.}$$

Una sucesión $(a_n)_{n\geq 0}, n \in \mathbb{N}$, así construida se denomina *progresión aritmética* de primer término a_0 y *diferencia* d. Es directo de la definición que

$$a_i = a_0 + id, \quad \forall i \geq 0.$$

En efecto, como $a_i = a_{i-1} + d$, entonces $a_i = a_{i-2} + 2d = ... = a_0 + id$ ■

La sucesión $0, 1, 2, 3, ..., n, ...$ es una progresión aritmética de primer término 0 y diferencia $d = 1$.

Al comienzo del capítulo calculamos el valor de la suma $\frac{n(n+1)}{2}$. La pregunta natural es cuál es el valor de la suma de los $n+1$ primeros términos en una progresión aritmética arbitraria:

$$S = \sum_{i=0}^{n} a_i = \ ?$$

Un método directo es similar al de Gauss (ver párrafo (2.1)):

$$S = \sum_{i=0}^{n} (a_0 + id), \tag{2.11}$$

pero también:

$$S = \sum_{i=0}^{n} (a_0 + (n-i)d).$$

Desarrollando las sumatorias:

$$\begin{array}{ccccccc} a_0 & + & a_0 + d & \cdots & +a_0 + nd & = & S \\ (a_0 + nd) & + & a_0 + (n-1)d & \cdots & +a_0 & = & S \end{array}$$

se obtiene

$$\begin{aligned} 2S &= \sum_{i=0}^{n} (a_0 + id + a_0 + (n-i)d) \\ &= \sum_{i=0}^{n} (2a_0 + nd) = (n+1)(2a_0 + nd), \end{aligned}$$

de donde

$$S = \frac{n+1}{2}(2a_0 + nd), \tag{2.12}$$

es la expresión de la fórmula cerrada de la suma de los $n+1$ primeros términos en progresión aritmética ■

Observación: También se puede hacer directamente de (2.11), distribuyendo la sumatoria y usando $S_n(1) = 1+2+...+n = \frac{n(n+1)}{2}$, aunque esto es menos elegante.

2.4.2. Progresiones geométricas.

En este caso tomamos una sucesión de números reales $(a_n)_{n\geq 0}$ tal que $a_{n+1} = ra_n \quad \forall n \geq 0$. Una sucesión así construida se denomina *progresión geométrica* de primer término a_0 y *razón* r.

Por ejemplo, para $a_0 = 1 \quad y \quad r = \frac{1}{2}$ se tiene:

$$1, \quad \frac{1}{2}, \quad \frac{1}{4}, \quad \frac{1}{8} \cdots$$

En general el i-ésimo término

$$a_i = ra_{i-1} = r^2 a_{i-2} = r^3 a_{i-3} = ... = r^i a_0,$$

por lo tanto,

$$S = \sum_{i=0}^{n} a_i = \sum_{i=0}^{n} a_0 r^i$$

pero,

$$\begin{aligned} S + a_0 r^{n+1} &= a_0 r^0 + \sum_{i=0}^{n} a_0 r^{i+1} \\ &= a_0 + \sum_{i=0}^{n} a_0 r r^i \\ &= a_0 + r \sum_{i=0}^{n} a_0 r^i = a_0 + rS, \end{aligned}$$

de donde

$$S(1-r) = a_0 - a_0 r^{n+1};$$

entonces, la suma de los $n+1$ primeros términos de una progresión aritmética es

$$S = \frac{a_0(1-r^{n+1})}{(1-r)} \qquad \text{para } r \neq 1. \tag{2.13}$$

Para el caso $r = 1$, trivialmente obtenemos $S = a_0(n+1)$.

Otra manera de realizar este cálculo es la siguiente:

$$(r-1)\sum_{i=0}^{n} a_i = a_0 \sum_{i=0}^{n}(r-1)r^i = a_0 \sum_{i=0}^{n}(r^{i+1} - r^i)$$

$$= a_0(r^{n+1} - r^0) \qquad \text{(de la propiedad telescópica)}$$

y finalmente

$$S = \sum_{i=0}^{n} a_i = a_0 \frac{r^{n+1}-1}{r-1} = a_0\left(\frac{1-r^{n+1}}{1-r}\right).$$

2.5. Coeficientes binomiales.

Los coeficientes binomiales son números muy importantes en matemáticas, tanto por sus diversas aplicaciones, como por los hermosos teoremas e interpretaciones que es posible asociarles. Antes de estudiarlos definiremos de manera recursiva, la noción de *factorial*:

$$\begin{aligned} 0! &= 1 \\ n! &= n(n-1)! \end{aligned} \qquad \text{(factorial de } n \in \mathbb{N})$$

o bien,

$$n! = n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1. \tag{2.14}$$

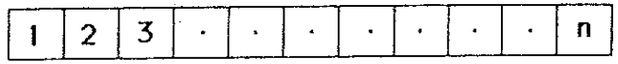
El número factorial tiene aplicación en el conteo finito de objetos. Veamos un ejemplo:

Dadas 4 cartas distintas, $\{A, B, C, D\}$, ¿de cuántas maneras distintas podemos alinearlas? Se tiene:

A	B	C	D	B	A	C	D	C	D	A	B	D	C	A	B
A	B	D	C	B	A	D	C	C	D	B	A	D	C	B	A
A	C	B	D	B	C	A	D	C	A	D	B	D	A	C	B
A	C	D	B	B	C	D	A	C	A	B	D	D	A	B	C
A	D	C	B	B	D	C	A	C	B	D	A	D	B	C	A
A	D	B	C	B	D	A	C	C	B	A	D	D	B	A	C
	6				6				6				6		

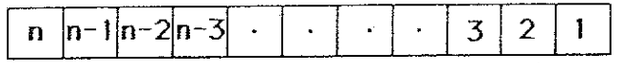
contabilizando $24 = 4 \times 3 \times 2 \times 1 = 4!$ maneras.

En general, supongamos que se tienen n objetos $\{A_1, ..., A_n\}$. ¿De cuántas maneras podemos ordenarlos en una fila?



Sean $1, 2, 3, ..., n$ las n posiciones en la fila. En la primera posición podemos colocar cualquier objeto de los n; se tienen entonces n maneras :

Una vez fijo el primero, el segundo puede ser elegido arbitrariamente entre los $n-1$ restantes. En general:



Obviamente el razonamiento es válido desde cualquier posición.

Luego, el *número total de maneras de colocar los n objetos sin repetición* (cada objeto aparece una y sólo una vez en la fila) es

$$n \times (n-1) \times (n-2) \times ... \times 3 \times 2 \times 1 = n!$$

2.5.1. Triángulo de Pascal.

Definimos el arreglo de números naturales denominado *triángulo de Pascal.*

n \ k	0	1	2	3	$\cdots$	$k-1$	k	$\cdots$	$n-1$	n
0	1									
1	1	1								
2	1	2	1							
3	1	3	3	1						
$\vdots$										
$n-1$	C_{n-1}^0	C_{n-1}^1	C_{n-1}^2	C_{n-1}^3	$\cdots$	C_{n-1}^{k-1}	C_{n-1}^k	$\cdots$	C_{n-1}^{n-1}	
n	C_n^0	C_n^1	C_n^2	C_n^3	$\cdots$	C_n^{k-1}	C_n^k	$\cdots$	C_n^{n-1}	C_n^n

O mediante una ecuación recursiva:

$$\begin{aligned} &C_n^0 = C_n^n = 1 \qquad \forall n \in \mathbb{N} \\ &C_n^k = C_{n-1}^{k-1} + C_{n-1}^k \qquad \forall k \in \mathbb{N}, \quad 1 \leq k \leq n-1. \end{aligned} \tag{2.15}$$

Estos números se denominan *coeficientes binomiales* y se notan C_n^k o bien $\binom{n}{k}$. La ecuación (2.15) es una *recurrencia*, en el sentido que los valores de la línea n se conocen en función de dos anteriores, de la línea $n-1$, ya calculados. La solución cerrada de esta recurrencia (en función de n y k) es la siguiente:

$$C_n^k = \frac{n!}{k!(n-k)!} \qquad 0 \leq k \leq n, \quad n \in \mathbb{N}. \tag{2.16}$$

En efecto, esto es cierto para $n = 0, k = 0$, $C_0^0 = \frac{0!}{0!0!} = 1$ y $C_0^0 = 1$, directamente de la definición de recurrencia. Supongamos que es cierto para $n-1$ y $0 \leq k \leq n-1$,

$$C_{n-1}^k = \frac{(n-1)!}{k!(n-1-k)!} \qquad 0 \leq k \leq n-1$$

demostremos para n y $0 \leq k \leq n$.

Para $k = 0$ y $k = n$ el resultado es directo de la definición:

$$1 = C_n^0 = \frac{n!}{0!n!} = C_n^n = \frac{n!}{n!0!}.$$

Para $1 \leq k \leq n-1$ se tiene de la recurrencia:

$$C_n^k = C_{n-1}^{k-1} + C_{n-1}^k$$

y por hipótesis de inducción:

$$\begin{aligned} C_n^k &= \frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{k!(n-1-k)!} \\ &= \frac{(n-1)!}{(k-1)!(n-k-1)!} \left\{ \frac{1}{n-k} + \frac{1}{k} \right\} \\ &= \frac{(n-1)!}{(k-1)!(n-k-1)!} \left\{ \frac{n}{k(n-k)} \right\} = \frac{n!}{k!(n-k)!} \end{aligned}$$ ■

Otra propiedad interesante puede observarse si escribimos el triángulo de Pascal de manera simétrica con respecto a la primera columna, $k = 0$;

$k=0$							
1							
1		1					
1		2		1			
1		3		3		1	
1		4		6		4	1

Vemos que los coeficientes binomiales son simétricos con respecto a la vertical $k = 0$:

$$C_n^k = C_n^{n-k} \tag{2.17}$$

En efecto:

$$C_n^{n-k} = \frac{n!}{(n-k)!(n-n+k)!} = \frac{n!}{(n-k)!k!} = C_n^k$$ ■

2.5.2. Binomio de Newton.

Otra observación es la siguiente: si desarrollamos las potencias de $x+y$:

$$\begin{aligned}
x+y &= x+y \\
(x+y)^2 &= x^2+2xy+y^2 \\
(x+y)^3 &= x^3+3x^2y+3xy^2+y^3 \\
(x+y)^4 &= x^4+4x^3y+6x^2y^2+4xy^3+y^4.
\end{aligned}$$

Vemos que los coeficientes corresponden a los observados en el triángulo de Pascal. De donde conjeturamos que:

$$(x+y)^n = C_n^0x^n + C_n^1x^{n-1}y + C_n^2x^{n-2}y^2 + ... + C_n^kx^{n-k}y^k + ... + C_n^ny^n.$$

Utilizando la notación de sumatoria

$$(x+y)^n = \sum_{k=0}^{n} C_n^k x^{n-k}y^k \quad \forall n \geq 1. \tag{2.18}$$

Esta propiedad se denomina el desarrollo del *binomio de Newton*. Para demostrarla utilizamos inducción sobre n. De los casos anteriores vemos que se verifica para $n = 1, 2, 3, 4$. Supongamos que se verifica para n y demostremos para $n+1$:

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

de la recurrencia (2.15) :

$$\begin{aligned}
&= C_{n+1}^0x^{n+1} + C_{n+1}^{n+1}y^{n+1} + \sum_{k=1}^{n} C_{n+1}^k x^{n+1-k}y^k \\
&= \sum_{k=0}^{n+1} C_{n+1}^k x^{n+1-k}y^k \quad \blacksquare
\end{aligned}$$

Una identidad interesante derivada del desarrollo del binomio es:

$$2^n = \sum_{k=0}^{n} C_n^k,$$

basta tomar el desarrollo de $(1+1)^n$ ■

Para ejercitar las meninges probemos la identidad:

$$\sum_{k=1}^{n} \frac{(-1)^k C_n^k}{k+1} = \frac{1}{n+1}.$$

En efecto,

$$\begin{aligned}
\frac{C_n^k}{k+1} &= \frac{n!}{k!(n-k)!(k+1)} = \\
&= \frac{(n+1)n!}{(n+1)(k+1)!(n-k)!} = \frac{1}{n+1} C_{n+1}^{k+1},
\end{aligned}$$

luego,

$$\sum_{k=0}^{n} \frac{(-1)^k C_n^k}{k+1} = \frac{1}{n+1} \sum_{k=0}^{n} (-1)^k C_{n+1}^{k+1} \tag{2.19}$$

pero, aplicada la recurrencia (2.15), de los coeficientes binomiales, se obtiene:

$$\begin{aligned}
\sum_{k=0}^{n} (-1)^k C_{n+1}^{k+1} &= (-1)^n + \sum_{k=0}^{n-1} (-1)^k C_{n+1}^{k+1} \\
&= (-1)^n + \sum_{k=0}^{n-1} (+1)^k C_n^k + \sum_{k=0}^{n-1} (-1)^k C_n^{k+1} \\
&= \sum_{k=0}^{n} (-1)^k C_n^k + \sum_{k=0}^{n-1} (-1)^k C_n^{k+1}
\end{aligned}$$

de la fórmula (2.18), del binomio de Newton:

$$= (1-1)^n + \sum_{k=0}^{n-1} (-1)^k C_n^{k+1},$$

realizando el cambio de índices, $j = k+1$:

$$= \sum_{j=1}^{n} (-1)^{j-1} C_n^j$$
$$= \sum_{j=1}^{n} (-1)^j (-1) C_n^j$$
$$= -\sum_{j=1}^{n} (-1)^j C_n^j = -(\sum_{j=0}^{n} (-1)^j C_n^j - 1).$$

Utilizando nuevamente la fórmula del binomio de Newton concluímos:

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

Reemplazando en (2.19), se obtiene la identidad propuesta ■

2.6. Interpretación combinatorial de los coeficientes binomiales.

Supongamos que se tienen cuatro cartas: $\{A, B, C, D\}$. ¿De cuántas maneras distintas podemos seleccionar $1 \leq r \leq 4$ entre ellas?
Para una carta ($r = 1$) obviamente la respuesta es 4 maneras A o B o C o D.

Para 2 cartas se tienen 6 maneras:

$$\{A, B\}, \{A, C\}, \{A, D\}, \{B, C\}, \{B, D\}, \{C, D\}.$$

Conviene señalar que nos da lo mismo tomar AB o BA (¡no se cuenta 2 veces!) y es por ello que utilizamos la notación de conjuntos ya que el orden no interesa.

Para 3 cartas se tienen cuatro maneras:

$$\{A, B, C\}, \{A, B, D\}, \{A, C, D\}, \{D, C, B\}.$$

Para $r = 4$ cartas se tiene una manera $\{A, B, C, D\}$.
De esto podemos concluir:

$$r = 1 : \text{número de maneras} = C_4^1 = \frac{4!}{1!3!} = 1$$
$$r = 2 : \text{número de maneras} = C_4^2 = \frac{4!}{2!2!} = 6$$
$$r = 3 : \text{número de maneras} = C_4^3 = \frac{4!}{3!1!} = 4$$
$$r = 4 : \text{número de maneras} = C_4^4 = \frac{4!}{4!0!} = 1.$$

En general se tiene que

$$C_n^k \textit{ es el número de maneras de seleccionar } k \textit{ objetos}$$
$$\textit{distinguibles entre } n \textit{ sin importar el orden.} \qquad (2.20)$$

En efecto, supongamos que sacamos k objetos distinguibles entre n teniendo en cuenta el orden:

$$\begin{array}{cccc} 1 & 2 & \cdots\cdots & k \\ n & n-1 & \cdots\cdots & n-k+1; \end{array}$$

luego, se tienen $n(n-1)...(n-k+1)$ maneras de seleccionar k objetos entre n teniendo en cuenta el orden. Como para cada selección de k objetos éstos pueden ordenarse de $k!$ maneras distintas, el número total de maneras sin importar el orden es:

$$\frac{n(n-1)\cdots(n-k+1)}{k!} = \frac{n!}{k!(n-k)!} = C_n^k \quad ■$$

Esto permite dar otra demostración del desarrollo del binomio. Se tiene que:

$$(x+y)^n = (x+y)(x+y)...(x+y)$$
$$n \text{ veces.}$$

Las potencias que aparecen en el desarrollo son $x^n, x^{n-1}y, ..., xy^{n-1}, y^n$. El coeficiente c, que multiplica el monomio $x^{n-k}y^k$ corresponde al número de veces que, en la multiplicación de los n monomios $(x+y)$, aparece el producto $x^{n-k}y^k$ y esto corresponde a las maneras de seleccionar k monomios entre los n, es decir C_n^k. Por ejemplo, si $n = 4$, el monomio x^3y aparece $C_4^3 = 4$ veces:

$$\begin{array}{lll} (\underline{x}+y)(\underline{x}+y)(\underline{x}+y)(x+\underline{y}) & x^3y & 1 \text{ vez} \\ (\underline{x}+y)(\underline{x}+y)(x+\underline{y})(\underline{x}+y) & x^3y & 1 \text{ vez} \\ (\underline{x}+y)(x+\underline{y})(\underline{x}+y)(\underline{x}+y) & x^3y & 1 \text{ vez} \\ (x+\underline{y})(\underline{x}+y)(\underline{x}+y)(\underline{x}+y) & x^3y & 1 \text{ vez.} \end{array}$$

2.7 Sumatorias múltiples.

Consideremos la suma de elementos:

$$\begin{aligned} S = & a_1b_1 + a_1b_2 + a_1b_3 \\ & + a_2b_1 + a_2b_2 + a_2b_3 \\ & + a_3b_1 + a_3b_2 + a_3b_3 \\ & + a_4b_1 + a_4b_2 + a_4b_3. \end{aligned}$$

Notamos:

$$S = \sum_{i=1}^{4}\sum_{j=1}^{3} a_ib_j = \sum_{i=1}^{4} a_i \sum_{j=1}^{3} b_j.$$

Supongamos que se tiene un arreglo de números reales de m filas y n columnas:

$$\begin{array}{cccccc} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ \vdots & & \vdots & & \\ a_{m1} & a_{m2} & a_{m3} & \cdots & a_{mn}. \end{array}$$

Notamos la suma de todos ellos como:

$$S = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}.$$

Claramente, como la suma no varía si sumamos por filas o por columnas, podemos intercambiar el orden de las sumatorias:

$$S = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij} = \sum_{j=1}^{n}\sum_{i=1}^{m} a_{ij}. \tag{2.21}$$

Veamos el caso particular siguiente:

$$a_{ij} = b_ic_j \qquad 1 \le i \le m, \quad 1 \le j \le n.$$

El arreglo de números es:

$$\begin{array}{ccccc} b_1c_1 & b_1c_2 & \cdots & b_1c_n \\ b_2c_1 & b_2c_2 & \cdots & b_2c_n \\ & \vdots & & \\ b_mc_1 & b_mc_2 & \cdots & b_mc_n. \end{array}$$

Luego,

$$\begin{aligned} \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij} &= \sum_{i=1}^{m}\sum_{j=1}^{n} b_ic_j \\ &= \sum_{i=1}^{m} b_i \sum_{j=1}^{n} c_jb_1 \sum_{j=1}^{n} c_j + \ldots + b_m \sum_{j=1}^{n} c_j \\ &= (b_1 + \ldots + b_m)(c_1 + \ldots + c_n) \\ &= \left(\sum_{i=1}^{m} b_i\right)\left(\sum_{j=1}^{n} c_j\right). \end{aligned} \tag{2.22}$$

de donde $$\sum_{i=1}^{m}\sum_{j=1}^{n} b_ic_j = \left(\sum_{i=1}^{m} b_i\right)\left(\sum_{j=1}^{n} c_j\right).$$

En particular:

$$\begin{aligned} \sum_{i=1}^{m}\sum_{j=1}^{n} ij = \left(\sum_{i=1}^{m} i\right)\left(\sum_{j=1}^{n} j\right) &= \frac{m(m+1)}{2}\frac{n(n+1)}{2} \\ &= \frac{mn(m+1)(n+1)}{4}. \end{aligned}$$

Calculemos por ejemplo:

$$S = \sum_{i=1}^{n}\sum_{j=1}^{i}(i-j)^2 = ?$$

Realizando un cambio de variables:

$$\begin{aligned} \sum_{i=1}^{n}\sum_{k=0}^{i-1} k^2 = \sum_{i=1}^{n}\sum_{k=1}^{i-1} k^2 &= \sum_{i=1}^{n} S_{i-1}(2) \\ &= \sum_{i=1}^{n} \frac{(i-1)(2(i-1)+1)i}{6} = \sum_{i=1}^{n} \frac{(i-1)i(2i-1)}{6} \end{aligned}$$

hemos reducido la sumatoria doble a una simple, donde aparece un polinomio de grado 3 en la variable i. Podemos utilizar entonces las fórmulas de $S_n(3)$, $S_n(2)$, $S_n(1)$ para evaluarlo ■

Para terminar, podemos definir sumatorias múltiples:

$$S = \sum_{i_1=1}^{n_1} \sum_{i_2=1}^{n_2} \cdots \sum_{i_s=1}^{n_2} a_{i_1 i_2 \ldots i_s}.$$

De manera análoga al caso anterior, podemos intercambiar las sumatorias sin alterar el valor:

$$\sum_{i_1} \cdots \sum_{i_s} = \sum_{i'_1} \cdots \sum_{i'_s},$$

donde $i'_1, \ldots, i'_s$ es otro orden de los índices.

En particular:

$$\sum_i \sum_j \sum_k = \sum_i \sum_k \sum_j = \sum_j \sum_i \sum_k$$

$$= \sum_j \sum_k \sum_i = \sum_k \sum_i \sum_j = \sum_k \sum_j \sum_i.$$

La demostración puede verse en un "cubo" de números de dimensión $n_1 \times n_2 \times n_3$ análogo al caso $m \times n$ anterior.

Ejercicios.

Inducción.

1. Demuestre las propiedades enunciadas en el capítulo.
2. Pruebe que $\forall n \in \mathbb{N}, n > 5 \Rightarrow 2^n > n^2$.
3. Demuestre que:
   (a) $\forall n \in \mathbb{N}, n \neq 1, 3, n$ puede expresarse como suma de 2's y/o 5's.
   (b) $\forall n \in \mathbb{N}, n \geq 14, n$ puede expresarse como suma de 3's y/o 8's.
4. Sea $n \in \mathbb{N}, n \geq 1$. Demuestre que si se tienen n^2 triángulos equiláteros iguales, entonces es posible construir con todos ellos otro triángulo equilátero, (sin superponerlos).
5. Demuestre que:
   (a) Si $|X| = n \Rightarrow |\mathcal{P}(X)| = 2^n$.
   (b) Dada la familia $\{A_i\}_{i=1}^n$ de conjuntos finitos, entonces

$$|\bigcup_{i=1}^n A_i| \leq \sum_{i=1}^n |A_i| \quad \forall n \geq 2.$$

6. Sean α y β las raíces de la ecuación $x^2 - 2x + 4 = 0$. Pruebe que $\forall n \in \mathbb{N}, \alpha^n + \beta^n \in \mathbb{Z}$.

Recurrencias.

7. Definamos $(a_n)_{n \in \mathbb{N}}$ tal que: $a_1 = 2, \quad a_{n+1} = \frac{12}{1+a_n}$.
   Demuestre por inducción que
   (a) $a_{2k-1} < a_{2k+1} \quad \forall k \geq 1, k \in \mathbb{N}$.
   (b) $a_{2k} > a_{2k+2} \quad \forall k \geq 1, k \in \mathbb{N}$.
   (c) $a_{2k-1} < 3 \quad \forall k \geq 1, k \in \mathbb{N}$.
   (d) $a_{2k} > 3 \quad \forall k \geq 1, k \in \mathbb{N}$.
8. Calcule las siguientes sumas:
   (a) $\sum_{i=1}^n 2^{i-1}$.
   (b) $\sum_{i=1}^n i^3, \sum_{i=1}^n i^4, \sum_{i=1}^n i^5$.
   (c) $\sum_{i=1}^n \frac{1}{i(i+1)}$.
   (d) $\sum_{i=1}^n 2^{i+1}(\frac{i}{(i+1)(i+2)})$.
   (e) $\sum_{i=1}^{2n}(-1)^i i^2$.

(f) La suma de los 20 primeros términos de: $1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + ...$

(g) La suma de los n primeros términos de:
$1 \cdot (n-1) + 2^2(n-2) + 3^2(n-3) + ...$

(h) $\sum_{k=5}^{250}, \sum_{k=1}^{n} \frac{2k+1}{k^2(k+1)^2}$.

(i) $\sum_{k=1}^{n} k\ell n(\frac{k+1}{k})$.

(j) $\sum_{i=0}^{n} \sum_{j=1}^{m} \frac{j}{3^i}$.

9. Demuestre por inducción que:

(a) La suma $\sum_{k=1}^{2n}(-1)^k(2k+1)$ es proporcional a n y determine la constante de proporcionalidad.

(b) Si $(a_n)_{n\in\mathbb{N}}$ es tal que $a_0 = 0$ y $a_n + \frac{3}{a_{n+1}} = 4$, entonces $a_n = \frac{3(3^n-1)}{3^{n+1}-1}$ $\forall n \in \mathbb{N}$.

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

(d) $\sum_{k=1}^{n}(-1)^{k+1}\frac{1}{4^n} = \frac{1}{5}(1 + \frac{1}{(-4)^n})$.

(e) $\sum_{k=1}^{2n}(-1)^k k^2 = \sum_{k=1}^{n}(4k-1)$.

10. Definamos, por recurrencia, el producto de $(a_n)_{n\in\mathbb{N}}$

$\prod_{k=0}^{0} a_k = a_0$

$\prod_{k=0}^{n} a_k = (\prod_{k=0}^{n-1} a_k) \cdot a_n \quad \forall n \in \mathbb{N}$. Pruebe que:

(a) $\frac{2^n \cdot n!}{\prod_{k=1}^{n}(3k+2)} < (\frac{2}{3})^n, \quad \forall n \in \mathbb{N}$.

(*b) $\sqrt{n+1} < \prod_{k=1}^{n}(n+k)^{\frac{1}{n+k}}$, para $n \geq 2$.

(*c) Si $a_n = \prod_{k=1}^{n} \frac{(2k-1)}{(k+1)}, a_0 = 1$, entonces $\sum_{k=0}^{n} a_k a_{n-k} = a_{n+1}$.

(d) $\prod_{i-1}^{n}(1 + \frac{1}{i})^{i+1} = \frac{(n+1)^{n+1}}{n!}, \quad \forall n \geq 1$.

11. Si $(1 + x + x^2)^n = \sum_{k=0}^{2n} a_k x^k$, pruebe que

$$a_0 + a_3 + a_6 + ... = a_1 + a_4 + a_7 + ... = a_2 + a_5 + a_8 + ...$$

*12. Dada la sucesión $(a_n)_{n\in\mathbb{N}^*}$, definimos

$$u_1 = a_1, \; u_i = a_i + \frac{1}{u_{i-1}}, \quad \forall i \geq 2.$$

La sucesión $(u_n)_{n\in\mathbb{N}^*}$ se dice *bien definida* si $(a_n)_{n\in\mathbb{N}^*}$ es tal que $u_n \neq 0, \forall n \in \mathbb{N}^*$. Sea $(q_n)_{n\in\mathbb{N}^*}$ tal que

$$q_1 = a_1, q_2 = a_2 a_1 + 1$$
$$q_i = a_i q_{i-1} + q_{i-2}, \quad \forall i \geq 3.$$

Pruebe que $u_i = q_i/q_{i-1} \quad \forall i \geq 2$, si $(u_n)_{n\in\mathbb{N}^*}$ está bien definida.

*13. Considere la siguiente tabla:

(0) $x_1 y_2$
(1) $x_1 y_2 y_3 x_4$
(2) $x_1 y_2 y_3 x_4 y_5 x_6 x_7 y_8$
(3) $x_1 y_2 y_3 x_4 y_5 x_6 x_7 y_8 y_9 x_{10} x_{11} y_{12} x_{13} y_{14} y_{15} x_{16}$.

Cada fila de la tabla se construye copiando la fila anterior, luego escribiendo tal secuencia pero intercambiando las "x" por "y" y continuando los índices en orden.
Notemos que en la fila (1), la suma de los índices de x es igual a la suma de los índices de y : $1 + 4 = 2 + 3$. Esto también sucede en la fila (2): $1+4+6+7 = 2+3+5+8$, y además $1^2+4^2+6^2+7^2 = 2^2+3^2+5^2+8^2$.

Demuestre que en la fila (n), la suma de las potencias de orden k de los índices de x coincide con la suma de las potencias de orden k de y, para $k = 1, 2, ..., n$.
Indicación: Use inducción sobre n. Para $(n+1)$ si $d = 2^{n+1}$, para todo índice i de x en la primera mitad de la expresión de la fila $n+1$, se tiene un índice $i + d$ de y en la segunda mitad, y viceversa.

Progresiones.

14. Calcular la suma de todos los múltiplos positivos de:
(a) 4 que son menores que 75.
(b) 6 que están entre 50 y 200.
(c) 3 que son menores que 99.

15. (a) Un número está formado por 5 dígitos en progresión aritmética. La suma de todos sus dígitos es 25 y la suma de los últimos tres dígitos es 12. Encuentre el número.
(b) La suma de tres números en progresión geométrica es 38 y su producto es 1728. Encuentre los números.

16. Si la diferencia d en una progresión aritmética es igual al doble del primer término, pruebe que la suma de los m primeros términos es a la suma de los n primeros términos como m^2 es a n^2.
17. Si π es el producto de n números en progresión artimética, S su suma y S' la suma de los recíprocos de dichos números, pruebe que $\pi^2 = (\frac{S}{S'})^n$.
18. Sea $(a_n)_{n\in\mathbb{N}}$ una progresión aritmética
    (a) Si $a_i = x, a_j = y, a_k = z$ para algunos $i, j, k \in \mathbb{N}$.
    Pruebe que $(j-k)x + (k-i)y + (i-j)z = 0$.
    (b) Pruebe que

$$\frac{1}{\sqrt{a_0}+\sqrt{a_1}} + \frac{1}{\sqrt{a_1}+\sqrt{a_2}} + ... + \frac{1}{\sqrt{a_{n-1}}+\sqrt{a_n}} = \frac{n}{\sqrt{a_0}+\sqrt{a_n}}$$

    (use inducción).
19. Sea la progresión geométrica $(b_n)_{n\in\mathbb{N}}$
    (a) Pruebe que $\sum_{k=1}^{n} \sqrt{b_{k-1}b_k} = \frac{\sqrt[2n]{b_o b_n}}{\sqrt[n]{b_o}-\sqrt[n]{bn}}(b_o - b_n)$.
    (b) Escriba en términos de la razón r, el valor de $\sum_{k=1}^{n} b_k b_{k+1}$.

*20. Una secuencia $(a_n)_{n\in\mathbb{N}}$ está en *progresión armónica* si la secuencia $(\frac{1}{a_n})_{n\in\mathbb{N}}$ es una progresión aritmética. Sea $(a_n)_{n\in\mathbb{N}}$ una progresión armónica de números positivos, pruebe que si $n \in \mathbb{N}, n > 1$, entonces $(a_{k+1})^n + (a_{k-1})^n > 2(a_k)^n$.

Coeficientes binomiales.

21. Pruebe que:
    (a) $\sum_{i=0}^{m} C_{n+i}^{i} = C_{n+m+1}^{m}, \quad \forall m \geq 0.$
    (b) $\sum_{k=0}^{n} (-1)^k C_n^k = 0.$
    (c) $C_{2n}^{n} + C_{2n}^{n-1} = \frac{1}{2} C_{2n+2}^{n+1}.$
    (d) $\sum_{k=0}^{n} (k+1)(C_n^k)^2 = \frac{(n+2)(2n-1)!}{n!(n-1)!}.$
    (e) $\sum_{k=0}^{n} \frac{(-1)^k C_n^k}{(k+2)(k+3)} = \frac{1}{(n+2)(n+3)}.$
22. Determine
    (a) El quinto término del desarrollo del binomio $(x-4)^{15}$.
    (b) El término central de $(a - \frac{1}{x})^{10}$.
    (c) El coeficiente que acompaña a x^7, en el desarrollo de $(x^3 + 3x)^9$.

23. (a) A partir de la igualdad $\{(1+x^2)^2 - 1\}^{2n} = x^{2n}(2+x)^{2n}$, demuestre que

$$C_{4n}^{2n} - C_{2n}^{1} C_{4n-2}^{2n} + C_{2n}^{2} C_{4n-4}^{2n} - ... = 4^n.$$

    (b) A partir de la identidad $\sum_{k=0}^{n} q^k = \frac{1-q^{n+1}}{1-q}$ pruebe que:

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

24. (a) Encuentre los valores de $n \in \mathbb{N}$ para los cuales C_n^k es impar, $k \in \{0, 1, ..., n\}$.
    (b) Demuestre (por inducción que): $\sum_{i=1}^{n} C_{m-1}^{i} = \sum_{j=1}^{n} C_{n-1}^{j}$.

* 25. (a) Pruebe que $(1+x)^n(1-x^2)^{-n} = (1-x)^{-n}$.
    (b) Deduzca de (a) que

$$\sum_{k=0}^{n} C_n^{j-2k} \cdot C_{n+k-1}^{k} = C_{n+j-1}^{j}.$$

* 26. Sean p y q reales positivos tales que $p + q = 1$. Demuestre que, si $r_k = C_n^k p^k q^{n-k}$, $\forall k = 0, ..., n$, entonces
    (a) $\sum_{k=0}^{n} k r_k = np.$
    (b) $\sum_{k=0}^{n} (k - np)^2 r_k = npq.$

* 27. Si $(1+x^2)^2(1+x)^n = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + ...$ y si $a_0, a_1, a_2, ...$ están en progresión aritmética, entonces existen sólo dos valores posibles para n. Encuéntrelos.

TEMAS CAPITULO II

1. Tallarines con salsa y/o tren al sur.
2. Partición de la Atlántida.
3. Fractal=Pascal.
4. Más recurrencias.

1. Tallarines con salsa y/o tren al sur.

De regreso de un Congreso, que se realizó en algún lugar del Sur, de cuyo nombre no quiero acordarme, un grupo de matemáticos reconfortan el estómago con tallarines a la Bolognesa, en el coche comedor del tren. En plena comida pasa el inspector y dice:

> "Lamento comunicarles que el servicio de baños no funciona. Y aquellos de entre ustedes que necesitan lavarse encontrarán servicios en cada estación."

Nuestros matemáticos, tan fecundos en astucias como en timidez, no se atreven a preguntar a sus colegas vecinos sobre el estado de sus caras y a la vez se ponen a discurrir si tienen o no la necesidad de lavarse y bajar en una de las estaciones del itinerario.
¿Qué va a suceder? El método inductivo permite demostrar la proposición:

P_n : *Si n matemáticos tienen la cara sucia, en la n-ésima estación los n bajarán a lavarse.*

En efecto, si hay un solo matemático y el inspector en su frase afirma que algunos (un) comensales (comensal) necesitan (necesita) lavarse entonces en la primera estación donde el tren se detenga el matemático descenderá a lavarse. Supongamos P_n verdadera (hipótesis de inducción) y demostremos para $n+1$, es decir los matemáticos $M_1, ..., M_{n+1}$ tienen la cara sucia. El matemático Dr. M_{n+1} ve en torno suyo n colegas con la cara sucia y piensa:

"Hay 2 casos posibles".
"O bien estoy limpio o bien sucio"

" Si estoy limpio ": los matemáticos sucios deberán bajar en la n-ésima estación para lavarse (por hipótesis de inducción).

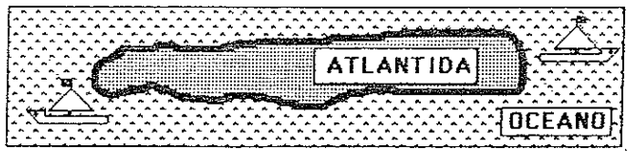
" Si estoy sucio ": Cada uno de mis colegas ve en torno suyo n rostros sucios y luego no bajan en la estación n-ésima esperando para saber el estado de su cara.

Luego, yo confirmo mi suciedad y ellos la suya, ergo, en la estación $n+1$ bajamos todos, luego, P_n es verdad $\forall n \in \mathbb{N}$ ∎

2. Partición de la Atlántida.

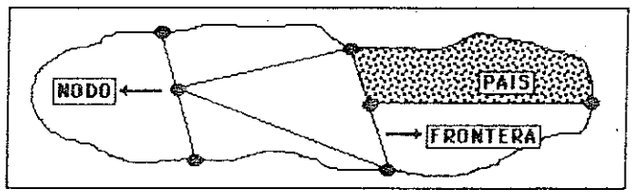
Fronteras y países.

Supongamos que se tiene un continente rodeado por el océano como en la figura:



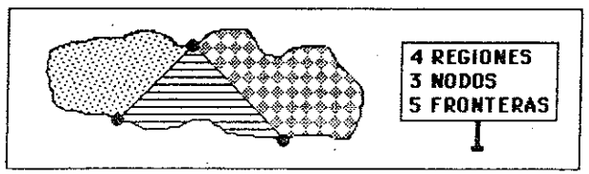
Este continente está dividido en países. Suponemos también que fuera de la frontera natural con el océano, existe al menos una "no natural" formando países (al menos dos).

La intersección de dos o más fronteras la denominaremos "nodo". Por ejemplo:



Además, prohibimos que existan países contenidos totalmente en otro.

Consideremos como regiones las superficies que forman países y el océano. Se verifica en la figura que sigue: $4+3=5+2$.

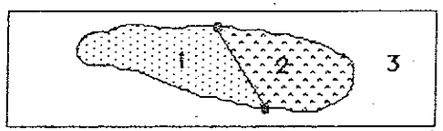


En general si notamos f = números de fronteras, p = número de regiones, n = número de nodos, se tiene:

Propiedad 1 (Teorema de Euler): $p+n=f+2$.

Demostración: por inducción sobre f.

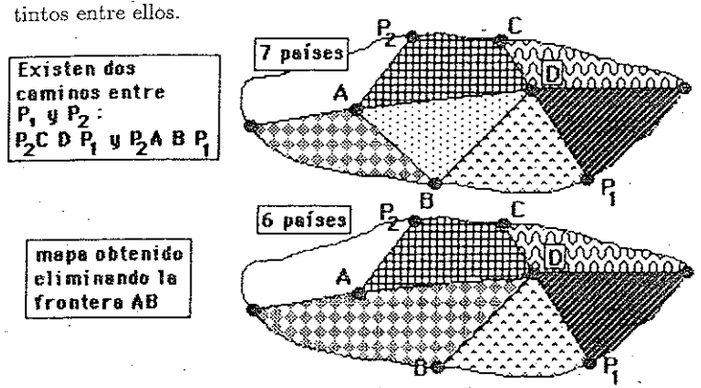
Para $f=3$ (caso de 2 países + océano)



$f=3 \Longrightarrow p=3,\ n=2$ de donde $5=3+2=5$.

Supongamos cierto para $f>3+y$ demostremos para $f+1$ fronteras.

Podemos ver que existen dos nodos P_1, P_2 tal que aceptan caminos distintos entre ellos.



$$\Longrightarrow f'=f-1, \quad n'=n, \quad p'=p-1,$$

luego, por hipótesis de inducción:

$$p'+n'=f'+2$$

$$\Longleftrightarrow p-1+n=f-1+2$$

$$p+n=f+2 \quad \blacksquare$$

Propiedad 2. Tomemos un mapa tal que cada nodo es la intersección de exactamente tres fronteras. Entonces existe una región (o país) con a lo más 5 fronteras.

Demostración:

Como cada nodo es la intersección de 3 fronteras, entonces:

$$3n = 2f.$$

Supongamos que cada país tiene a lo menos seis fronteras:

$$\sum_{i=1}^{p}(\ \#\ \text{fronteras país i}) \geq 6p;$$

como cada frontera se cuenta 2 veces:

$$f = \frac{1}{2}\sum_{i=1}^{p}(\ \#\ \text{fronteras país i})\ \geq \frac{6}{2}p = 3p,$$

por lo tanto,

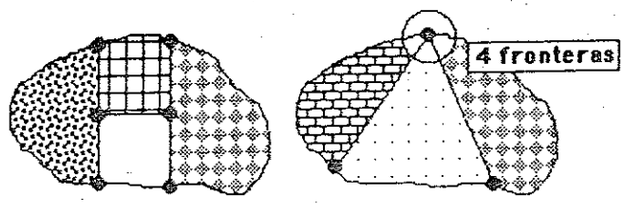
$$p + n \leq \frac{f}{3} + \frac{2f}{3} = f < f + 2,$$

lo cual es una contradicción con la propiedad 1 ■

Coloración de mapas.

Entenderemos como *coloración de un mapa* (incluyendo el mar) una asignación de colores a cada región tal que a dos regiones arbitrarias con frontera común se les asignen colores diferentes. El problema de colorear un mapa es antiguo y data al menos del siglo pasado y ha sido origen de una conjetura que sólo se "demostró" en la presente década mediante la utilización de métodos computacionales (aún hay controversias sobre la fiabilidad de una demostración con ayuda del computador ...). La conjetura dice que un mapa puede colorearse con a lo más cuatro colores. Este problema tan simple se ha revelado extremadamente difícil y buena parte del desarrollo de algunas teorías matemáticas se debe al interés por resolverlo. Acá daremos una demostración para un tipo de mapas particulares y en un contexto más débil.

Diremos que un mapa es *regular* si es una isla dividida en al menos dos países y tal que un nodo es la intersección exacta de tres fronteras. Por ejemplo:



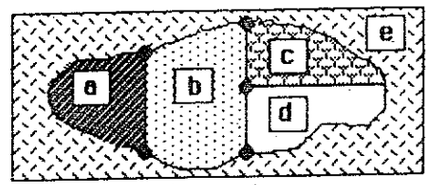
Regular No Regular

Teorema de los 5 colores :

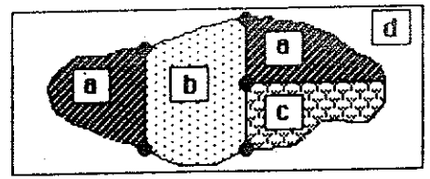
Bastan 5 colores para colorear (incluyendo el mar) cualquier mapa regular .

Demostración: por inducción sobre el número de regiones ó países.

Si el número de países es ≤ 5, obviamente se requieren a lo más 5 colores.



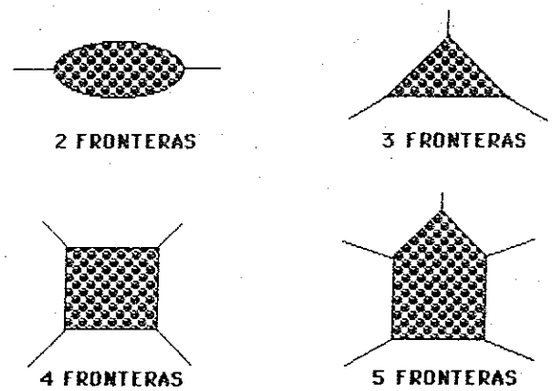
Coloración para cinco países con 5 colores



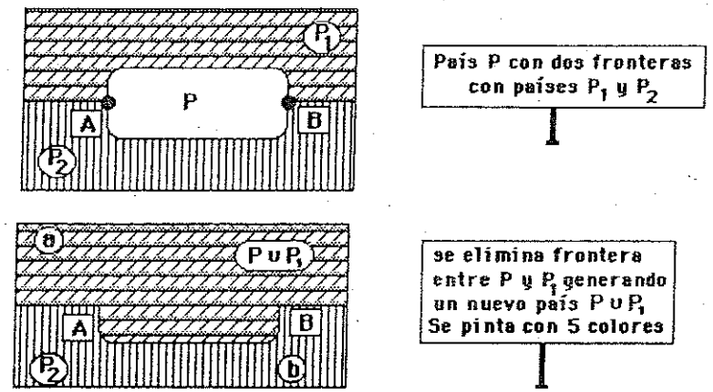
Coloración mejorada para el mismo mapa pero con 4 colores

Supongamos el teorema verdadero para un mapa normal con $p \geq 5$ regiones o países y demostremos para $p + 1$:

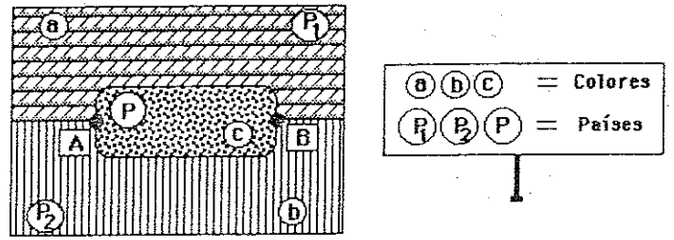
Si $p + 1 > 5$, como el mapa es normal, de la propiedad 2 sabemos que existe alguna región con a lo más cinco fronteras. Se tienen varios casos:



Caso 1. Eliminamos la frontera entre P y P_1 (con lo cual desaparecen los nodos A y B). Luego el mapa sigue siendo normal pero con $p' = p$ regiones. Por hipótesis de inducción podemos colorearlo con 5 colores.

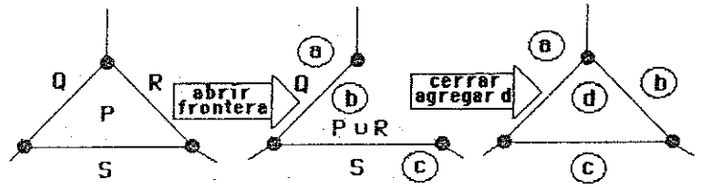


Posteriormente colocamos nuevamente la frontera entre P y P_1, y le asignamos un color $c \neq a$ y $c \neq b$



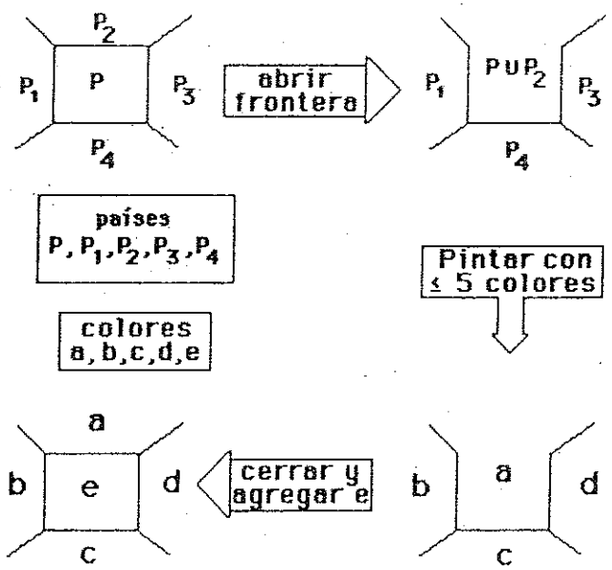
Luego, el mapa con $p+1$ regiones admite una coloración con ≤ 5 colores.

Caso 2. Análogamente al caso anterior:

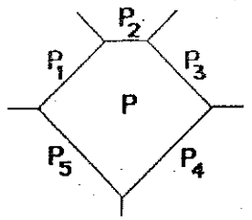


Al abrir la frontera aplicamos la hipótesis de inducción y coloreamos con a lo más 5 colores. Suponemos que los países limítrofes de P tienen los colores a, b, c. Se cierra nuevamente la frontera agregando un color $d \neq a, b, c$

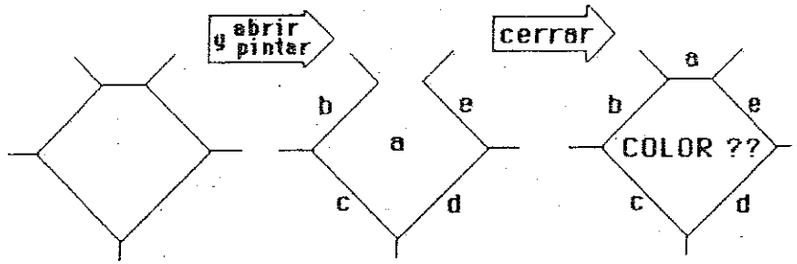
Caso 3. Se tiene:



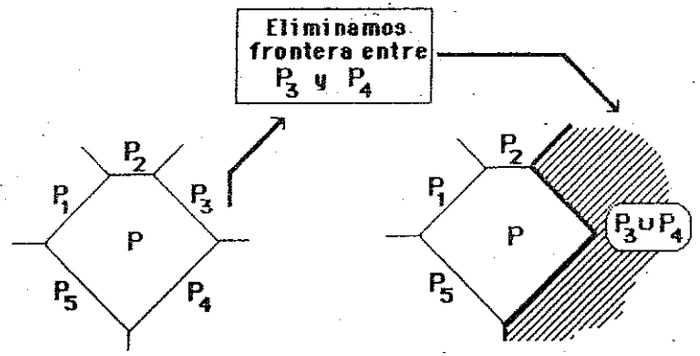
Caso 4. Se tiene:



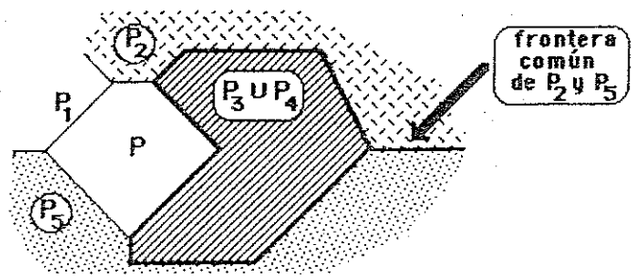
Aquí el problema es más delicado. Si realizamos directamente el procedimiento anterior; por ejemplo:



Con lo cual deberíamos utilizar un sexto color. Para evitar esto debemos demostrar que entre los 5 países fronterizos existe al menos una pareja que no tiene frontera común.
Supongamos por un momento que $P_3 \cup P_4 = P'$ es una sola región:

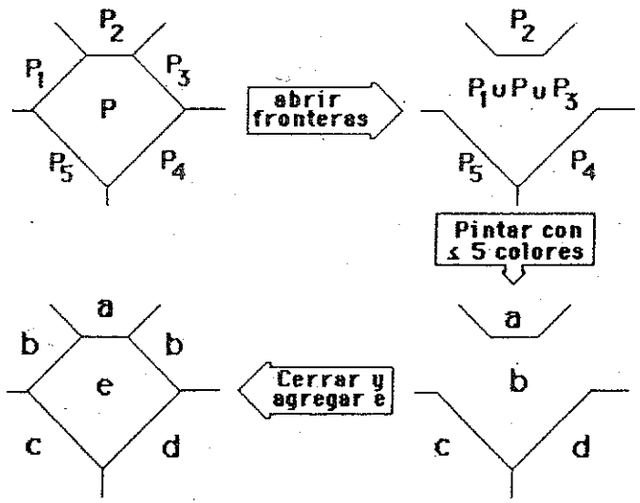


Supongamos, por ejemplo, que P_2 y P_5 tienen frontera común:



Entonces P_1 y $P_3 \cup P_4$ no tienen frontera común y luego (P_1, P_3) (P_1, P_4) no tienen fronteras comunes.

De manera análoga se demuestra que si P_1 y $P_3 \cup P_4$ tienen frontera común entonces (P_2, P_5) no la tienen. Luego, podemos economizar un color, ya que entre los 5 países vecinos existen al menos dos sin fronteras comunes. Supongamos que éstos sean P_1 y P_3. Realizando ahora un procedimiento un poco más sofisticado, eliminamos dos fronteras:



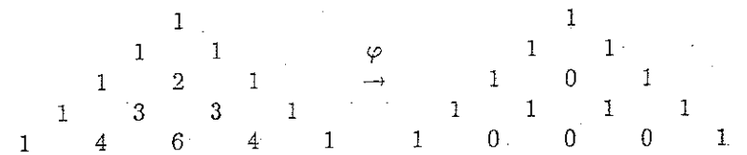
con lo cual demostramos el teorema ■

3. Fractal=Pascal.

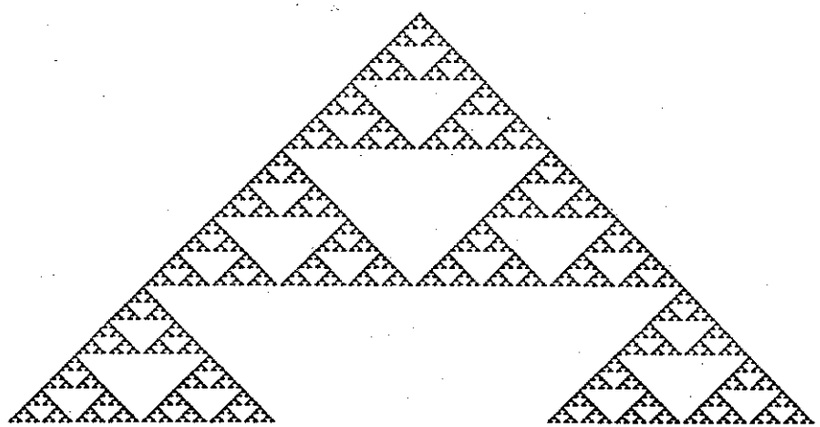
Una aplicación artística del triángulo de Pascal es la siguiente:
Asociemos a los coeficientes binomiales los valores 0 y 1 como sigue:

$$\varphi(C_n^k) = \begin{cases} 0 & \text{si } C_n^k \text{ es par} \\ 1 & \text{si } C_n^k \text{ es impar.} \end{cases}$$

Es decir:



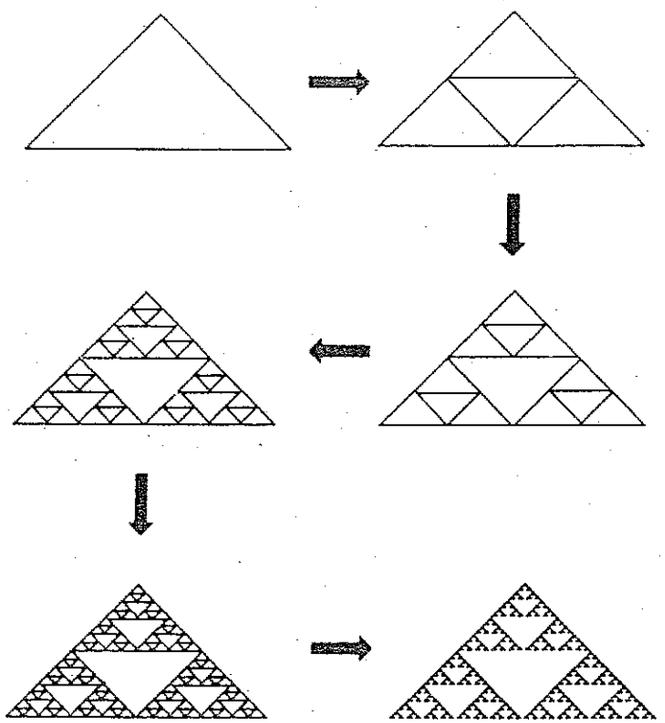
Si esto lo llevamos a un programa computacional y escribimos en la pantalla un punto negro para el valor 1 y un punto blanco para 0, se obtiene la figura siguiente:



Una pregunta interesante es saber, dado $k, n \in \mathbb{N}$, si el punto correspondiente en el triángulo es blanco o negro. Es decir, cuando C_n^k es par o impar. La respuesta no es trivial.

Además puede verse, al menos visualmente, que el triángulo de paridad obedece a la construcción geométrica siguiente:

Se toma un triángulo y se parte reiteradamente en triángulos más pequeños, de acuerdo al procedimiento siguiente:

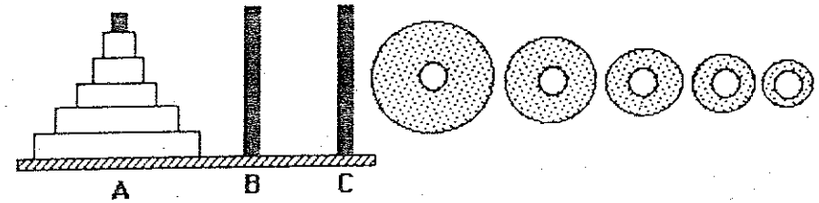


Si usted compara el triángulo generado en la figura anterior con la regla "par-impar" del triángulo de Pascal, verá que los dos procedimientos arrojan un resultado similar: ambos engendran una progresión de triángulos cada vez más pequeños. Objetos de esta naturaleza, puestos a la moda por el matemático B. Mandelbrot, gozan actualmente de excelente salud y popularidad y se les denomina *fractales*.

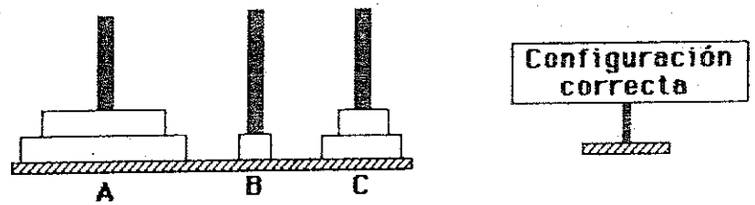
4. Más recurrencias.

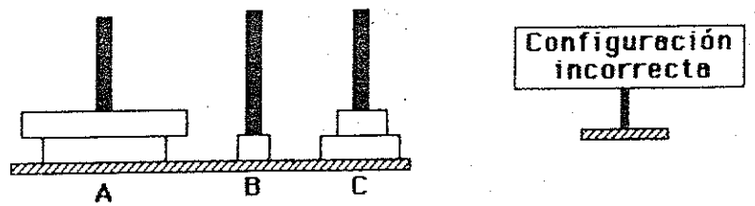
4.1 Torre de Hanoi.

Se tienen tres postes $\{A, B, C\}$ y n discos de diámetro decreciente. Inicialmente todos los discos están ordenados (de diámetro mayor a menor) en el poste A, como en la figura siguiente:

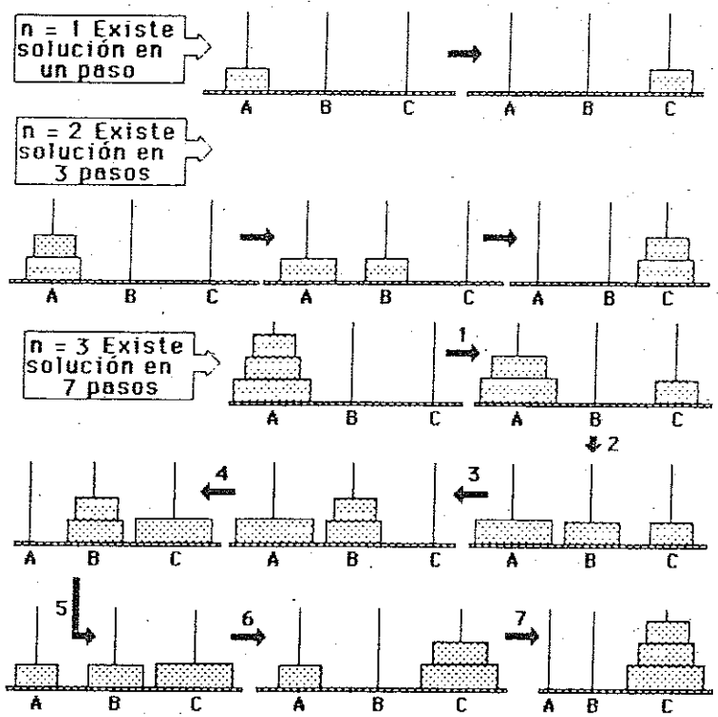


El problema consiste en determinar un procedimiento (si existe) para trasladar, uno a uno, los n discos de un poste a otro (digamos desde A hasta C) de manera que en cada paso (traslado de un disco), se respete la regla de que un disco de mayor diámetro no puede ponerse sobre otro de diámetro menor.



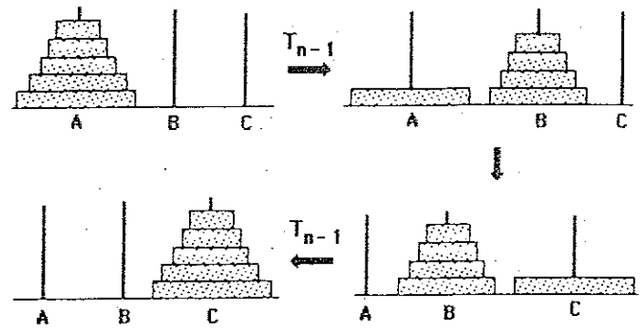


Desarrollaremos el procedimiento para $n = 1, 2, 3$:



Conviene analizar el caso $n = 3$: Los pasos 1,2,3 consisten solamente en repetir el caso $n = 2$, sin mover el disco mayor. El paso 4 consiste en cambiar el disco mayor al poste C (donde deseamos ubicarlo) y el resto es realizar nuevamente el caso $n = 2$. Esto nos permite determinar, de manera inductiva, un procedimiento general:

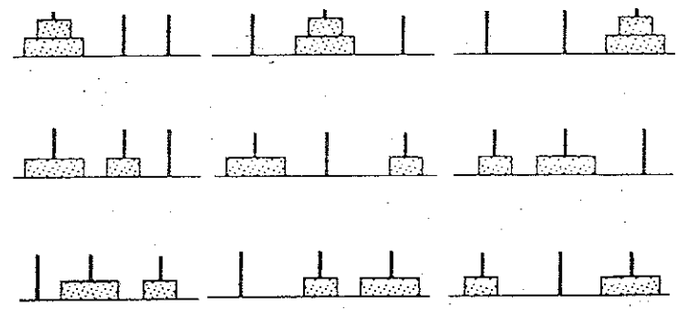
Dado n discos, primero trasladamos $n-1$ del poste A al poste B luego trasladamos el mayor al poste C y posteriormente los $n-1$ de B a C como sigue:



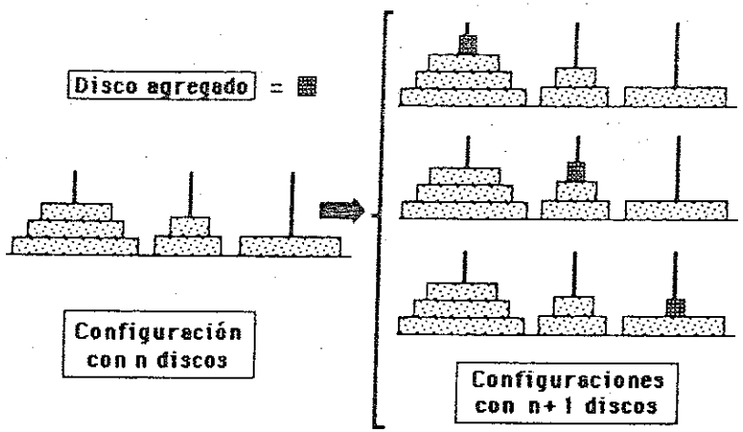
Veamos esto por inducción: conocemos un procedimiento para $n = 2$. Suponiéndolo conocido para n es posible para $n+1$, según el esquema anterior. Luego, el problema tiene solución para cualquier número de discos. (¡ Solución que hemos determinado de manera constructiva!).

Ahora bien, otra pregunta interesante es cuántos pasos demoramos en obtener la solución y si nuestra estrategia es la mejor posible (en el sentido que se obtiene la solución en el menor número de pasos).

Veamos primero cuánto es lo máximo que podríamos demorarnos: el peor caso sería recorrer todas las configuraciones permitidas posibles. ¿Cuántas hay? Para $n = 2$ hay 9:



Sea U_n el número de configuraciones posibles con n discos. Para $n+1$ discos tomamos cualquier configuración de n y le agregamos en cualquier posición un disco de diámetro inferior.



Luego a cada configuración de n discos le asociamos tres configuraciones de $n+1$ de donde: $U_{n+1} = 3U_n$, $U_1 = 3$ Claramente:

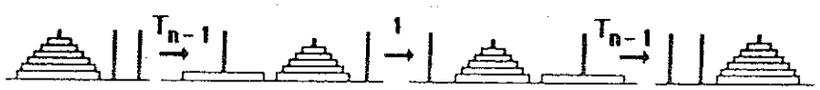
$$U_{n+1} = 3U_n = 3^2U_{n-1} = 3^3U_{n-2} = \cdots = 3^{n+1}.$$

Concluímos entonces que nuestro procedimiento debería terminar en a lo más 3^n pasos para n discos.

Sea T_n = número mínimo de pasos para trasladar n discos de un poste a otro.
Claramente $T_0 = 0, \quad T_1 = 1.$
De nuestro procedimiento inductivo es claro que podemos trasladar $n+1$ discos en a lo más $2T_n + 1$. Luego el número mínimo de pasos para $n+1$ verifica:

$$T_{n+1} \leq 2T_n + 1; \quad T_0 = 0.$$

Por otra parte, dado $n+1$ discos, cada vez que cambiamos de poste el disco de diámetro mayor se debe tener el siguiente esquema:



Es decir, haber sacado los otros n discos que están encima (en T_n pasos que es el tiempo mínimo) y luego cambiar el $n+1$. Posteriormente debemos aún poner los n discos sobre el mayor en T_n pasos. Luego, como al menos debemos mover el disco de diámetro mayor 1 vez $\Longrightarrow T_{n+1} \geq T_n + 1 + T_n = 2T_n + 1$ de donde obtenemos la ecuación recursiva de los tiempos mínimos:

$$T_{n+1} = 2T_n + 1, \qquad T_0 = 0.$$

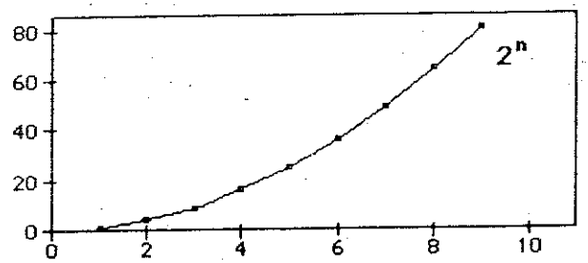
n	0	1	2	3	4	$\cdots$
T_n	0	1	3	7	15	$\cdots$
	2^0-1	2^1-1	2^2-1	2^3-1	2^4-1	$\cdots$

Luego la solución, dada en forma cerrada (es decir en función de n) de la recurrencia es :

$$T_n = 2^n - 1 \qquad n \geq 0.$$

En efecto $2^{n+1} = 2(2^n - 1) + 1$.

Concluímos entonces que el mejor procedimiento para obtener una solución requiere un número grande (exponencial) de pasos. Además cuando n crece, el mínimo de pasos crece extremadamente rápido.



Suponiendo que el cambio de un disco nos tome $1[seg]$, cuando se tienen 30 discos nos demoraríamos aproximadamente ¡ cinco siglos! (verificar).

Una observación importante entonces es que cuando deseamos realizar un procedimiento que involucre pasos elementales (como en este caso particular) nos agradaría que el número de pasos no creciera demasiado rápido con n, es decir $T_n = cn$, ó $T_n = cn^2$ pero no cosas del estilo n^n, 2^n, 3^n, etc.

Otra consideración : La determinación de la fórmula cerrada de $T_n = 2^n - 1$, la hicimos "al ojo".

Una manera menos fortuita podría ser: dada esta ecuación, hacer el cambio de variables: $V_n = T_n + 1$ obteniéndose:

$$V_{n+1} = 2V_n, \qquad V_1 = 2,$$

que es una progresión geométrica de razón 2. Luego:

$$V_{n+1} = 2^2 V_{n-1} = 2^3 V_{n-2} = \cdots = 2^n V_1 = 2^{n+1},$$

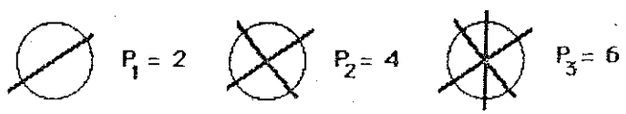
de donde

$$T_{n+1} = 2^{n+1} - 1 \quad \blacksquare$$

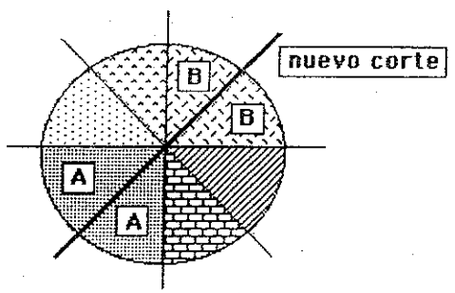
4.2 Variaciones sobre trozos de pizza.

Dada una pizza circular: ¿Cuántos trozos de pizza generamos con n cortes no colineales, con intersección común en el centro de la pizza?

Sea P_n el número de porciones para $n \geq 1$. Para valores pequeños de n se tiene:



Supongamos $n-1$ cortes con P_n trozos y agreguemos un corte:



El nuevo corte divide en dos porciones dos trozos, (digamos A y B) luego el número de trozos para n cortes es:

$$P_n = P_{n-1} + 2, \quad P_1 = 2, \quad n \geq 2.$$

Sumando las diferencias:

$$\sum_{i=2}^{n} (P_i - P_{i-1}) = \sum_{i=2}^{n} 2.$$

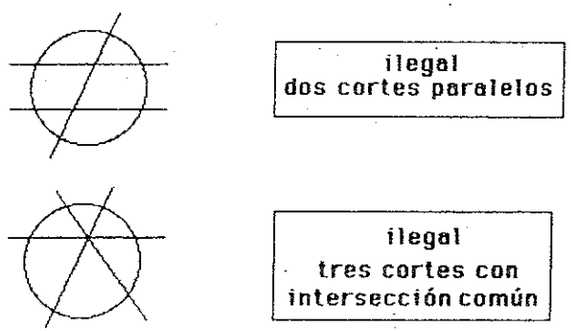
de donde

$$P_n - P_1 = 2(n-1) \Longrightarrow P_n = 2n - 2 + P_1 = 2n,$$

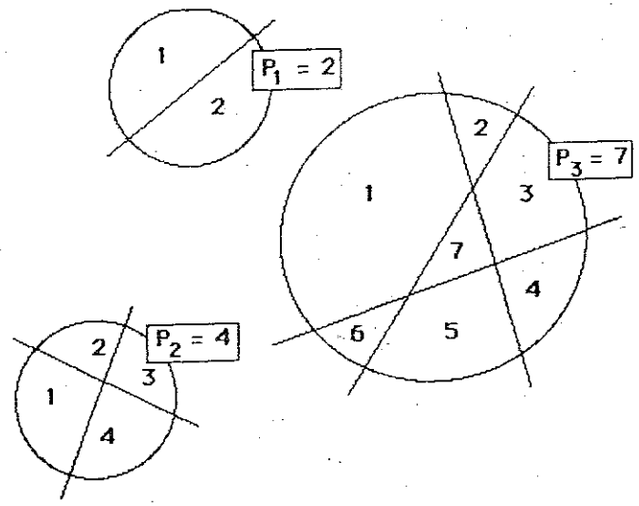
por lo tanto

$$P_n = 2n, \quad n \geq 1 \quad \blacksquare$$

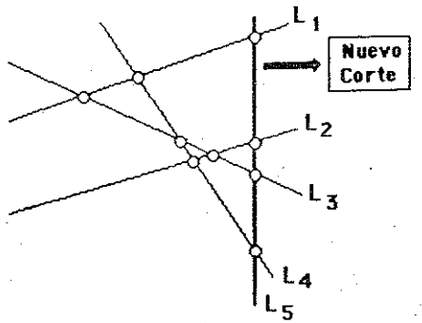
Compliquemos un poco la distribución de la pizza. Supongamos que los cortes no se intersectan necesariamente en el centro. Más aún, los comensales (que son los mismos matemáticos del tren al sur) exigen que no se permitan cortes paralelos y entre tres o más cortes no se tengan intersecciones comunes:



¿ Cuántas porciones se generan entonces con n cortes? Sea L_n este número. Para $n = 1$ y 2 :



Es fácil ver que dado $n-1$ cortes en las condiciones anteriores, al agregar un corte (como éste no coincide con otros puntos de intersección y no es paralelo a otro) la nueva recta ℓ_n corta todos los otros en $n-1$ nuevos puntos:



y éstos generan n nuevas regiones.

Se tiene entonces:

$$L_n = L_{n-1} + n, \qquad L_1 = 2, \quad n \geq 2,$$

o bien:

$$L_j - L_{j-1} = j;$$

sumando

$$\sum_{j=2}^{n} (L_j - L_{j-1}) = \sum_{j=2}^{n} j$$

se obtiene:

$$L_n - L_1 = \sum_{j=2}^{n} j,$$

como $L_1 = 2$:

$$L_n = \sum_{j=1}^{n} j + 1,$$

obteniéndose la fórmula cerrada:

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

Ejercicios.

1. ¿Qué podría decir si cada corte fuese hecho con un cuchillo en forma de V sobre una pizza que cubriese todo el plano?
2. En el caso en que la pizza se reparte mediante cortes, entre los cuales no hay dos paralelos ni tres que se intersecten en un mismo punto ¿Cuántos puntos de intersección tienen estos cortes?
3. Supongamos que deseamos repartir una pizza rectangular (como aquellas, frente al Duomo de Florencia ...). Para ello marcamos en el borde superior n puntos y en el borde inferior m puntos. ¿Cuántos cortes triangulares se pueden hacer, cuyos vértices sean estos puntos?
4. Distingamos en una pizza circular dos puntos interiores A y B, de manera que si realizamos n cortes, de ellos p cortes pasan por A y q cortes pasan por B, y además no hay tres que pasen por un mismo punto; ninguno que pasa por ambos puntos A y B y ningún par de cortes paralelos. ¿Cuántos trozos se obtienen?
5. Si ahora, lo que deseamos repartir es un queque Pantagruélico (que cubre todo el espacio), el cual podemos cortar en cualquier dirección, según planos entre los cuales no hay dos paralelos, ni tres que pasen por una misma recta, ni cuatro que pasen por un mismo punto. ¿Cuántos trozos puede conseguir con n cortes?

4.3 Números de Fibonacci.

Durante la Edad Media (1202) en el libro *Liber Abacci*, el matemático Leonardo de Piza presentó el problema siguiente: ¿ Cuántos pares de conejos puede engendrar una sola pareja durante un año? Para dar una respuesta Leonardo de Pizza planteó la recurrencia siguiente: si f_n es el número de pares de conejos en el año n :

$$f_n = f_{n-1} + f_{n-2} \quad n \geq 2, \quad f_0 = f_1 = 1.$$

Esta sucesión tiene innumerables propiedades y aplicaciones, incluso existe una revista científica de circulación internacional que está dedicada completamente a ella. Buscaremos su solución entre las progresiones geométricas $(q^n)_{n\geq 0}$. Supongamos entonces que la solución es del tipo:

$$q^n = q^{n-1} + q^{n-2},$$

de donde:

$$q^2 = q + 1.$$

Las raíces de esta ecuación cuadrática son

$$\alpha = \frac{1+\sqrt{5}}{2}, \qquad \beta = \frac{1-\sqrt{5}}{2}.$$

Tenemos entonces dos progresiones geométricas:

$$(\alpha^n)_{n\geq 0}, \qquad (\beta^n)_{n\geq 0}.$$

Si tomamos dos constantes $c_1, c_2 \in \mathbb{R}$ y reemplazamos $c_1\alpha^n + c_2\beta^n$ en la expresión $\psi = q^n - q^{n-1} - q^{n-2}$ se obtiene:

$$\begin{aligned}\psi &= c_1\alpha^{n+1} + c_2\beta^{n+1} - (c_1\alpha^{n-1} + c_2\beta^{n-1} + c_1\alpha^{n-2} + c_2\beta^{n-2}) \\ &= c_1[\alpha^n - \alpha^{n-1} - \alpha^{n-2}] + c_2[\beta^n - \beta^{n-1} - \beta^{n-2}] \\ &= c_1\alpha^{n-2}(\alpha^2 - \alpha - 1) + c_2\beta^{n-2}(\beta^2 - \beta - 1);\end{aligned}$$

como α, β son raíces de $x^2 - x - 1$ se obtiene $\psi = 0$, es decir $c_1\alpha^n + c_2\beta^n$ es solución general de la recurrencia de Fibonacci.

Calculemos el valor de los constantes:

$$\begin{aligned} n = 0: \quad & c_1\alpha^0 + c_2\beta^0 = 1 \qquad & c_1 + c_2 = 1 \\ & \iff & \\ n = 1: \quad & c_1\alpha + c_2\beta = 1 \qquad & c_1\alpha + c_2\beta = 1, \end{aligned}$$

obteniendo

$$c_1 = \frac{1+\sqrt{5}}{2\sqrt{5}}; \quad c_2 = -\frac{1-\sqrt{5}}{2\sqrt{5}},$$

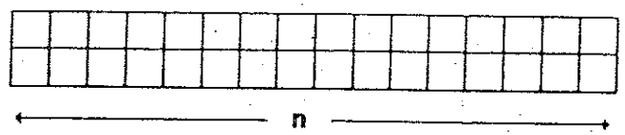
con lo cual, la solución general de la recurrencia es

$$f_n = \frac{(\frac{1+\sqrt{5}}{2})^n - (\frac{1-\sqrt{5}}{2})^n}{\sqrt{5}}.$$

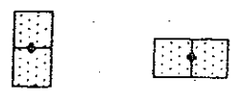
Esta expresión se conoce también como la *fórmula de Binet.*

Embaldosados $2 \times n$.

Una hermosa aplicación de la recurrencia de Fibonacci es la siguiente: Dado un tablero de 2 filas y n columnas:

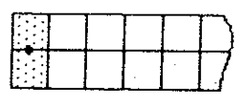


¿De cuántas maneras podemos embaldosarlo con n piezas de dominó?

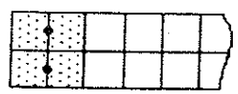


Sea x_n el número de maneras para un tablero de $2 \times n$. Es vital advertir que los dos primeros cuadrados del extremo izquierdo sólo pueden cubrirse de dos maneras:

(a) con una pieza de dominó.



(b) con dos piezas de dominó.



Para completar cualquier embaldosado de tipo (a) se requiere cubrir el tablero restante de dimensión $2 \times (n-1)$ con $n-1$ piezas. Análogamente,

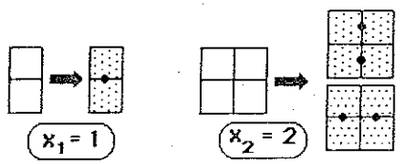
en el caso (b) se requiere cubrir el tablero restante de $2 \times (n-2)$ con $n-2$ piezas. El número de maneras de hacerlo es x_{n-1} y x_{n-2} respectivamente. Como un embaldosado de (a) es siempre distinto de uno de (b), obtenemos la recurrencia:

$$x_n = x_{n-1} + x_{n-2} \qquad \forall n \geq 2,$$

con las condiciones iniciales:

para un tablero de $2 \times 1 \Rightarrow x_1 = 1$,

para un tablero de $2 \times 2 \Rightarrow x_2 = 2$.



Obteniendo la sucesión

$$1, 2, 3, 5, 8, 13, 21, 34, ...$$

Es claro que esta recurrencia es similar a la de Fibonacci, salvo en la condición inicial

$$f_n = f_{n-1} + f_{n-2}, f_1 = f_2 = 1 \qquad \forall n \geq 2$$

$$1, 1, 2, 3, 5, 8, 13, 21, 34, ...$$

luego $x_n = f_{n+1} \quad \forall n \geq 1$.

Utilizando la fórmula de Binet:

$$x_n = f_{n+1} = \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^{n+1} - (\frac{1-\sqrt{5}}{2})^{n+1}) \quad \blacksquare$$

Ejercicios.

Consideremos $(f_n)_{n\geq 1}$ la sucesión de Fibonacci con $f_0 = f_1 = 1$. Demuestre,

1. $\sum_{i=0}^{n} f_i = f_{n+2} - 1$.

2. $\sum_{i=1}^{n} f_{2i-1} = f_{2n} - 1$.
3. $\sum_{i=0}^{n} f_{2i} = f_{2n+1}$.
4. $\sum_{i=0}^{n} f_i^2 = f_n \cdot f_{n+1}$.
5. $f_{n+m} = f_{n-2} f_m + f_n, f_{m+1}$.
6. $f_{n+5} > 10 f_n$.

* 7. $f_{n-1} \cdot f_{n+1} - f_{n-2} \cdot f_{n+2} = 2(-1)^{n+1}$.

8. Sea $a_n = (3+\sqrt{5})^n + (3-\sqrt{5})^n, n \in I\!N$ Pruebe que $a_n \in I\!N \quad \forall n$. Indicación: Muestre que $a_{n+1} = 6a_n - 4a_{n-1}$.
9. Luego de n días de un experimento con moscas de la fruta, el número $M(n)$ de moscas satisface $M(n) = 3M(n-1) - 2M(n-2)$, $\forall n \geq 2$. con $M(0) = 3$, $M(1) = 7$. Determine una solución de la recurrencia.

CAPITULO III

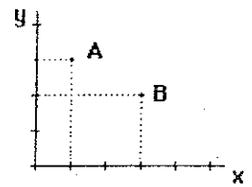
Estoy en medio de un triángulo
(bolero)

RELACIONES

En el capítulo I definimos la noción de conjunto, pero éste es un objeto amorfo. Podríamos verlo como una bolsa donde se colocan objetos sin importar el orden, cuya única característica es estar o no en la bolsa. En matemáticas y en la vida diaria son importantes los ordenamientos o el orden entre objetos, noción que no es capturada por los conjuntos. Por ello introduciremos en este capítulo elementos matemáticos que recuperan la noción intuitiva de orden, permitiendo estructurar objetos de acuerdo a la relación que tienen entre ellos.

3.1 Pares ordenados y n-tuplas.

Recordemos el eje cartesiano usual



El punto A tiene como primera coordenada 1 y segunda coordenada 3. Esto se escribe $A = (1, 3)$. De manera análoga $B = (3, 2)$. Conviene señalar que no es lo mismo (2,3) que (3,2) ambos son puntos distintos en el plano. De esto podemos deducir que es importante la posición de cada coordenada, es decir *importa el orden.*

En términos abstractos diremos que, dados dos objetos arbitrarios a y b, el *par ordenado* (a, b) es una lista ordenada de ambos objetos.

Claramente, dados a y b podemos construir cuatro pares ordenados:

$$(a,a),(a,b),(b,a),(b,b)$$

los cuales son distintos; no da lo mismo escribir primero a seguido de b que b seguido de a: $(a,b) \neq (b,a)$.

Diremos que dos pares ordenados son *iguales* si tienen coordenadas iguales:

$$(a,b) = (c,d) \Longleftrightarrow (a = c) \ \wedge \ (b = d) \tag{3.1}$$

Conviene señalar que podríamos haber definido los pares ordenados a partir de la teoría de conjuntos:

$$(a,b) = \{\{a\},\{a,b\}\},$$

en particular:

$$(a,a) = \{\{a\},\{a,a\}\} = \{\{a\},\{a\}\} = \{\{a\}\}.$$

Esto permite distinguir, en cuanto a orden (a,b) de (b,a). En efecto, $(b,a) = \{\{b\},\{a,b\}\} \neq \{\{a\},\{a,b\}\} = (a,b)$.

De manera más general, dados n objetos arbitrarios $\{a_1\}_{i=1}^n = \{a_1, a_2, ..., a_n\}$ definimos la *n-tupla* como una lista ordenada de estos n objetos:

$$(a_1, a_2, a_3, ..., a_{n-1}, a_n).$$

Además, diremos que dos n-tuplas son iguales:

$$(a_1, ..., a_n) = (b_1, ..., b_n) \Longleftrightarrow (a_i = b_i) \ (\forall i = 1, ..., n) \tag{3.2}$$

Por ejemplo, dado el conjunto $\{0,1\}$, determinemos todas las 3-tuplas (o tríos), cuyos elementos sean 0 o 1:

$$(0,0,0),(0,0,1),(0,1,0),(0,1,1),(1,0,0),(1,0,1),(1,1,0),(1,1,1)$$

Para n grande este tipo de problema no es trivial, por ello es conveniente definir conjuntos que contengan todas las n-tuplas.

3.2 Productos cartesianos.

Dados A, B dos conjuntos arbitrarios, diremos que el *producto cartesiano* entre A y B, que notaremos $A \times B$, es la colección de todos los pares ordenados formados con un primer elemento en A y un segundo elemento en B. En lenguaje de conjuntos:

$$A \times B = \{(a,b)/(a \in A) \wedge (b \in B)\} \tag{3.3}$$

de manera equivalente:

$$(x,y) \in A \times B \Longleftrightarrow (x \in A) \wedge (y \in B).$$

En general, dada una colección $\{A_i\}_{i=1}^n = \{A_1, ..., A_n\}$ de conjuntos se define su producto cartesiano como la colección de todas las n-tuplas donde la primera componente pertenece a A_1, la segunda a A_2, ..., la n-ésima a A_n. Formalmente

$$\times_{i=1}^n A_i = A_1 \times A_2 \times ... \times A_n = \{(a_1, ..., a_n)/a_i \in A_i, 1 \leq i \leq n\} \tag{3.4}$$

o bien:

$$(x_1, ..., x_n) \in \times_{i=1}^n A_i \Longleftrightarrow x_i \in A_i \quad 1 \leq i \leq n.$$

En el caso particular de que todos los conjuntos A_i sean iguales a un conjunto A ($A_i = A, \forall i = 1, ..., n$):

$$A \times ... \times A = A^n = \{(a_1, ..., a_n)/a_i \in A \quad 1 \leq i \leq n\}.$$

Por ejemplo, $\{0,1\}^n = \{0,1\} \times \{0,1\} \times ... \times \{0,1\}$ es el conjunto de todas las n-tuplas con componentes 0 ó 1, también llamado "hipercubo n-dimensional".

Del hecho que (a,b) es usualmente distinto de (b,a) se desprende que en general $A \times B \neq B \times A$. Sean $A = \{a,b\}$ y $B = \{1,2,3\}$ se tiene:

$$A \times B = \{(a,1),(a,2),(a,3),(b,1),(b,2),(b,3)\}$$

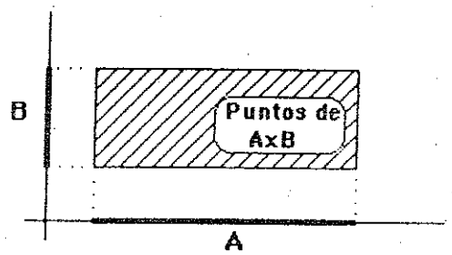
$$B \times A = \{(1,a),(1,b),(2,a),(2,b),(3,a),(3,b)\}$$

de donde concluímos, vía un contraejemplo para la igualdad, que $A \times B \neq B \times A$.

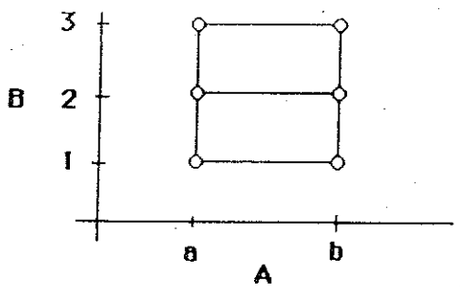
Otras propiedades del producto cartesiano aparecen en los ejercicios propuestos.

Algunos productos usuales son $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2 = \{(x,y)/x,y \in \mathbb{R}\}$ correspondiente a los puntos del plano. $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z} = \{(x,y)/x,y \in \mathbb{Z}\}$ correspondiente a los puntos del plano con coordenadas enteras.
$\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ correspondiente a los puntos del espacio tri-dimensional, $\mathbb{Z}^3 = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$, los puntos de coordenadas enteras en tres dimensiones y $\{0,1\}^3$, el cubo tri-dimensional.

Podemos representar (como los casos de $\mathbb{R}^2$ y $\mathbb{Z}^2$) un producto cartesiano de la manera siguiente:



En el ejemplo anterior:



Concluímos del dibujo que, en el caso finito (A y B con un número finito de elementos) el número de pares ordenados es igual al área del rectángulo así formado. En general para dos conjuntos de cardinalidad finita:

$$|A_1 \times A_2| = |A_1| \cdot |A_2|$$

En efecto, sean $A_1 = \{a_1,...,a_n\}, A_2 = \{b_1,...,b_m\}$, es decir $|A_1| = n$ y $|A_2| = m$. Se tiene entonces la tabla siguiente de todos los pares ordenados de $A_1 \times A_2$:

$$\begin{array}{llll} (a_1,b_1), & (a_1,b_2), ..., (a_1,b_m) & & \\ (a_2,b_1), & (a_2,b_2), ..., (a_2,b_m) & & \\ & & & n \quad \text{filas} \\ (a_n,b_1), & (a_n,b_2), ..., (a_n,b_m) & & \end{array}$$

$$m \quad \text{columnas}$$

que contiene nm pares ordenados. En general, utilizando inducción se puede demostrar que dados los conjuntos $A_1,...,A_n$ de cardinalidad finita:

$$|A_1 \times A_2 \times ... \times A_n| = \prod_{i=1}^{n} |A_i| \tag{3.5}$$

La noción de producto cartesiano es útil para *contar* objetos. Por ejemplo, si las patentes de automóviles se componen de dos letras y tres dígitos. ¿Cuántas patentes distintas pueden formarse de manera que las letras ocupen las dos primeras posiciones y los dígitos las tres últimas?

Los conjuntos de letras y dígitos son los siguientes: $L = \{a,b,c,...,y,z\}$, $D = \{0,1,...,9\}$. Claramente, una patente de automóviles corresponde a una 5-tupla de $L \times L \times D \times D \times D = L^2 \times D^3$ y el número de patentes distintas es el cardinal del producto cartesiano:

$$\#\text{ patentes } = |L^2 \times D^3| = 26^2 \times 10^3 = 676.000.$$

En el caso de que dígitos y letras ocupen cualquier posición, el número sería

$$C_5^2 \cdot |L^2 \times D^3| = 10 \times 676.000 = 6.760.000.$$

En efecto, basta ver en cuántas posiciones distintas pueden colocarse las dos letras y para cada caso calcular el número de patentes con posición fija

de letras:

L	L	D	D	D	$\lvert L^2 \times D^3 \rvert$
L	D	L	D	D	$\lvert L^2 \times D^3 \rvert$
L	D	D	L	D	.
L	D	D	D	L	.
D	L	L	D	D	.
D	L	D	L	D	.
D	L	D	D	L	.
D	D	L	L	D	.
D	D	L	L	L	.
D	D	D	L	L	$\lvert L^2 \times D^3 \rvert$

3.3 Relaciones binarias.

La noción intuitiva de relación entre objetos surge continuamente en la vida diaria y ha aparecido ya en este libro. Por ejemplo:

Pedro es padre de Javier
Javier es hijo de Pedro
5 es igual a 5
Javier es menor que Pepo
Pepo es mayor que Pangolín
cuatro es mayor que cero
a pertenece a A, $(a \in A)$
b no pertenece a A, $(b \notin A)$
Geguén, Tchuente y Tacaná son cameruneses... etc.

En todas las sentencias anteriores tenemos relaciones entre objetos, en algunos casos son de ordenamiento, en otros de igualdad, en otros de pertenencia. La característica común de todas ellas es que son relaciones entre dos elementos y en tal sentido las denominaremos *relaciones binarias*. En este párrafo formalizaremos esta noción para, posteriormente, clasificar las relaciones binarias.

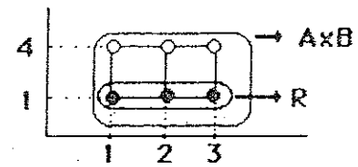
Dados dos conjuntos arbitrarios A y B no vacíos, una *relación binaria* $\mathcal{R}$ es un subconjunto no vacío de pares ordenados $R \subseteq A \times B$. Si $(a,b) \in R$ diremos que a está *relacionado* con b y notaremos $a\mathcal{R}b$:

$$\begin{aligned} a\mathcal{R}b &\Leftrightarrow (a,b) \in R \Leftrightarrow \text{“}a \text{ está relacionado con } b\text{”} \\ a\mathcal{R}b &\Leftrightarrow (a,b) \notin R \Leftrightarrow \text{“}a \text{ no está relacionado con } b\text{”} \end{aligned} \tag{3.6}$$

El conjunto de pares ordenados de $A \times B$ cuyos elementos están relacionados es el *dominio* de la relación $\mathcal{R}$, y se denota R.

Ejemplos:

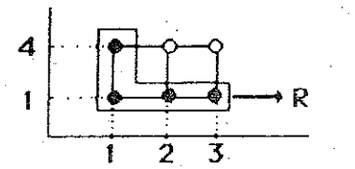
1) Sea A=$\{1,2,3\}$; B=$\{1,4\}$ y la relación $\mathcal{R}$ dada por R=$\{(1,1),(2,1),(3,1)\}$:



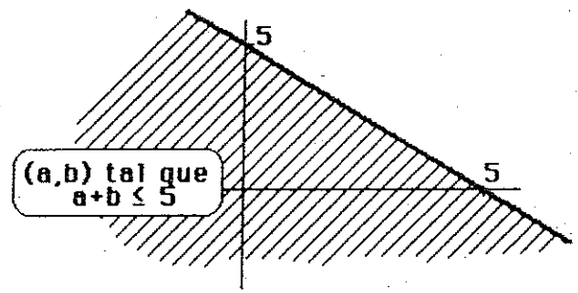
2) Sobre los conjuntos del ejemplo anterior definimos la relación:

$$a\mathcal{R}b \Leftrightarrow a+b \leq 5, \quad a \in A, b \in B$$

En tal caso $R = \{(1,1),(1,4),(2,1),(3,1)\}$



3) En una relación $\mathcal{R}$ los conjuntos A y B juegan un papel importante. Tomemos, por ejemplo $A = B = \mathbb{R}$ y $a\mathcal{R}b \Leftrightarrow a+b \leq 5$, $\quad a,b \in \mathbb{R}$.
En este caso $R = \{(a,b) \in \mathbb{R}^2 / a+b \leq 5\}$, que se grafica de la manera siguiente:



De los dos últimos ejemplos vemos que aunque la relación entre elemen-

tos es la misma, sus dominios pueden ser distintos. Esto lleva a definir la igualdad de relaciones:

Sea $\mathcal{R}_1$ definida en A_1, B_1 y $\mathcal{R}_2$ definida en A_2, B_2.

$$\begin{array}{l} \textit{Ambas relaciones son iguales } (\mathcal{R}_1 = \mathcal{R}_2), \\ \textit{si y sólo si } A_1 = A_2, B_1 = B_2, R_1 = R_2. \end{array} \tag{3.7}$$

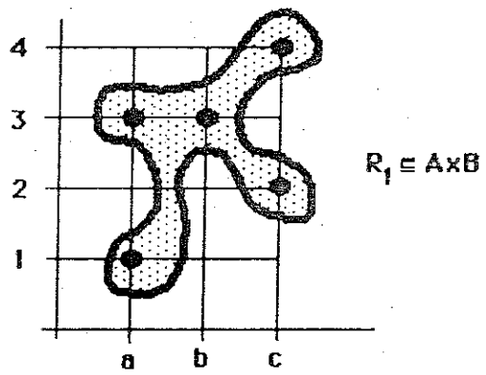
En este contexto las relaciones definidas en los ejemplos 2 y 3 son distintas.

Es importante en álgebra representar un objeto matemático, de manera de visualizar sus propiedades y operar con él de manera simple. A continuación presentamos los tres modos más usuales y prácticos de representar una relación.

3.4 Representáciones de una relación.

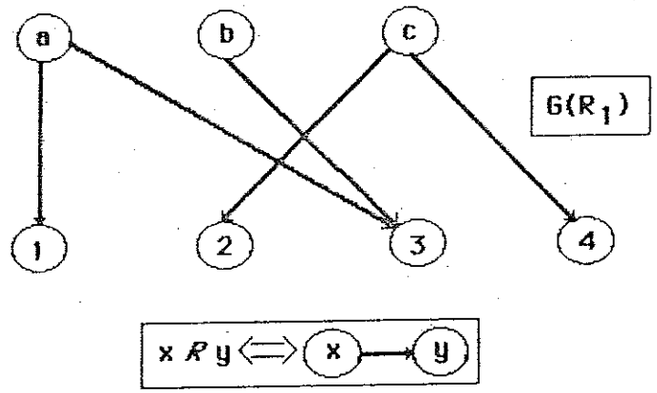
Introduciremos las diversas representaciones a partir de un ejemplo: Sea $A = \{a, b, c\}, B = \{1, 2, 3, 4\}$. Sea $R_1 = \{(a, 1), (a, 3), (b, 3), (c, 2), (c, 4)\}$. Es decir, $x\mathcal{R}_1 y \Leftrightarrow (x, y) \in R_1$.

Representación cartesiana.



Representación mediante un grafo.

Definimos un conjunto de puntos etiquetados con los elementos de A y B de manera que existe una flecha de a hacia b si y sólo si $(a, b) \in R$, es decir, $xRy \Leftrightarrow x \to y$. En el ejemplo anterior:



El caso de relaciones sobre un mismo conjunto, $A = B = E$, lo trataremos en el punto 3.5.

Representación matricial.

Definimos una matriz, A, de m filas y n columnas como un arreglo rectangular de $m \times n$ números reales:

$$A = (a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \tag{3.8}$$

donde $a_{ij} \in \mathbb{R}$, $1 \le i \le m, 1 \le j \le n$.

El elemento a_{ij} es el que aparece en la posición (i, j) del rectángulo (intersección de la fila i y la columna j).

Dadas dos matrices A, B definimos su igualdad como sigue:

Diremos que $A = B$ si y sólo si tienen igual número de filas y columnas y $(a_{ij} = b_{ij})(\forall i, j)$.

Por ejemplo: $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \neq \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

Para la representación matricial de una relación nos limitaremos a elegir los elementos de la matriz en el conjunto $\{0, 1\}$.

Volviendo a la relación $R_1 = \{(a,1),(a,3),(b,3),(c,2),(c,4)\}$ del ejemplo anterior, definamos su matriz asociada, $M(R_1)$, de tres filas y cuatro columnas:

$$\begin{array}{c} \\ a \\ b \\ c \end{array}\begin{array}{c} \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \end{array} = M(\mathcal{R}_1).$$

El elemento de la fila b y la columna 3 es 1 ya que $(b,3) \in R_1$. Análogamente, el elemento de la fila c y la columna 1 es 0 ya que $(c,1) \notin R_1$.

$M(\mathcal{R}_1)$ se denomina la matriz asociada a la relación $\mathcal{R}_1$ y se tiene

$$m_{xy} = 1 \Leftrightarrow x\mathcal{R}_1 y$$

donde m_{xy} es el elemento de la fila asociada a x y la columna asociada a y de la matriz $M(\mathcal{R}_1)$.

La representación cartesiana de la relación es bastante clásica y suficientemente clara como para no insistir en su formalización. No sucede lo mismo con las otras dos, por lo cual las definiremos de manera más formal.

Sean $A = \{a_1,...,a_p\}$, $B = \{b_1,...,b_n\}$ conjuntos finitos y sea $\mathcal{R}$ definida por $R \subseteq A \times B$.

El grafo, $G(\mathcal{R})$ asociado a la relación está definido como:

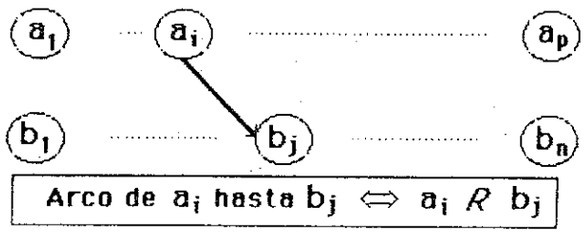
$$G(\mathcal{R}) = (U,V)$$

donde U es el conjunto de nodos o vértices etiquetados

$$U = \{a_1,...,a_p,b_1,...,b_n\}$$

y V es el conjunto de arcos tales que:

$$\text{(el arco } x \to y\text{, desde } x \text{ hasta } y\text{, está en el grafo)} \Leftrightarrow (x,y) \in R. \qquad (3.9)$$



La matriz asociada a $\mathcal{R}$, $M(\mathcal{R})$, está definida por:

$$M(\mathcal{R}) = (m_{ij}) = \begin{pmatrix} m_{11} & \cdots\cdots & m_{1n} \\ m_{i1} \quad \cdots & m_{ij} \quad \cdots & m_{in} \\ m_{p1} & \cdots\cdots & m_{pn} \end{pmatrix} \quad p \text{ filas} \qquad (3.10)$$

n columnas

donde

$$m_{ij} = \begin{cases} 1 & \text{si } a_i \mathcal{R} b_j \\ 0 & \text{si } a_i \not\mathcal{R}\, b_j \end{cases}$$

Observemos que dado un grafo $G = (U,V)$ es posible definir su matriz representante como:

$$M(G) = (m_{ij}) \quad \text{tal que} \quad m_{ij} = \begin{cases} 1 & \text{si existe el arco } i \to j \\ 0 & \text{si no existe el arco } i \to j \end{cases}$$

$M(G)$ se denomina la matriz de incidencia del grafo G. Es fácil ver que dada una relación $\mathcal{R}$:

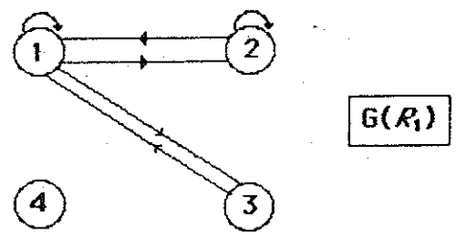
$$M(G(\mathcal{R})) = M(\mathcal{R}) \quad \text{(verifíquelo)}$$

lo cual muestra que ambas representaciones "codifican" la misma relación.

Desarrollemos un ejemplo algo más interesante para ver la representación gráfica y matricial. Sea $E = A = B = \{1,2,3,4\}$ tal que:

1) $a\mathcal{R}_1 b \Leftrightarrow a + b \leq 4$

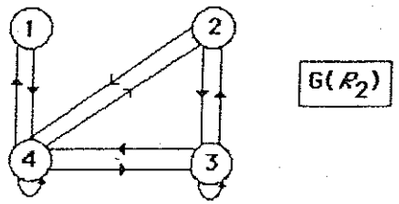
Grafo asociado:



Matriz asociada:

$$M(\mathcal{R}_1) = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

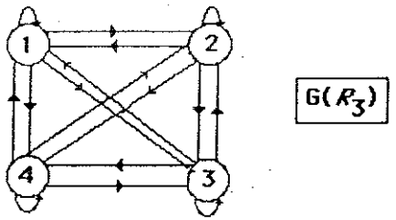
2) $a\mathcal{R}_2 b \Leftrightarrow a + b > 4$, sobre el conjunto $E = \{1, 2, 3, 4\}$. En este caso:



$G(\mathcal{R}_2)$

$$M(\mathcal{R}_2) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

3) Si tomamos, sobre el mismo conjunto $E = \{1, 2, 3, 4\}$ la relación trivial (que llamamos universal): $a\mathcal{R}_3 b \Leftrightarrow (a, b) \in E \times E$ (es decir todos los pares ordenados) obtenemos:



$G(\mathcal{R}_3)$

$$M(\mathcal{R}_3) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

La propiedad siguiente relaciona la representación gráfica y matricial:

Dadas dos relaciones $\mathcal{R}_1$ y $\mathcal{R}_2$ se tiene la equivalencia:

$$\mathcal{R}_1 = \mathcal{R}_2 \Leftrightarrow G(\mathcal{R}_1) = G(\mathcal{R}_2) \Leftrightarrow M(\mathcal{R}_1) = M(\mathcal{R}_2) \tag{3.11}$$

En efecto: si $M(\mathcal{R}_1) = A$ y $M(\mathcal{R}_2) = B$ se tiene

$$a_i \mathcal{R}_1 b_j \Leftrightarrow a_i \mathcal{R}_2 b_j \Leftrightarrow a_{ij} = 1 \Leftrightarrow b_{ij} = 1$$

de donde $A = B$, es decir $M(\mathcal{R}_1) = M(\mathcal{R}_2)$ ■

3.5 Clasificación de relaciones.

Trabajaremos a continuación con relaciones definidas sobre un solo conjunto $E = A = B$ y hablaremos de una relación $\mathcal{R}$ sobre E, en el sentido de que $R \subseteq E^2 = E \times E$.

Dada una relación $\mathcal{R}$ sobre E diremos que:

$$\mathcal{R} \text{ es } \textit{refleja} \Leftrightarrow (\forall a \in E) \quad (a\mathcal{R}a). \tag{3.12}$$

$$\mathcal{R} \text{ es } \textit{simétrica} \Leftrightarrow (\forall a, b \in E) \quad (a\mathcal{R}b \Rightarrow b\mathcal{R}a). \tag{3.13}$$

$$\mathcal{R} \text{ es } \textit{antisimétrica} \Leftrightarrow (\forall a, b \in E)(a\mathcal{R}b \wedge b\mathcal{R}a \Rightarrow a = b). \tag{3.14}$$

$$\mathcal{R} \text{ es } \textit{transitiva} \Leftrightarrow (\forall a, b, c \in E)(a\mathcal{R}b \wedge b\mathcal{R}c \Rightarrow a\mathcal{R}c). \tag{3.15}$$

Obviamente, podríamos definir muchas otras propiedades interesantes, pero los cuatro anteriores cubren dos tipos de relación muy importantes, las de orden y equivalencia.

Relación de Orden: Diremos que $\mathcal{R}$ en E es una *relación de orden* si y sólo si es refleja, antisimétrica y transitiva.

Relación de Equivalencia: Diremos que $\mathcal{R}$ en E es una *relación de equivalencia* si y sólo si es refleja, simétrica y transitiva.

Ejemplos.

1. Sea E el conjunto de los seres humanos. Sean las relaciones:
   $a\mathcal{R}b \Leftrightarrow a$ es hijo de b.
   - Es fácil verificar que $\mathcal{R}$ no es refleja, no es simétrica, es antisimétrica, no es transitiva.
   $a\mathcal{R}b \Leftrightarrow a$ está casado con b.
   - $\mathcal{R}$ no es refleja, es simétrica, no es antisimétrica y no es transitiva.
   $a\mathcal{R}b \Leftrightarrow a$ es de la misma nacionalidad que b.
   - Es refleja, es simétrica, no es antisimétrica, es transitiva. Luego es relación de equivalencia.

2. Sea $E = \mathbb{R}$ y las relaciones:
   $a\mathcal{R}b \Leftrightarrow a \leq b$.
   - Es refleja, no es simétrica ($4 \leq 5$ pero $5 \not\leq 4$), es antisimétrica ($a \leq b \wedge b \leq a \Rightarrow a = b$), es transitiva ($a \leq b \wedge b \leq c \Rightarrow a \leq c$). Luego es relación de orden.
   $a\mathcal{R}b \Leftrightarrow a = b$.
   - Es refleja, simétrica, antisimétrica, transitiva. Luego es relación de equivalencia.

3. Sea $E = \mathbb{N}$ y la relación:
   $a\mathcal{R}b \Leftrightarrow a$ divide $b \Leftrightarrow b = \alpha a, \alpha \in \mathbb{N}$. Notaremos $\mathcal{R} = |$.
   - Es refleja, no es simétrica, es antisimétrica: $(a|b) \wedge (b|a)$ $\Leftrightarrow (b = \alpha a) \wedge (a = \beta b)$ $(\alpha, \beta \in \mathbb{N})$, luego

$$b = \alpha\beta b \Rightarrow \alpha\beta = 1 \Rightarrow a = b.$$

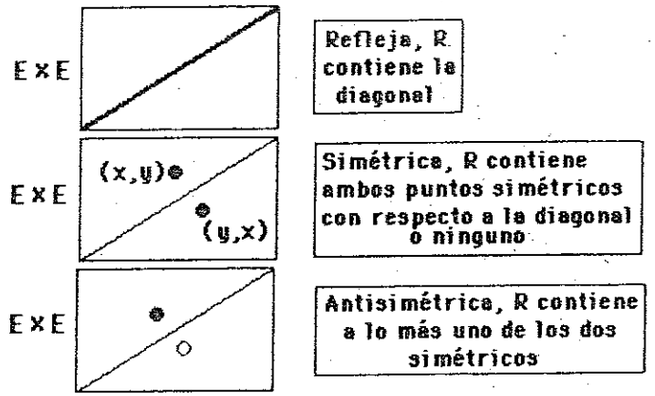
   Es transitiva: $(a|b) \wedge (b|c) \Leftrightarrow (b = \alpha a) \wedge (c = \beta b) \Rightarrow c = \beta\alpha a \Leftrightarrow a|c$.

4. Sea $\mathcal{R}$ con dominio $R = \{(1,2),(2,1),(2,3)\}$. $\mathcal{R}$ no es refleja, no es simétrica ($(3,2) \notin R$), no es antisimétrica ($(2,1) \wedge (1,2) \in R$ pero $1 \neq 2$), no es transitiva ($1\mathcal{R}2 \wedge 2\mathcal{R}1$ pero $1 \not\mathcal{R} 1$).

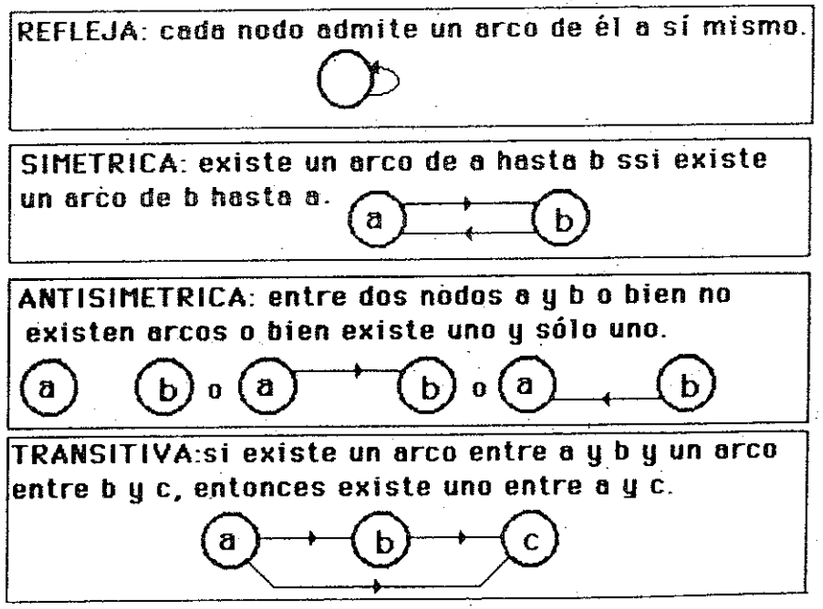
5. Sea $E = \mathcal{P}(U)$ (el conjunto de las partes de U) y la relación:
   $X\mathcal{R}Y \Longleftrightarrow X \subseteq Y$.
   - $\mathcal{R}$ es refleja, antisimétrica y transitiva. Luego es relación de orden.

Tratemos de visualizar las propiedades definidas, a través de los tres modos de representación que hemos introducido anteriormente.

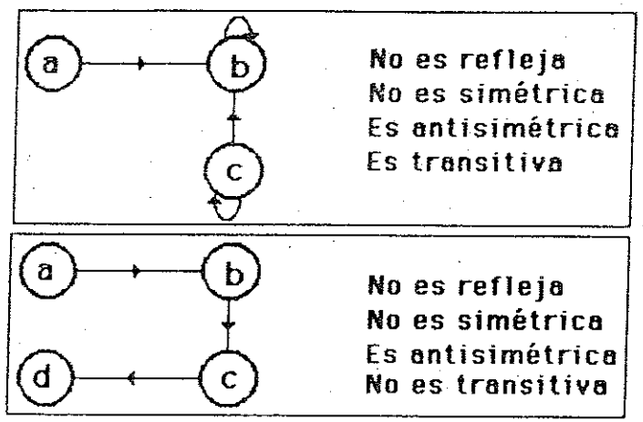
1. Representación cartesiana. En este modo de representación es fácil visualizar la reflexibidad, simetría y antisimetría pero no la transitividad.



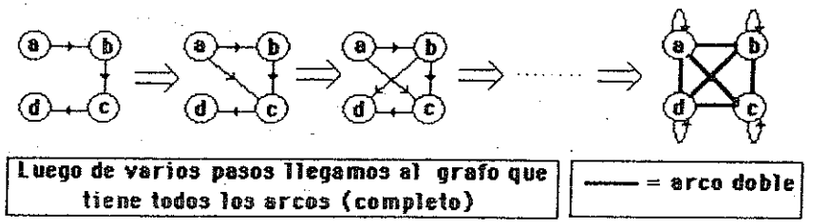
2. Representación mediante el Grafo.



Tomemos por ejemplo las relaciones definidas por los grafos siguientes:



Veamos cuál es el número mínimo de arcos que podemos agregar en la relación definida por el grafo anterior para que sea transitiva. Recuerde que por cada dos arcos en el mismo sentido debe existir el arco de atajo:



3. Representación Matricial. Sea $E = \{a_1, ..., a_p\}$, la relación $\mathcal{R}$ es refleja $\Leftrightarrow a_i \mathcal{R} a_i \Leftrightarrow M(\mathcal{R})$ contiene unos en la diagonal:

$$M(\mathcal{R}) = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} \tag{3.16}$$

R simétrica $\Leftrightarrow (a_i \mathcal{R} a_j \Leftrightarrow a_j \mathcal{R} a_i) \Leftrightarrow ((m_{ij} = 1) \Leftrightarrow (m_{ji} = 1))$:

$$M(\mathcal{R}) = \begin{pmatrix} \ddots & & a \\ & \ddots & \\ a & & \ddots \end{pmatrix} \text{ con } a \in \{0,1\} \tag{3.17}$$

O sea los elementos de $M(\mathcal{R})$ son simétricos con respecto a la diagonal de la matriz. Esto también puede verse de una manera que nos será útil más adelante. Definamos la matriz *traspuesta* de $M(\mathcal{R})$, que notaremos ${}^tM(\mathcal{R})$, como la matriz resultante de intercambiar filas por columnas: Si $M(\mathcal{R}) = (m_{ij}) \Leftrightarrow {}^tM(\mathcal{R}) = (m_{ji})$ Por ejemplo:

$$M(\mathcal{R}) = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} \Rightarrow {}^tM(\mathcal{R}) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Para definir la traspuesta de $M(\mathcal{R})$ no es necesario que ésta sea cuadrada (una matriz de $n \times n$). Por ejemplo:

$$M(\mathcal{R}) = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \Rightarrow {}^tM(\mathcal{R}) = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}$$

Con esta notación tenemos que $\mathcal{R}$ es simétrica $\Leftrightarrow M(\mathcal{R}) = {}^tM(\mathcal{R})$, (verifique).

Para analizar las otras propiedades de relaciones es necesario introducir dos nuevos conceptos para trabajar con matrices. El primero es un modo de comparar matrices, es decir una solución similar a la que conocemos para decir que un número real es mayor o menor o igual a otro real. Dadas dos matrices A y B de $p \times q$ (p filas y q columnas). Definamos la relación:

$$A \leq B \Leftrightarrow (a_{ij} \leq b_{ij}) \ (\forall i, j) \tag{3.18}$$

la desigualdad de la derecha corresponde a la relación de orden $\leq$, usual en $\mathbb{R}$.

Ejemplo:

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

$$A = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \not\leq \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = B$$

y $B \not\leq A$ (matrices no comparables).

La relación $\leq$ es trivialmente refleja. Es antisimétrica:
$(A \leq B) \wedge (B \leq A) \Leftrightarrow (\forall i,j)(a_{ij} \leq b_{ij}) \wedge (b_{ij} \leq a_{ij}) \Rightarrow (\forall i,j)(a_{ij} = b_{ij})$
$\Leftrightarrow A = B$.
Transitiva: $(A \leq B) \wedge (B \leq C) \Leftrightarrow$

$$(\forall i,j)\ \ (a_{ij} \leq b_{ij} \wedge b_{ij} \leq c_{ij}) \Rightarrow (\forall i,j)\ \ (a_{ij} \leq c_{ij}) \Leftrightarrow A \leq C.$$

Luego (¡oh, sorpresa!) "$\leq$" es una relación de orden ■

La otra noción que necesitamos es la de multiplicación de matrices con ceros y unos:

Definamos primero la suma y la multiplicación de dos elementos
$x, y \in \{0,1\}$

$+$	0	1
0	0	1
1	1	1

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

Claramente $+ = \vee$ y $\cdot = \wedge$ cuando 0 se codifica como F y 1 como V.
Veamos un ejemplo:

$$(1\ 1\ 0\ 1)\begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} = 1\cdot 0 + 1\cdot 1 + 0\cdot 0 + 1\cdot 1 = 0 + 1 + 0 + 1 = 1 + 1 = 1.$$

Hemos sumado los productos de elementos en igual posición de ambas 4-tuplas. Si se tienen más filas y columnas, hacemos lo mismo para cada fila de A con todas las columnas de B:

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

$$= \begin{pmatrix} 1\cdot 0 + 1\cdot 1 + 0\cdot 0 + 1\cdot 1 & 1\cdot 1 + 1\cdot 1 + 0\cdot 1 + 1\cdot 0 \\ 0\cdot 0 + 0\cdot 1 + 1\cdot 0 + 0\cdot 1 & 0\cdot 1 + 0\cdot 1 + 1\cdot 1 + 0\cdot 0 \\ 1\cdot 0 + 0\cdot 1 + 1\cdot 0 + 0\cdot 1 & 1\cdot 1 + 0\cdot 1 + 1\cdot 1 + 0\cdot 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} \text{1ra. fila} \times \text{1ra. col.} & \text{1ra. fila} \times \text{2da. col.} \\ \text{2da. fila} \times \text{1ra. col.} & \text{2da. fila} \times \text{2da. col.} \\ \text{3ra. fila} \times \text{1ra. col.} & \text{3ra. fila} \times \text{2da. col.} \end{pmatrix}$$

Notamos que para definir esta multiplicación se requiere que el número de columnas de A sea igual al número de filas de B. Además el resultado es una matriz con el número de filas de A y el número de columnas de B. Es decir,

$$A \cdot B = C$$

$$(p \times q)(q \times r) \Rightarrow (p \times r)$$

Como ya conocemos la notación de suma, los elementos c_{ij} de la matriz resultante se calculan de la manera siguiente:
$\forall i = 1, ..., p; \quad \forall j = 1, ..., r$

$$c_{ij} = (a_{i1}, a_{i2}, ..., a_{iq})\begin{pmatrix} b_{1j} \\ b_{2j} \\ \vdots \\ b_{qj} \end{pmatrix} = a_{i1}\cdot b_{1j} + ... + a_{iq}\cdot b_{qj} = \sum_{k=1}^{q} a_{ik}\cdot b_{kj}$$

donde $\sum$ se entiende como la disyunción ($\sum_{\ell=1}^{s} v_\ell = v_1 \vee v_2 \vee v_3 \vee ... \vee v_s$).

Con las dos nociones anteriores estamos en condiciones de caracterizar mediante matrices las propiedades de una relación sobre un conjunto $E = \{a_1, ..., a_n\}$:

$$\mathcal{R}\ \textit{refleja} \Leftrightarrow I = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \leq M(\mathcal{R}) \tag{3.19}$$

$$\mathcal{R}\ \textit{simétrica} \Leftrightarrow {}^tM(R) = M(\mathcal{R}). \tag{3.20}$$

$$\mathcal{R}\ \textit{transitiva} \Leftrightarrow M^2(\mathcal{R}) = M(\mathcal{R})\cdot M(\mathcal{R}) \leq M(\mathcal{R}). \tag{3.21}$$

Esta última propiedad no es trivial y merece una demostración:

$\Leftarrow$) Supongamos primero que $\mathcal{R}$ es transitiva. Sea $M = M(\mathcal{R}) = (m_{ij})$ y sea $C = M^2(\mathcal{R}) = M(\mathcal{R}) \cdot M(\mathcal{R}) = (c_{ij})$. Debemos probar que $(\forall i, j)\ (c_{ij} \leq m_{ij})$ o de manera equivalente:

$$(\forall i, j)\ (c_{ij} = 1) \Rightarrow m_{ij} = 1.$$

Supongamos entonces $c_{ij} = 1$, luego:

$$1 = c_{ij} = \sum_{k=1}^{n} m_{ik} m_{kj}$$

Luego, existe un índice $\ell \in \{1, ..., n\}$ tal que:

$$m_{i\ell} \cdot m_{\ell j} = 1 \Leftrightarrow m_{i\ell} = 1 \wedge m_{\ell j} = 1$$

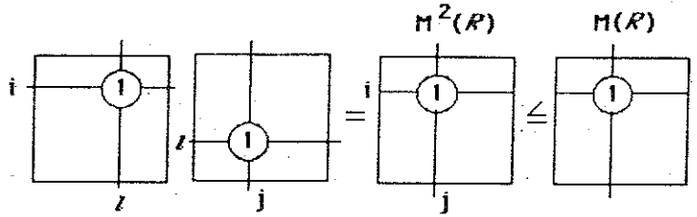
Por definición de $M(\mathcal{R})$ esto es equivalente a:

$$a_i \mathcal{R} a_\ell \wedge a_\ell \mathcal{R} a_j \text{ y por transitividad } \Rightarrow a_i \mathcal{R} a_j \Leftrightarrow m_{ij} = 1.$$

$\Rightarrow$) Supongamos que $M^2(R) \leq M(R)$ y sean $a_i \mathcal{R} a_\ell \wedge a_\ell \mathcal{R} a_j$ se tiene entonces:

$$(m_{i\ell} = 1) \wedge (m_{\ell j} = 1)$$

Matricialmente:



luego $c_{ij} = \sum_{k=1}^{n} m_{ik} m_{kj} = ... + m_{i\ell} \cdot m_{\ell j} + ... = 1$
por lo tanto, como $M^2(R) \leq M(R) \Rightarrow c_{ij} \leq m_{ij} \Leftrightarrow 1 \leq m_{ij}$
de donde $m_{ij} = 1 \Leftrightarrow a_i \mathcal{R} a_j$
Es decir $\mathcal{R}$ es transitiva: $(a_i R a_\ell) \wedge (a_\ell R a_j) \Rightarrow a_i R a_j$ ■

3.6 Relaciones de orden.

Recordemos que una relación $\mathcal{R}$ sobre E es de *orden* si y sólo si es refleja, antisimétrica y transitiva. Veremos acá algunas relaciones de orden importantes.

1. Relación de orden entre números reales, $a \leq b$ que ya analizamos.

2. Dado $E = \{a, b, c, ..., z\}$, el abecedario.

   $$\alpha \leq \beta \Leftrightarrow (\alpha = \beta) \vee (\alpha \text{ aparece antes que } \beta \text{ en el abecedario}).$$

3. En n-tuplas. Sea $E \subseteq \mathbb{R}$. Definamos $\leq$ en E^n como:

   $$X = (x_1, ..., x_n) \leq Y = (y_1, ..., y_n) \Leftrightarrow (\forall i = 1, ..., n)(x_i \leq y_i)$$

   donde $\leq$ en el lado derecho corresponde al orden usual en $\mathbb{R}$.

   Refleja: $X \leq X \Leftrightarrow (x_i \leq x_i)\ (\forall i = 1, ..., n)$.

   Antisimétrica:
   $(X \leq Y) \wedge (Y \leq X) \Leftrightarrow (\forall i \in \{1, ..., n\})(x_i \leq y_i) \wedge (y_i \leq x_i)$
   $\Rightarrow (\forall i \in \{1, ..., n\})\ \ (x_i = y_i) \Leftrightarrow X = Y.$

   Transitiva: $(X \leq Y) \wedge (Y \leq Z) \Leftrightarrow (\forall i = 1, ..., n)(x_i \leq y_i) \wedge (y_i \leq z_i)$
   $\Rightarrow (\forall i = 1, ..., n)(x_i \leq z_i) \Leftrightarrow X \leq Z.$

4. Orden *lexicográfico*. Sea E el conjunto abecedario y E^* el conjunto de todas las palabras. Dadas dos palabras $v = v_1 ... v_n$, $u = u_1 ... u_m$ en E^*, definimos la relación:

   $$v \leq u \Leftrightarrow (\exists k \leq n)(v_i = u_i, i \leq k)(v_{k+1} \text{ está "antes" de } u_{k+1} \text{ en } E).$$

   En el caso particular $n < m$ y $v_i = u_i$, $i = 1, ..., n$, se asume $v \leq u$.

   Ejemplos: casa $\leq$ casas, dragón $\leq$ drama.

Es directo que $\leq$ es una relación de orden correspondiente a la que aparece en los diccionarios (verifique).

5. Sea $E = \mathcal{M}_{p,q}(\{0, 1\})$ el conjunto de todas las matrices de p filas y q columnas con elementos 0's y 1's. :

   $$A \leq B \Leftrightarrow (\forall i, j)\ \ (a_{ij} \leq b_{ij})$$

es una relación de orden, como vimos anteriormente.

Notaremos en general una relación de orden en E por "$\leq$". Dos conceptos importantes son los de orden *parcial* y *total* inducidos en el conjunto E por la relación $\leq$. La idea es simple, por ejemplo en $\mathbb{R}$, la relación de orden usual $\leq$, permite comparar cualquier par de números reales $a, b \in \mathbb{R}$, pero, por ejemplo, la de divisibilidad no lo permite: $5 \not| \ 6 \wedge 6 \not| \ 5$, es decir 5 y 6 son incomparables (o no comparables con la relación de orden $|$). En este sentido, dada una relación de orden $\leq$ sobre E diremos que:

- Es relación de *orden total* si $\forall x, y \in E$ se tiene:

$$(x \leq y) \vee (y \leq x)$$

- Es relación de *orden parcial* si existen elementos $x, y \in E$ tales que:

$$(x \not\leq y) \wedge (y \not\leq x).$$

Ejemplos:

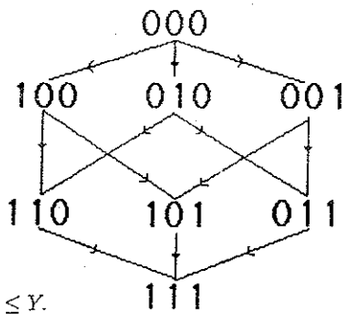
1) El orden $\leq$ en $\mathbb{R}$ y el lexicográfico son órdenes totales.
2) La divisibilidad en $\mathbb{N}$ y $\leq$ entre n-tuplas o matrices son órdenes parciales:

En efecto, sea $E = \{0,1\}^2 \quad (0,1) \not\leq (1,0) \wedge (1,0) \not\leq (0,1)$. Sea

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

$$A \not\leq B \wedge B \not\leq A.$$

En general, para las 3-tuplas en $\{0,1\}^3$ se tienen las siguientes relaciones de "comparación":



donde $X \to Y \Leftrightarrow X \leq Y$.

3.7 Teoría de números.

Una relación de orden importante es la divisibilidad en $\mathbb{N}$. Dados $a, b \in \mathbb{N}$ diremos que $a|b \Leftrightarrow b$ *es divisible por* $a \Leftrightarrow b$ *es múltiplo de* $a \Leftrightarrow (\exists \alpha \in \mathbb{N})(b = \alpha a)$. Recordemos sus propiedades:

Refleja: $a \Leftrightarrow a = 1 \cdot a$.

Antisimétrica:

$$\begin{aligned} &a|b \wedge b|a \Leftrightarrow b = \alpha a \wedge a = \beta b; \alpha, \beta \in \mathbb{N} \\ &\Leftrightarrow b = \alpha\beta b \Leftrightarrow \alpha\beta = 1 \Rightarrow \alpha\beta = 1 \\ &\Rightarrow a = b. \end{aligned}$$

Transitiva:

$$\begin{aligned} &a|b \wedge b|c \Leftrightarrow b = \alpha a \wedge c = \beta b, \alpha, \beta \in \mathbb{N} \Rightarrow \\ &c = \alpha\beta a \Leftrightarrow a|c \quad \blacksquare \end{aligned}$$

La divisibilidad es obviamente una relación de orden parcial. Además, ésta permite determinar propiedades muy importantes de los números naturales, algunas de las cuales desarrollaremos a continuación.

3.7.1. Algoritmo de la división.

Sean $a, b \in \mathbb{N}, b > 0$, entonces existen enteros $q, r \in \mathbb{N}$,únicos, tales que:

$$a = qb + r, \quad 0 \leq r < b \tag{3.22}$$

donde el natural q se denomina el cociente y r el resto de la división de a por b.

Ejemplo: Sea $a = 105$, $b = 8$:

$$\begin{array}{r} \underline{105} : 8 = 13 \\ \underline{25} \\ 1 \end{array} \qquad 105 = 13 \times 8 + 1$$

Demostración de la factorización:

Si $a < b$, el resultado es trivial $a = 0 \cdot b + a$ donde $q = 0, r = a$.

Supongamos $a \geq b$:

1) Si $b|a \Leftrightarrow a = cb$, luego basta tomar $q = c$ y $r = 0$ de donde $a = cb + 0$.
2) Supongamos entonces $b\not| a$ y construyamos la sucesión de números naturales:

$$a, a-b, a-2b, \ldots$$

Claramente, existe un valor $q \in I\!N$ tal que $a - qb > 0$ y $a - (q+1)b < 0$ (Observación: no se anula, pues, si no se tendría $b|a$).

Sea $r = a - qb \Leftrightarrow a = qb + r$ además $r < b$. En caso contrario, es decir $r \geq b \Leftrightarrow a - qb \geq b \Leftrightarrow a - b(q+1) \geq 0$ lo cual contradice el hecho que $a - (q+1)b < 0$. Luego, hemos demostrado la propiedad ■

Unicidad de la representación:

Supongamos $a = q_1 b + r_1, a = q_2 b + r_2 \Leftrightarrow r_1 - r_2 = q_2 b - q_1 b = (q_2 - q_1)b$, pero $0 \leq r_1 < b$ y $0 \leq r_2 < b \Rightarrow |r_1 - r_2| < b$. Como $|r_1 - r_2| = |q_2 - q_1|b$:

$$|q_2 - q_1|b < b \Rightarrow |q_2 - q_1| < 1.$$

Como $q_i \in I\!N$, $|q_2 - q_1| = 0$, de donde $q_2 = q_1$ y $r_2 = r_1$ ■

3.7.2. Algoritmo de Euclides.

Sean $a, b \in I\!N$, se define el *máximo común divisor*, $mcd(a,b) = c \in I\!N$ tal que:

$$(c|a) \wedge (c|b) \tag{3.23}$$

$$(\forall d \in I\!N)\ (d|a) \wedge (d|b) \Rightarrow d|c \tag{3.24}$$

Calculemos por ejemplo el $mcd(6,9)$

$mcd(6,9) = 3$	divisores de 6	divisores de 9
	1	1
	2	**3**
	3	9
	6	

Daremos un algoritmo, adjudicado a la Escuela de Euclides (tiempos del hilo negro...), para calcular este número:

Sean $a, b \in I\!N$ tales que $b < a$.

Dividamos a por b con resto:

$$a = bq_o + r_1; \qquad 0 \leq r_1 < b$$

si $r_1 \neq 0$ podemos dividir b por r_1:

$$b = r_1 q_1 + r_2; \qquad 0 \leq r_2 < r_1$$

si $r_2 \neq 0$, podemos dividir r_1 por r_2

$$r_1 = r_2 q_2 + r_3; \qquad 0 \leq r_3 < r_2, \text{ etc ...}$$

Determinándose así una sucesión estrictamente decreciente:

$$b > r_1 > r_2 > r_3 > \ldots \geq 0$$

Como cada r_i debe disminuir a lo menos una unidad en cada paso, en el peor de los casos:

$$b, b-1, b-2, \ldots b-(b-1), 0$$

$$b > r_1 > r_2 \ > \ldots \ > r_{b-1}$$

luego, en a lo más b pasos determinamos un resto nulo, con lo cual el algoritmo se detiene en un número finito de pasos $\leq b$. Estudiemos la sucesión de restos:

$$\begin{aligned}
a &= bq_o + r_1 && 0 \leq r_i < b \\
b &= r_1 q_1 + r_2 && 0 \leq r_2 < r_1 \\
r_1 &= r_2 q_2 + r_3 && 0 \leq r_3 < r_2 \\
r_i &= r_{i+1} q_{i+1} + r_{i+2} && 0 \leq r_{i+2} < r_{i+1} \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n && 0 \leq r_n < r_{n-1} \\
r_{n-1} &= r_n q_n, \text{ con resto nulo } r_{n+1} = 0.
\end{aligned}$$

La recurrencia es:

$$r_i = r_{i+1} q_{i+1} + r_{i+2} \quad k = 1, 2, \ldots, n-1$$

Afirmamos que $r_n = mcd(a,b)$.

Primero demostraremos que r_n es divisor común de a y b:

esto lo hacemos por inducción sobre los diferentes restos:
es claro que $r_n | r_{n-1}$, además, como $r_{n-2} = r_{n-1} q_{n-1} + r_n \Rightarrow r_n | r_{n-2}$.
Supongamos que:

$$r_n | r_{n-1}, \ldots, r_n | r_{i+1}, r_n | r_i \quad i < n$$

y demostremos que $r_n | r_{i-1}$.

De la ecuación de recurrencia:

$$r_{i-1} = r_i q_i + r_{i+1}$$

y por hipótesis de inducción $r_i = \alpha r_n, r_{i+1} = \beta r_n$ luego $r_n | r_{i-1}$.

Ergo r_n es divisor de todos los restos, en particular: como $b = r_1 q + r_2 \Rightarrow r_n | b \Rightarrow r_n | a$ luego r_n es divisor común de a y b.

Sea ahora d otro divisor común de a y b. Como $a = bq_o + r_1 \Leftrightarrow r_1 = a - bq_o \Rightarrow d | r_1$.

Como $r_2 = b - r_1 q_1 \Rightarrow d | r_2$.

Supongamos $d | r_1, ..., d | r_i$. De la ecuación de recurrencia: $r_{i-1} = r_i q_i + r_{i+1}$ concluímos $r_{i+1} = r_{i-1} - r_i q_i \Rightarrow d | r_{i+1}$.

Luego d es divisor de todos los restos $r_1, r_2, ..., r_n$, y en particular $d | r_n$. Hemos demostrado entonces que $r_n = mcd(a, b)$ ■

El algoritmo de Euclides nos permite probar algunas propiedades profundas de los números enteros. Por ejemplo:

Dados $a, b \in \mathbb{N}, \exists x, y \in \mathbb{Z}$ tales que

$$ax + by = mcd(a, b). \tag{3.25}$$

Demostración: recordemos que $mcd(a, b) = r_n$: n-ésimo resto del algoritmo de Euclides.

Demostraremos que cada resto admite una escritura del tipo (3.25): En efecto

$$r_1 = a - bq_o \Rightarrow x_1 = 1, y_1 = -q_o$$
$$r_2 = b - r_1 q_1$$

luego,

$$r_2 = b - (a - bq_o)q_1 = (-1)a + (1 + q_o q_1)b,$$

de donde,

$$x_2 = -1, y_2 = 1 + q_o q_1$$

supongamos entonces:

$$r_j = x_j a + y_j b \quad \forall j \leq k$$

y demostremos para $k + 1$:

Sabemos que

$$r_{k-1} = r_k q_k + r_{k+1} \Rightarrow$$
$$r_{k+1} = -r_k q_k + r_{k-1} = -q_k(x_k a + y_k b) + x_{k-1} a + y_{k-1} b$$
$$= (x_k - q_{k-1} x_{k-1})a + (y_k - q_{k-1} y_{k-1})b.$$

Luego, para todo $k = 1, ..., n$ se tiene la escritura (3.24).

Por lo tanto, existen x_n, y_n tales que $r_n = x_n a + y_n b$. Como $r_n = mcd(a, b)$, se obtiene el resultado ■

Dados $a, b \in \mathbb{N}$, diremos que a, b son *primos relativos* si y sólo si $mcd(a, b) = 1$.

Por ejemplo $a = 3,\ b = 5$; $a = 6,\ b = 11$.

Directamente del Algoritmo Euclides y de la proposición anterior, tenemos que *$a, b \in \mathbb{N}$ son primos relativos si y sólo si existen $x, y \in \mathbb{Z}$ tales que:*

$$ax + by = 1 \tag{3.6}$$

En efecto, si $mcd(a, b) = 1 \Rightarrow \exists x, y \in \mathbb{Z}$ tales que $ax + by = mcd(a, b) = 1$.

En el otro sentido, si $ax + by = 1$, como $mcd(a, b) | a$ y $mcd(a, b) | b \Rightarrow mcd(a, b) | ax + by = 1 \Rightarrow mcd(a, b) = 1$ ■

Un corolario importante es el siguiente:

Lema de Euclides. *Sean $a, b, c \in \mathbb{N}$. Si $a | bc$ y además los naturales a, b son primos relativos entonces $a | c$.*

En efecto, como $mcd(a, b) = 1, \exists x, y \in \mathbb{Z}$ tales que $ax + by = 1$, por lo tanto $c = (ax + by)c = a(cx) + (bc)y$ pero $a | a$ y por hipótesis $a | bc$, entonces $a | a(cx) + (bc)y = c$ ■

La noción de máximo común divisor tiene innumerables aplicaciones, entre otras puede utilizarse para determinar la irracionalidad de algunos números reales. Consideremos el número $\sqrt{2} \in \mathbb{R}$, y demostremos que es irracional ($\forall p, q \in \mathbb{Z}, \sqrt{2}$ no admite una escritura de la forma p/q). Supongamos que $\sqrt{2}$ es racional, luego existen $p, q \in \mathbb{N} \setminus \{0\}$, tales que $\sqrt{2} = \frac{p}{q}$. Sin pérdida de generalidad podemos suponer que p y q son primos relativos ($mcd(p, q) = 1$), ya que, en caso contrario simplificamos los factores comunes obteniendo dos enteros, primos relativos.

De la ecuación $p^2 = 2q^2$ es evidente que p^2 es par. Más aún, p es par. En efecto, si p fuese impar entonces $p = 2m+1, m \in \mathbb{N}$, luego $p^2 = 2(2m^2 + 2m) + 1$ que es impar.

Como p es par, $p = 2k, k \in \mathbb{N} \setminus \{0\}$, luego $4k^2 = 2q^2$, concluyendo, de manera análoga al caso de p, que q es par. Pero esto es una contradicción, ya que siendo p y q pares se tiene $mcd(p,q) \geq 2$. Concluímos entonces que $\sqrt{2}$ no puede escribirse como p/q, ergo es irracional ■

Diremos que $p \in \mathbb{N}$ es un número *primo* si y sólo si $p > 1$ y p es divisible sólo por 1 y por sí mismo.

Obviamente existen números primos: 2,3,5,7,11,13,... La pregunta es si esta secuencia es finita o infinita. Antes de responder a esto demostraremos algo importante:

Teorema fundamental de la aritmética: *cualquier natural $n \geq 2$ puede escribirse de manera única, salvo el orden, como producto de primos:*

$$n = p_1 p_2 ... p_r \tag{3.27}$$

donde los números p_i son primos y $2 \leq p_1 \leq p_2 \leq ... \leq p_r$.

Demostración: Existencia. Por inducción sobre n. Para $n = 2; 2$ es la factorización, pues 2 es primo.

Supongamos que sea cierto para cualquier entero $k \leq n$ y demostremos para $k = n+1$.

Si $n+1$ es primo $\Rightarrow n+1 = n+1$ es la factorización. Si no, $n+1 = bc$; $1 \leq b < n+1$ y $1 \leq c < n+1$. Aplicando la hipótesis de inducción a los enteros b y c:

$$b = p_1 ... p_r, c = p'_1 ... p'_s, \qquad \text{donde } p_i, p'_i \text{ son primos}$$

luego $a = p_1 ... p_r p'_1 ... p'_s$ es un producto de primos ■

Unicidad: Supongamos $n = p_1 ... p_s = q_1 ... q_m; p_i, q_i$ primos
Si $s = 1$, entonces:

$$n = p_1 = q_1 ... q_m \Rightarrow p_1 = q_1(q_2 ... q_m).$$

como p_1 es primo, $m = 1$ y $p_1 = q_1$.

Supongamos entonces $s > 1$ y que el resultado es cierto para todo $1 \leq k < s$ salvo el orden de los elementos.

Demostremos entonces para el valor s:

$$p_1 p_2 ... p_s = q_1 ... q_m \Rightarrow p_1 | q_1 ... q_m$$

luego

$$p_1 | q_\ell (\prod_{j \neq \ell} q_j) \quad \ell = 1, ..., m$$

pero

$$mcd(p_1, q_\ell) = 1 \Rightarrow p_1 | (\prod_{j \neq \ell} q_j)$$

$$\Rightarrow p_1 | q_r \text{ para algún índice } r$$

Por lo tanto $p_1 = q_r$, cancelando:

$$p_2 ... p_s = q_1 ... q_{r-1} q_{r+1} ... q_m$$

obteniendo una expresión a la izquierda con $s-1$ primos. Por hipótesis inductiva sobre $s-1$ elementos se concluye $p_i = q_i \quad \forall i$ ■

Una consecuencia inmediata es que:

La sucesión de primos es infinita. (3.28)

La demostración es por el absurdo: supongamos que la sucesión sea finita $\{p_1 < p_2 < ... < p_n\}$ y sea

$$p = \prod_{i=1}^{n} p_i + 1$$

Como p no es primo y $p \geq 1$, del teorema fundamental de la aritmética, p se escribe como un producto de primos del conjunto $\{p_i\}_{i=1}^n$. Luego existe $1 \leq k \leq n$ tal que $p_k | p$.

Pero

$$p_k | p \Rightarrow p_k | (p - \prod_{i=1}^{n} p_i) = 1$$

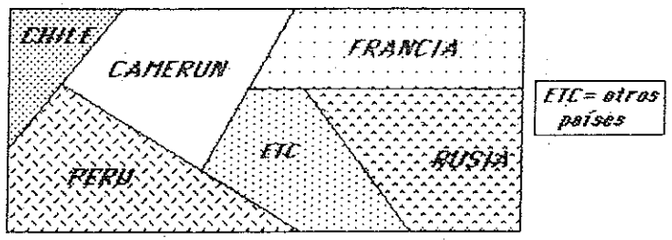
luego $p_k = 1$, lo cual es contradicción ya que $p_i \geq 2 \quad \forall i = 1, ..., n$ ■

Otros tópicos relacionados con teoría de números se desarrollan en los temas 2 y 3, al final del capítulo.

3.8. Relaciones de equivalencia.

Recordemos que $\mathcal{R}$ sobre E es una *relación de equivalencia* si y sólo si es refleja, simétrica y transitiva.

Denotaremos una relación de equivalencias $\mathcal{R}$ por $\sim$. La más clásica es sin duda la igualdad ($=$) entre números reales, otra es la de "nacionalidad" entre los habitantes del planeta. En este último caso la nacionalidad permite clasificar los habitantes del globo mediante una partición en países:



Esta propiedad de particionar un conjunto es de gran utilidad y la desarrollaremos en detalle más adelante.

Un ejemplo interesante de relación de equivalencia es el siguiente:

Sea $E = \mathcal{M}_{22}(\{0,1\})$ el conjunto de matrices de 2×2 con elementos en $\{0,1\}$.

Sean $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, I^* = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ dos matrices de este conjunto.

Definimos la relación:

$$A \sim B \Leftrightarrow \exists P \in \{I, I^*\} \text{ tal que } A = P \cdot B$$

$\sim$ es relación de equivalencia. En efecto

Es refleja: basta tomar $P = I$

$$IA = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_{11} & q_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = A$$

Es simétrica:

$$A \sim B \Leftrightarrow A = PB.$$

1er. Caso: $P = I \Rightarrow A = IB = B \Leftrightarrow B = IA$ luego $B \sim A$.

2do. Caso: $P = I^*$ es decir $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} B$ pero si multiplicamos toda la ecuación por I^*:

$$A = I^*B \qquad /I^*$$
$$I^*A = I^*(I^*B)$$

es fácil verificar que:

$$= (I^*I^*)B$$

pero $I^*I^* = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$

por lo tanto $I^*A = B \Leftrightarrow B = I^*A \Leftrightarrow B \sim A$

Es transitiva.

$$A \sim B \wedge B \sim C \Leftrightarrow A = PB \ \wedge \ B = QC; \quad P, Q \in \{I, I^*\}$$
$$\Rightarrow A = P(QC) = (PQ)C$$

para el producto PQ tiene cuatro posibilidades

1) $PQ = I \cdot I$,
2) $PQ = I \cdot I^*$,
3) $PQ = I^*I$,
4) $PQ = I^*I^*$.

Si 1: $A = IC$ por lo tanto $A \sim C$.

Si 2: $PQ = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = I^*$ por lo tanto $A = I^*C \Leftrightarrow A \sim C$

Si 3: $PQ = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I^*$ por lo tanto $A = I^*C \Leftrightarrow A \sim C$.

Si 4: $PQ = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = I$ por lo tanto $A = IC \Leftrightarrow A \sim C$.

Con lo cual hemos verificado que $\sim$ es relación de equivalencia ■

Podríamos haber visto esto de una manera más directa, observando lo que hacen I e I^* al premultiplicar una matriz:

1) Si $P = I$, entonces $A = IB = B$
2) Si $P = I^*$

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} b_{21} & b_{22} \\ b_{11} & b_{12} \end{pmatrix}$$

En este caso se intercambian las filas de B.

De 1 y 2 podemos concluir:

$A \sim B \Leftrightarrow (A = B) \vee$ (A corresponde a la matriz B con sus filas intercambiadas).

Veamos, en este mismo ejemplo, cómo podemos clasificar las matrices según la relación de equivalencia $\sim$. La idea, tal como en las nacionalidades, es colocar en un mismo saco todos aquellos objetos equivalentes entre sí.

No es difícil percatarse que hay exactamente 16 matrices de 2×2 con 0's y 1's

$$\begin{array}{cccc} A_0 & A_1 & A_2 & A_3 \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \\ A_4 & A_5 & A_6 & A_7 \\ \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} & \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \\ A_8 & A_9 & A_{10} & A_{11} \\ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} & \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \\ A_{12} & A_{13} & A_{14} & A_{15} \\ \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} & \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \end{array} = \mathcal{M}_{22}(\{0,1\})$$

Claramente A_0 está sola en una clase, pasa lo mismo con A_5, A_{10} y A_{15}.

Notaremos como $C(X)$ el conjunto de todas las matrices relacionadas con la matriz X. Luego $C(A_0) = \{A_0\}, C(A_5) = \{A_5\}, C(A_0) = \{A_{10}\}$, $C(A_{15}) = \{A_{15}\}$. Por otra parte:

$$C(A_1) = \{A_1, A_4\},\ C(A_2) = \{A_2, A_8\}$$
$$C(A_3) = \{A_3, A_{12}\},\ C(A_6) = \{A_6, A_9\}$$
$$C(A_7) = \{A_7, A_{13}\},\ C(A_{11}) = \{A_{11}, A_{14}\}.$$

y se tiene:

$$\mathcal{M}_{22}(0,1) = C(A_0) \cup C(A_1) \cup \cup C(A_2) \cup C(A_5) \cup C(A_6) \cup$$
$$\cup C(A_7) \cup C(A_{10}) \cup C(A_{11}) \cup C(A_{15}).$$

Conviene observar que cada matriz pertenece a una y sólo una clase, lo cual permite formar la partición.

Este tipo de propiedades podemos formularlas en el marco general de cualquier relación de equivalencia, para esto primero formalizamos la idea de *clase de equivalencia*.

Dada una relación de equivalencia $\sim$ sobre E y un elemento $x \in E$ definimos la *clase de equivalencia de* x:

$$[x] = \{y \in E / x \sim y\}. \tag{3.29}$$

La primera constatación es que $x \in [x]$, luego $\forall x \in E, [x] \neq \phi$. En efecto, ya que $\sim$ es refleja $x \sim x$ ■

Veamos que $\{[x]/x \in E\}$ es una partición de E. Es inmediato que:

$$E = \bigcup_{x \in E} [x]$$

Basta entonces demostrar que:

$$\text{Si } x \not\sim y \Rightarrow [x] \cap [y] = \phi. \tag{3.30}$$

$$\text{Si } x \sim y \Rightarrow [x] = [y]. \tag{3.31}$$

Demostración:

(3.30): Supongamos $z \in [x] \cap [y] \Leftrightarrow (z \in [x]) \wedge (z \in [y]) \Leftrightarrow (x \sim z) \wedge (z \sim y)$.

Por transitividad se tiene $x \sim y$, lo cual es una contradicción ya que $x \not\sim y$. Luego $[x] \cap [y] = \phi$.

(3.31): Si $x \sim y \Rightarrow (x \in [y]) \wedge (y \in [x])$. Sea $z \in [x] \Rightarrow x \sim z$ como $x \sim y \Rightarrow z \sim y \Rightarrow z \in [y]$ luego $[x] \subseteq [y]$ y de manera análoga se demuestra $[y] \subseteq [x]$, es decir $[x] = [y]$.

Luego E puede escribirse como la unión de las clases de equivalencia distintas ■

La familia de conjuntos (clases de equivalencia) de la partición se nota

$$E/\sim \quad = \quad \{ \text{ clases de equivalencia distintas } \} \tag{3.32}$$

y se denomina *conjunto cociente* asociado a la relación de equivalencia $\sim$ sobre E.

Hemos probado entonces que a una relación de equivalencia $\sim$ sobre E le podemos asociar una partición.

A la inversa, dada una partición $\mathcal{F} = \{A_i\}_{i\in I}$ de E siempre es posible asociarle una relación de equivalencia inducida por la partición $\mathcal{F}$ de manera que al "particionar" mediante esta relación de equivalencia reencontremos $\mathcal{F}$. En efecto sea $\sim$ definida como en el caso de la relación de nacionalidad:

$$x \sim y \Leftrightarrow (\exists i \in I) \ \ (x, y \in A_i)$$

Claramente es de equivalencia y dado $x \in E \Rightarrow (\exists!\ i \in I)(x \in A_i)$. Es decir, como $x \in A_i$:

$$[x] = \{y/y \sim x\} = \{y/y \in A_i\} = A_i$$

por lo tanto $E/\sim = \{A_i\}_{i\in I}$ ■

Una relación de equivalencia muy importante es la de los enteros "módulo p" que estudiaremos a continuación.

3.9 Clases de congruencia módulo p.

Sea $p \in \mathbb{N}, E = \mathbb{Z}$. Definamos la relación en $\mathbb{Z}$:

$$x \sim y \Leftrightarrow (\exists k \in \mathbb{Z})(x - y = kp). \tag{3.33}$$

Lo cual es equivalente a decir que la diferencia es múltiplo de p, o bien que la diferencia es divisible por p. Esta relación es de equivalencia. En efecto, es:

Refleja: $x - x = 0p$, luego $x \sim x$.

Simétrica: $x \sim y \Leftrightarrow x - y = kp \Leftrightarrow y - x = (-k)p \Leftrightarrow y \sim x$.

Transitiva: $(x \sim y) \wedge (y \sim z) \Leftrightarrow (x - y = kp) \wedge (y - z = k'p) \Rightarrow$
$x - z = x - y + y - z = (k + k')p \Leftrightarrow x \sim z$.

Utilizaremos como notación de $x \sim y$ la siguiente: $x \equiv y(mod p)$. Veamos cuál es el conjunto cociente $\mathbb{Z}/\sim$ que notaremos $\mathbb{Z}_p$.

Analicemos primero el caso particular $p = 2$. Veamos que significa:

$$x = y(mod 2) \Leftrightarrow x - y = 2k$$

es decir la diferencia entre x e y es par. Luego, la clase del 0 es:

$$[0] = \{..... -4, 2, 0, 2, 4, ...\} = \{x/x = 2k, k \in \mathbb{Z}\}$$

y la clase del 1:

$$[1] = \{..., ... -5, -3, -1, 1, 3, 5, ..., ...\} = \{x/x = 2k + 1, k \in \mathbb{Z}\}$$

obteniendo $\mathbb{Z} = [0] \cup [1], \quad [0] \cap [1] = \phi$.

Gráficamente:

$\mathbb{Z}$:	...	−6	−5	−4	−3	−2	−1	0	1	2	3...
$[0] \cup [1]$:		...0	1	0	1	0	1	0	1	0	1...

Mediante esta relación se discrimina la "paridad" entre los enteros. Dos de ellos son equivalentes si tienen igual paridad (ambos pares o ambos impares).

Veamos en general, las clases para $p \in \mathbb{N}, p > 0$

$$\begin{aligned}[0] &= \{x \in \mathbb{Z}/x - 0 = kp, k \in \mathbb{Z}\} = \{x/x = kp, k \in \mathbb{Z}\} \\ &= \{....., -2p, -p, 0, p, 2p, 3p, ...\}\end{aligned}$$

$$\begin{aligned}[1] &= \{x \in \mathbb{Z}/x = kp + 1, k \in \mathbb{Z}\} \\ &= \{....., -2p + 1, -p + 1, 1, p + 1, 2p + 1, ...\}\end{aligned} \tag{3.34}$$

$$[2] = \{x \in \mathbb{Z}/x = kp + 2, k \in \mathbb{Z}\}$$

$$\vdots$$

$$[p-1] = \{x \in \mathbb{Z}/x = kp + (p-1), k \in \mathbb{Z}\}$$

cuando $s \geq p$, las clases se repiten. Sea $s \geq p \Rightarrow s = q \times p + r, 0 \leq r < p$.

$$\begin{aligned}[s] &= \{x/x - s = kp, k \in \mathbb{Z}\} \\ &= \{x/x = kp + s, k \in \mathbb{Z}\} \\ &= \{x/x = kp + qp + r, k \in \mathbb{Z}\} \\ &= \{x/x = k'p + r, k' \in \mathbb{Z}\} = [r]\end{aligned}$$

Luego, $\mathbb{Z} = \bigcup_{i=0}^{p-1} [i]$ y el conjunto cociente es $\mathbb{Z}_p = \{[0], [1], ..., [p-1]\}$.

Ejercicios.

1. Para los conjuntos A, B, C, demuestre:
   (a) $A \times (B \cup C) = (A \times B) \cup (A \times C)$.
   (b) $A \times (B \cap C) = (A \times B) \cap (A \times C)$.
   (c) $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$.
   (d) $A \times B = \bigcup_{b \in B} (A \times \{b\})$.
2. Demuestre que:
   (a) $(A \times C = B \times C) \wedge (C \neq \phi) \Rightarrow A = B$.
   (b) $C_{E \times F}(B \times D) = (C_E B \times F) \cup (E \times C_F D)$.
   (c) Determine si $\forall A, B, C$: $(A \Delta B) \times C = (A \times C) \Delta (B \times C)$.
3. Estudie, clasifique y grafique las relaciones
   (a) $x \mathcal{R} y \iff xy \geq 0$ en $\mathbb{R}$.
   (b) $x \mathcal{R} y \iff \max(x, y) \leq 2$ en $\mathbb{N}$.
   (c) $x \mathcal{R} y \iff \max(x, y) = 20$ en $\mathbb{N}$.
   (d) $x \mathcal{R} y \iff mcd(x, y) = 1$ en $\mathbb{N}$.
   (e) $x \mathcal{R} y \iff x^2 + y^2 \leq 1$ en $\mathbb{R}$.
   (f) $X \mathcal{R} Y \iff x_{ii} = y_{ii} \quad i = 1, 2$ en $\mathcal{M}_{22}(\{0, 1\})$.
   (g) $X \mathcal{R} Y \iff X \cdot Y = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ en $\mathcal{M}_{22}(\{0, 1\})$.
   (h) $X \mathcal{R} Y \iff X + Y = \begin{pmatrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{pmatrix}$ en $\mathcal{M}_{nn}(\{0, 1\})$.
   (i) $G \mathcal{R} G' \iff$ (ambos grafos tienen algún camino de largo 4) en el conjunto de los grafos con 4 nodos. Es decir, existen al menos dos nodos tales que se puede ir de x a y utilizando cuatro arcos (no necesariamente distintos).
   (j) $x \mathcal{R} y \iff$ (si la palabra x termina con una letra lexicográficamente menor o igual a la última letra de la palabra y).
   (k) $x \mathcal{R} y \iff$ (ambas palabras empiezan y terminan con vocal) .
4. Sea $\mathcal{R}$ definida en $\mathbb{N}$ por: $x \mathcal{R} y \iff (2x + 3y = 15) \vee (x + y = 8)$. Encuentre las representaciones cartesiana, matricial y el grafo asociado a $\mathcal{R}$.
5. Dibuje la representación cartesiana de $\mathcal{R}$ definida en $\mathbb{R}$, por:
   (a) $R = \{(x, y)/x + 2y < 2\}$.
   (b) $R = \{(x, y)/x < y, 0 \leq y \leq 1\}$.
   (c) $R = \{(x, y)/x^2 - y^2 + x > 0\}$.
6. Dé ejemplos mediante matrices de 3×3 con 0's y 1's de relaciones:
   - refleja, simétrica pero no transitiva.

- refleja, transitiva, pero no simétrica.
- simétrica, transitiva pero no refleja.

7. Sean $\mathcal{R}_1, \mathcal{R}_2$ dos relaciones sobre un conjunto E. Se define

$$\mathcal{R}_1 \wedge \mathcal{R}_2 \Longleftrightarrow (x\mathcal{R}_1 \wedge \mathcal{R}_2 y \Longleftrightarrow x\mathcal{R}_1 y \ \wedge x\mathcal{R}_2 y)$$
$$\mathcal{R}_1 \vee \mathcal{R}_2 \Longleftrightarrow (x\mathcal{R}_1 \vee \mathcal{R}_2 y \Longleftrightarrow x\mathcal{R}_1 y \ \vee x\mathcal{R}_2 y).$$

   (a) Estudie las propiedades de la conjunción y disyunción de relaciones según las propiedades de $\mathcal{R}_1$ y $\mathcal{R}_2$.
   (b) Considere $E = \{a_1, ..., a_n\}$: Calcule los grafos y matrices de la conjunción y disyunción, en función de aquellos de $\mathcal{R}_1$ y $\mathcal{R}_2$. (Construya primero ejemplos con $n = 4$).

8. Dada $\mathcal{R}$ una relación definida en E, definimos $\mathcal{R}^{-1}$ de la siguiente manera:

$$\forall (a,b) \in E^2 \quad a\mathcal{R}b \Longleftrightarrow b\mathcal{R}^{-1}a.$$

   Pruebe que:
   (a) Si $\mathcal{R}$ es relación de equivalencia, entonces $\mathcal{R}^{-1}$ es de equivalencia.
   (b) Si $\mathcal{R}$ es relación de orden, entonces $\mathcal{R}^{-1}$ es de orden.
   (c) Si $\mathcal{R}$ es refleja y transitiva, entonces $\mathcal{R} \wedge \mathcal{R}^{-1}$ (ver ejercicio 7) es relación de equivalencia.

9. En $\mathbb{R}^2$ se define: $(x,y)R(u,v) \Longleftrightarrow x^2 + y^2 = u^2 + v^2$.
   (a) Demuestre que $\mathcal{R}$ es relación de equivalencia.
   (b) Determine las clases de equivalencia e interprete geométricamente el significado de una clase.

10. En $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ se define la relación $\mathcal{R}$ por:

$$x\mathcal{R}y \Leftrightarrow \frac{x}{y} \in A, \text{ donde } A \subseteq \mathbb{R}.$$

    (a) Probar que $\mathcal{R}$ es una relación de equivalencia si $A = \mathbb{R}$. Encuentre la clase de equivalencia de $\frac{1}{3}$.
    (b) Probar que $\mathcal{R}$ es una relación de orden si $A = \mathbb{N}$. Determine si es relación de orden parcial o total.

11. (a) Dado el conjunto $E = \{a_1, ..., a_n\}$. Determine cuántas relaciones hay en E.
    (b) Cuántas de ellas son reflejas.
    (c) Cuántas son simétricas.
    (d) Cuántas son antisimétricas.
    Observación: para b,c,d piénselo en términos de matrices con 0's y 1's.

12. Sea R y S relaciones de equivalencia en E y F respectivamente. Sobre $E \times F$ se define T: $(x,y)T(x',y') \Longleftrightarrow (x\mathcal{R}x') \wedge (ySy')$. Encuentre las propiedades de T.

13. Sea $\mathcal{R}_k$ definida en $\mathcal{P}(E)$, con $E \neq \phi$, definida por $A\mathcal{R}_K B \Longleftrightarrow B \cap K \subseteq A$, para $K \in \mathcal{P}(E), K \neq \phi$, fijo.
    (a) Pruebe que $\mathcal{R}_K$ es refleja y transitiva.
    (b) Dé condiciones sobre el conjunto K para que $\mathcal{R}_K$ sea antisimétrica.

14. Dadas dos matrices $A, B \in \mathcal{M}_{nn}(\{0,1\})$ qué opinión le merecen las afirmaciones:
    (a) $A \leq B \Longrightarrow \forall X \in \mathcal{M}_{nn}(\{0,1\}), A + X \leq B + X, \ AX \leq BX$.
    (b) Si A no es comparable con B, entonces:

$$-\forall X \in \mathcal{M}_{nn}(\{0,1\}), \ A + X \text{ no es comparable con } B + X.$$
$$-\forall X \in \mathcal{M}_{nn}(\{0,1\}), AX \text{ no es comparable con } BX.$$

    (c) Estudie las propiedades de las relaciones en $\mathcal{M}_{nn}(\{0,1\})$:

$$A\mathcal{R}B \Longleftrightarrow \exists n \in \mathbb{N} \text{ tal que } A^n = B^n = 0 \text{ (matriz nula).}$$
$$A\mathcal{R}B \Longleftrightarrow A \cdot B = I \text{(matriz identidad).}$$

    Observación: Entendemos la suma como sigue: $A = (a_{ij}), \quad B = (b_{ij})$ $A + B = (a_{ij} + b_{ij})$, con $1 + 0 = 0 + 1 = 1 + 1 = 1$ y $0 + 0 = 0$.

15. Considere la relación en $\mathbb{Z}^2$ definida por:

$$(x,y)\mathcal{R}_{(p_1,p_2)}(u,v) \Longleftrightarrow \begin{cases} x = u(mod p_1) \\ y = v(mod p_2) \end{cases}$$

    con p_1 y p_2 en $\mathbb{N}_+$.
    (a) Pruebe que $\mathcal{R}_{(p_1,p_2)}$ es relación de equivalencia.
    (b) Encuentre $\mathbb{Z}/(p_1,p_2)$, el conjunto cociente asociado a la relación.

* 16. Sea $\mathcal{R}$ definida en E, una relación simétrica i.e. $\forall a, b \quad a\mathcal{R}b \Rightarrow b\mathcal{R}a$.
    Definamos una nueva relación en E de la forma siguiente:
    $a\hat{\mathcal{R}}b \Longleftrightarrow \exists n \in \mathbb{N}, \{x_0, ..., x_n\} \in E$ tal que $a = x_0, b = x_n$ y
    $(\forall i = 0, ..., n-1)(x_i\mathcal{R}x_{i+1}) \vee (x_i = x_{i+1})$.
    Demuestre que $\hat{\mathcal{R}}$ es relación de equivalencia.

* 17. Sea E un conjunto no vacío y $\mathcal{R}$ una relación de equivalencia en E. Sea $\phi \neq A \subseteq E$. Se dice que A es "saturado" para $\mathcal{R}$ si y sólo si $\forall x \in A, [x] \subseteq A$.
    (a) Demuestre que si $\{X_i\}_{i \in I}, I \neq \phi$, es una familia de partes saturadas de E, entonces $\bigcup_{i \in I} X_i$ y $\bigcap_{i \in I} X_i$ son saturados.
    (b) Demuestre que A es saturado si y sólo si A es la unión de clases de equivalencias según $\mathcal{R}$.

* 18. Sea $\mathbb{N}^n = \mathbb{N} \times \mathbb{N} \times ... \times \mathbb{N}$, el conjunto de n-tuplas con componentes naturales. Se define: $\forall X, \ Y \in \mathbb{N}^n, \ X = (x_1, ..., x_n), \ Y = (y_1, ..., y_n)$

$$X\mathcal{R}_1 Y \Longleftrightarrow \sum_{i=1}^{k} x_i \leq \sum_{i=1}^{k} y_i \quad \forall k = 1, ..., n.$$

(a) Demuestre que $\mathcal{R}_1$ es relación de orden (¿parcial o total?).
(b) Dada la relación $\mathcal{R}_2$ de orden usual en n-tuplas:

$$\forall X, Y \in \mathbb{N}^n \; X R_2 Y \iff x_i \leq y_i \; \forall i = 1, ..., n.$$

Demuestre que $X\mathcal{R}_2 Y \Rightarrow X\mathcal{R}_1 Y$. Con un contraejemplo indique la falsedad de la implicancia en el otro sentido.

* 19. Sea $\{a, b\}^*$ el conjunto de palabras que se escriben con a's y b's. Por ejemplo, $aaab, babaa, baabbba$, etcétera. Suponga que cada vez que tenga una palabra que contiene ab, usted puede borrar este término. Por ejemplo

$$\underline{ab}\; bbaaa \rightarrow bbaaa$$
$$\underline{ababab} \rightarrow \text{ palabra vacía } v.$$
$$\underline{ab}\; a\; \underline{ab}\; a\; \underline{ab} \rightarrow aa.$$

Estudie la relación:
(a) $\forall w, u \in \{a, b\}^*, \quad w\mathcal{R}u \iff$ al eliminar todos los términos ab posibles se obtiene, en ambos casos, la misma palabra.
(b) Agregue el hecho que, además de borrar ab, se verifica $ab = ba$. Estudie de nuevo la relación anterior y determine el conjunto cociente $\{a, b\}^*/\mathcal{R}$.
(c) Considere ahora que las reglas en $\{a, b\}^*$ son: $a^2 = a \cdot a, \quad b^2 = b \cdot b$ son eliminables y, además, $ab = ba$. Estudie $\mathcal{R}$, el conjunto cociente, etc.
Observación: No olvide, en los tres casos, considerar la palabra vacía $\underline{v}$.

* 20. Sea $(f_n)_{n \geq 0}$ la sucesión de Fibonacci, demuestre que:
(a) $m|n \Rightarrow f_m | f_n$ (Idea: suponga $n = km$ y aplique inducción sobre k).
(b) $\forall n \in \mathbb{N}, mcd(f_n, f_{n+1}) = 1$.
(c) $\forall n, m \in \mathbb{N}, mcd(f_n, f_m) = f_{mcd(m,n)}$.
(Idea: aplique la factorización en cociente y resto para n, m y aplique el algoritmo de Euclides que involucra la descomposición de $m = nq_0 + r_i$).

21. Sea $n \in \mathbb{N}_+$, si n es compuesto (es decir $n = ab, a, b \in \mathbb{N}$), pruebe que $\exists p$, primo tal que $p|n \wedge p \leq \sqrt{n}$.
22. Calcule el $mcd(1154, 322), mcd(236, 28)$.
23. Sea $n = \sum_{i=0}^{k} r_i 10^i$. Pruebe que:

$$2|n \iff 2|r_0$$
$$4|n \iff 4|(r_1 10 + r_0)$$
$$8|n \iff 8|(r_2 10^2 + r_1 \cdot 10 + r_0).$$

¿Cuál es el teorema general?
24. Pruebe que $mcd(a, b) = 1 \Rightarrow mcd(a - b, a + b) \in \{1, 2\}$.
25. Sean $p_1, ..., p_n$ números primos diferentes.
(a) ¿Cuántos divisores tiene el número $q = p_1^{\alpha_1}, ..., p_n^{\alpha_n}$ si $\alpha_1, ..., \alpha_n$ son naturales? (Incluya los divisores 1 y q).
(b) ¿Cuánto vale la suma de los divisores?

TEMAS CAPITULO III

1. Parentesco en la gran pradera.

2. Sobre bases, Euclides y otras hierbas.

3. Congruencias lineales.

4. Grafos y matrices.

5. Agencia matrimonial
   "La Solución".

6. Ordenes son órdenes.

1. Parentesco en la gran pradera.

1. El indio A declara:
   "B y yo somos del mismo Λ"
   o bien
   "Yo soy del mismo Λ que B"
   o aún
   "B es de mi Λ", etc.
2. Se constata que cada vez que A declara "yo soy el mismo Λ que B", al interrogar a B éste dirá "A y yo somos del mismo Λ".
   Luego la relación notada Λ es simétrica:
   "A y B declaran mutualmente ser del mismo Λ".
3. La experiencia confirma que la relación es transitiva:
   si A y B declaran ambos ser de Λ y si B y C se declaran ambos en Λ entonces A y C declaran ser del mismo Λ.
4. Algunas declaraciones relativas a Λ se explican por relaciones de parentesco. Todo indio afirma:
   "mi madre y yo estamos en Λ";
   de esto se deduce
   que "dos hermanos de la misma madre están necesariamente en el mismo Λ".
   En efecto, si A, B son hermanos de madre:
   A está en el mismo Λ que su madre y la madre está en el mismo Λ que su hijo B, luego, de la propiedad 3 (transitividad):
   "A y B están en el mismo Λ"

¿Qué puede decir de la hermana de la madre de A?
¿Qué puede decir sobre la afirmación: "Cada indio (hombre o mujer) declara estar en el mismo Λ que los hijos de su tía materna"?

Resumiendo, en la tribu hemos constatado las siguientes propiedades:
(1) Todo individuo y su madre declaran ser del mismo Λ.
(2) Λ es *transitiva*.
(3) Nadie declara Λ si no es utilizando (1) y (2).
(4) En un matrimonio los cónyuges deben ser de la misma generación.
(5) Todo hombre afirma:
   "mi hijo y el padre de mi padre declaran ser del mismo Λ"

De estas reglas es trivial que la regla (5) se deduce de (1) y (2) (¿por qué?, ¿cómo?, invente alternativas plausibles). No tan directo es que:

un individuo h debe elegir esposa del mismo Λ y generación que la hija de la hija de la hermana del padre de su padre.

En efecto, si el individuo h tiene un hijo puede afirmar que

la madre de su hijo y su hijo está en el mismo Λ

o bien que:

"*su esposa y su hijo están en el mismo* Λ",

pero en virtud de (5)

"*su hijo y el padre de su padre están en el mismo* Λ';

por transitividad:

"*su esposa y el padre de su padre están en el mismo* Λ".

Por otra parte, sabemos que:

el padre de su padre y la hermana del padre de su padre están en el mismo Λ.

Luego, por transitividad:

su esposa y la hermana del padre de su padre están en el mismo Λ.

Como sabemos por (1) que todo individuo está en el mismo Λ que su madre:

su esposa y la hija de la hermana del padre de su padre están en el mismo Λ, y por la misma propiedad:

su esposa y la hija de la hija de la hermana del padre de su padre están en el mismo Λ.

Además, la hija de la hija de la hermana del padre de su padre es de su misma generación.
En efecto:

Generación 1:	padre del padre de h	hermana del padre del padre de h
Generación 2:	padre de h	hija de la hermana del padre del padre de h
Generación 3:	h	hija de la hija de la hermana del padre del padre de h

Luego concluímos

Que una candidata a esposa de h debe pertenecer al mismo Λ y generación que la hija de la hija de la hermana del padre del padre del presunto marido ■

Ejercicio.

1. Salga a dar una vuelta a la manzana, tome aire hasta despejar las meninges y construya otro modelo en el cual se cambia la propiedad (5) por:
   (5') "*Mi hijo y mi padre afirman ser del mismo* Λ"
   o bien
   (5") "*Mi hijo y mi abuelita son de distinto* Λ"
   Analice, en cada caso, si no hay contradicciones con las otras propiedades. De no haberlas, deduzca reglas de matrimonio, tabúes incestuosos, etcétera, etcétera.
   Salga ahora definitivamente a dar dos vueltas a la manzana. Tome aire.

2. Sobre bases, Euclides y otras hierbas.

2.1. Expresión de un número en base b.

Dado $b \in \mathbb{N}$, expresemos $a \in \mathbb{N}$ en función de las potencias de b, $\{b^0, b^1, b^2, ..\}$. Esto lo podemos hacer mediante la utilización reiterada del algoritmo de la división. En efecto, dividiendo a por b:

$$a = bq_0 + r_0 \qquad 0 \leq r_0 < b$$

si $q_0 > 0$, dividimos q_0 por b:

$$q_0 = bq_1 + r_1 \qquad 0 \leq r_1 < b$$

obteniendo

$$\begin{aligned} a &= b(bq_1 + r_1) + r_0 \\ &= b^2 q_1 + br_1 + r_0 \end{aligned}$$

si $q_0 = 0 \Rightarrow$ ALTO
si $q_1 > 0$, dividimos q_1 por b:

$$q_1 = bq_2 + r_2 \qquad 0 \leq r_2 < b$$

obteniendo

$$\begin{aligned} a &= b^2(bq_2 + r_2) + br_1 + r_0 \\ &= b^3 q_2 + b^2 r_2 + br_1 + r_0 \end{aligned}$$

En el paso $i = 1$, si $q_{i-1} > 0$:

$$q_{i+1} = bq_i + r_i \qquad 0 \leq r_i < b$$

obteniendo $a = b^{i+1} q_i + b^i r_i + b^{i-1} r_{i-1} + ... + br_1 + r_0$

Supongamos $q_n = 0$, ergo:

$$q_{n-1} = b \cdot 0 + r_n$$

obteniendo $a = b^n r_n + b^{n-1} r_{n-1} + ... + br_1 + b^0 r_0$. O bien

,

$$a = \sum_{i=0}^{n} r_i b^i, \; r_i \in \{0, ..., b-1\} \tag{3.35}$$

denominada *expresión de a en base b*, cuya notación es

$$a = (r_n r_{n-1} r_{n-2} ... r_1 r_0)_b.$$

Ejemplo. Sea $a = 1432$. Expresemos este número en base 2:

$$\begin{aligned} 1432 &= \\ &= 2 \cdot 716 + 0 \\ &= 2 \cdot [2 \cdot 358 + 0] + 0 \\ &= 2^2 \cdot 358 \\ &= 2^2(2 \cdot 179) = 2^3 \cdot 179 \\ &= 2^3(2 \cdot 89 + 1) \\ &= 2^4 \cdot 89 + 2^3 \\ &= 2^4(2 \cdot 44 + 1) + 2^3 \\ &= 2^5 \cdot 44 + 2^4 + 2^3 \\ &= 2^6 \cdot 22 + 2^4 + 2^3 \\ &= 2^7 \cdot 11 + 2^4 + 2^3 \\ &= 2^7(2 \cdot 5 + 1) + 2^4 + 2^3 \\ &= 2^8(2 \cdot 2 + 1) + 2^7 + 2^4 + 2^3 \\ &= 2^{10} + 2^8 + 2^7 + 2^4 + 2^3 \\ &= 1 \cdot 2^{10} + 0 \cdot 2^9 + 1 \cdot 2^8 + 1 \cdot 2^7 + 0 \cdot 2^6 + 0 \cdot 2^5 \\ &\quad + 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0 \\ &\equiv (1\,0\,1\,1\,0\,0\,1\,1\,0\,0\,0)_2 \text{ (representación en base 2).} \end{aligned}$$

Representemos el mismo número en base 10:

$$\begin{aligned} 1432 &= 10 \times 143 + 2 = 10(10 \times 14 + 3) + 2 \\ &= 10^2 \cdot 14 + 3 \cdot 10 + 2 = 10^2(10 \times 1 + 4) + 3 \cdot 10 + 2 \\ &= 10^3 + 4 \cdot 10^2 + 3 \cdot 10 + 2 \cdot 10^0 \equiv (1432)_{10} \end{aligned}$$

En este último caso la expresión en base 10 coincide con la notación que utilizamos a diario.

Terminemos señalando que el algoritmo para determinar la expresión de a en base a b converge en un número finito de pasos. Basta observar que:

$$q_{i-1} > q_i \geq 0, \quad q_j \in \mathbb{N}$$

luego, en un número finito de "divisiones" encontramos un valor $q_n = 0$ ■

Veamos ahora una relación entre $n \in \mathbb{N}$ y el número de dígitos que lo representa en base $b > 0$. Por ejemplo $n = 4534$ tiene 4 dígitos en base 10.

Sea $d(n,b)$ = número de dígitos de n en base b. Supongamos $d(b,n) = k$:

$$n = (a_{k-1}a_{k-2}...a_1a_0)_b, \quad a_{k-1} \geq 1$$

o bien $n = \sum_{j=0}^{k-1} a_j b^j$.

Luego, $n \geq a_{k-1}b^{k-1} \geq b^{k-1}$, concluyendo:

$$k - 1 \leq log_b n,$$

de donde $d(n,b) \leq log_b n + 1$ ■

2.2. Complejidad Euclidiana.

Sabemos que el algoritmo de Euclides converge en un número finito de pasos (ver punto 3.7.2), pero esto desde el punto de vista práctico no es suficiente. Daremos acá una cota más satisfactoria para la convergencia.

Sean $a, b \in I\!N$, $a > b$, demostraremos que el número de pasos del algoritmo de Euclides necesarios para calcular $mcd(a,b)$ es menor que cinco veces el número de dígitos del menor entero, b:

(pasos de Euclides)$\leq 5 \cdot$ *(dígitos de b en base 10).* (3.36)

Esta "joyita" fue "encontrada" (¿determinada?) en 1844 por el matemático Gabriel Lamé. Entregaremos acá una bella demostración aparecida posteriormente en la revista American Mathematical Monthly (31, 1924).

Supongamos que $n \in I\!N$ sea exactamente el número de pasos para el cálculo de $mcd(a_{n+1}, a_n), a_{n+1} > a_n$. En el esquema del algoritmo:

$$\begin{array}{ll}
a_{n+1} = q_n a_n + a_{n-1} & 0 < a_{n-1} < a_n \\
a_n = q_{n-1}a_{n-1} + a_{n-2} & 0 < a_{n-2} < a_{n-1} \\
\vdots \qquad \vdots & \vdots \\
a_4 = q_3 a_3 + a_2 & 0 < a_2 < a_3 \\
a_3 = q_2 a_2 + a_1 & 0 < a_1 < a_2 \\
a_2 = q_1 a_1 + 0, & a_1 = mcd(a_{n+1}, a_n)
\end{array}$$

Es claro que $q_1 \geq 2$ (sino $a_1 = a_2$). Luego podemos acotar los valores, a_i, desde la última a la primera ecuación:

$$\begin{array}{l}
q_1 \geq 2, a_1 \geq 1 \Rightarrow a_2 \geq 2 \cdot 1 = 2 \\
q_2 \geq 1, a_1 \geq 1, a_2 \geq 2 \Rightarrow a_3 \geq 1 \cdot 2 + 1 = 3 \\
q_3 \geq 1, a_3 \geq 3, a_2 \geq 2 \Rightarrow a_4 \geq 1 \cdot 3 + 2 = 5
\end{array}$$

En general, $a_j \geq a_{j-1} + a_{j-2}, a_1 \geq 1, a_2 \geq 2$. Desigualdad que es similar a la sucesión de Fibonacci (ver Tema 4, párrafo 4.3, capítulo II):

$$x_j = x_{j-1} + x_{j-2}, x_1 = 1, x_2 = 2$$

Es decir: $1, 2, 3, 5, 8, 13, 21, 34, 55, ...$ Luego $a_1 \geq x_1, a_2 \geq x_2, ..., a_n \geq x_n$. Además, en Fibonacci:

$$x_{n+5} > 10x_n$$

o, de manera equivalente, el término de orden $n+5$ tiene, al menos, un dígito más, en base 10, que el término n-ésimo.

Esto se verifica por recurrencia:
es cierto para $n = 1, x_6 = 13 > 10 \cdot 1 = 10$.

Supongamos cierto para $k \leq n$ y demostremos para $n + 1$:

$$\begin{array}{l}
x_{n+1+5} = x_{n+5} + x_{n+4} = x_{n+5} + x_{n-1+5} \\
\qquad > 10x_n + 10x_{n-1} = 10(x_n + x_{n-1}) = 10x_{n+1}
\end{array}$$ ■

Por otra parte, se tiene que:

$$\begin{array}{ll}
0 < n \leq 5 & x_n \text{ tiene al menos un dígito} \\
5 < n \leq 2 \cdot 5 & x_n \text{ tiene al menos dos dígitos} \\
\vdots & \\
k \cdot 5 < n \leq (k+1) \cdot 5 & x_n \text{ tiene al menos } k+1 \text{ dígitos.}
\end{array}$$

En efecto, esto se demuestra también por recurrencia: por inspección de la sucesión, se verifica en el intervalo $0 < n \leq 5$. Supongamos cierto para $(k-1) \cdot 5 < n \leq k \cdot 5$ y demostremos para el siguiente intervalo; $k \cdot 5 < n \leq (k+1)5$.
Se tiene $x_{k \cdot 5+1} > 10 \cdot x_{k \cdot 5+1-5} = 10x_{k \cdot 5-4}$
como $k \cdot 5 - 4 > (k-1)5, x_{k \cdot 5-4}$ tiene al menos k dígitos, luego, $x_{k \cdot 5+1}$ tiene al menos $k+1$ dígitos ■

Finalmente, dado $n \in \mathbb{N}, \exists k \in \mathbb{N}$ tal que

$$k \cdot 5 < n \leq (k+1)5,$$

luego x_n tiene al menos $(k+1)$ dígitos. Como $a_n \geq x_n$ entonces a_n tiene al menos $k+1$ dígitos, de donde:

$$5 \cdot (\text{número de dígitos de } a_n) \geq 5 \cdot (k+1)$$

luego, $n \leq 5 \cdot (k+1) \leq 5$ (dígitos de a_n), lo cual demuestra el resultado ■

Para terminar, recordemos que el número de dígitos del entero a_n en base 10 está acotado por:

$$d(a_n, 10) \leq log_{10} a_n + 1$$

concluyendo que el número de pasos, t_{ab}, del algoritmo de Euclides aplicado al par $(a, b), b > a$, está acotado por:

$$t_{ab} \leq 5(log_{10} a + 1). \tag{3.37}$$

Ejercicios.

1. Represente 30421 y 542 en bases:
   (a) 2 (b) 10 (c) 16.

3. Congruencias lineales.

Consideremos el conjunto de enteros $\mathbb{Z}$ con la relación $\equiv$ de congruencia módulo p; sabemos que es relación de equivalencia y el conjunto cociente es

$$\mathbb{Z}_p = \{[0], [1], ..., [p-1]\}.$$

Nos interesan algunas propiedades de $\equiv$.

Propiedades evidentes:

1) $a \equiv b(modp) \Rightarrow a + n \equiv b + n(modp) \quad \forall n \in \mathbb{Z}$.
2) $a \equiv b(modp) \wedge c \equiv d(modp) \Rightarrow a + c \equiv b + d(modp) \quad ac \equiv bd(modp)$.

La demostración de 1 es directa:

$$a \equiv b(modp) \Leftrightarrow a - b = kp \Rightarrow a + n - n - b = kp$$

$$\Leftrightarrow a + n - (b + n) \equiv kp \Leftrightarrow a + n \equiv b + n(modp).$$

Para la propiedad 2: $(a - b = k_1 p) \wedge (c - d = k_2 p)$, luego,
$(a + c) - (b + d) = (k_1 + k_2)p$ ■

Una propiedad más delicada e interesante es la siguiente:

Teorema.

1) *La ecuación de congruencia $ax \equiv b(modp)$ en la incógnita x tiene solución si y sólo si $mcd(a, p)|b$.*

2) *Además, si $mcd(a, p)|b$ el número de soluciones no congruentes entre ellas es exactamente $mcd(a, p)$.*

Demostración:

Parte 1: $\Rightarrow$) Sea x_o una solución $\Rightarrow \exists k \in \mathbb{Z}$ tal que

$$ax_o = b + kp \Rightarrow b = ax_o - kp$$

pero $mcd(a, p)$ divide a y $p \Rightarrow mcd(a, p)|b$

$\Leftarrow$) Supongamos que $mcd(a,p)|b$, por definición de Máximo Común Divisor, existen k_1, k_2 tales que

$$a = k_1 mcd(a,p)$$
$$p = k_2 mcd(a,p)$$

Además, como $mcd(a,p)|b \Rightarrow \exists k_3$ tal que $b = k_3 mcd(a,p)$.

Por otra parte $mcd(k_1,k_2) = 1$, pues $mcd(a,p)$ es el mayor entero que divide a y p, luego existen $\alpha, \beta \in \mathbb{Z}$ tales que:

$$\alpha k_1 + \beta k_2 = 1$$

entonces:

$$b\alpha k_1 + b\beta k_2 = b;$$

por lo tanto,

$$b = k_3 mcd(a,p)\alpha k_1 + k_3 mcd(a,p)\beta k_2$$
$$b = \alpha k_3 a + \beta k_3 p$$

de donde,

$$(\alpha k_3)a = b + (-\beta k_3)p$$

o de manera equivalente,

$$(\alpha k_3)a \equiv b(mod p).$$

Es decir, $x_o = \alpha k_3$ es solución de la congruencia. ■

Demostremos ahora la parte 2:

Si x_o es solución, $ax_o = b + k_1 p$. Sea $n \in \mathbb{Z}$

por lo tanto,

$$ax_o + \frac{nap}{mcd(a,p)} = b + k_1 p + \frac{nap}{mcd(a,p)}$$

$$a(x_o + n\frac{p}{mcd(a,p)}) = b + (k_1 + n\frac{a}{mcd(a,p)})p,$$

$$\text{pero } mcd(a,p)|a \Rightarrow k_1 + n\frac{a}{mcd(a,p)} \in \mathbb{Z}.$$

Luego, $a(x_o + n\frac{p}{mcd(a,p)}) \equiv b(mod p)$.

Es decir, x_o es solución $\Rightarrow x_o + n\frac{p}{mcd(a,p)}$ es solución.

De esta manera tenemos que el conjunto de soluciones es:

$$\{x_o + n\frac{p}{mcd(a,p)}\}_{n\in\mathbb{Z}}. \tag{3.38}$$

¿ Falta alguna solución?

Supongamos x_1 una solución, luego $ax_1 \equiv b(mod p)$. Como además x_0 es solución

$$-ax_0 \equiv -b(mod p)$$

es decir,

$$a(x_1 - x_0) \equiv 0(mod p)$$

de donde,

$$ax_1 = ax_0 + kp,$$

$$\text{pero } a = k_1 mcd(a,p), \quad p = k_2 mcd(a,p) \tag{3.39}$$

por lo tanto, $k_1 mcd(a,p)x_1 = k_1 mcd(a,p)x_0 + kk_2 mcd(a,p)$, que implica las relaciones

$$k_1 x_1 = k_1 x_0 + kk_2$$
$$k_1(x_1 - x_o) = k \cdot k_2$$

luego, $k_1|k \cdot k_2$. El hecho que $mcd(k_1,k_2) = 1 \Rightarrow \quad k_1|k$ (ver (3.39)).

Sea $k = k_3 k_1 \Rightarrow x_1 - x_o = k_3 k_2$ por lo tanto, $x_1 = x_o + k_3 k_2$, pero $k_2 = \frac{p}{mcd(a,p)}$, luego:

$$x_1 = x_0 + k_3\frac{p}{mcd(a,p)} \in \{x_o + n(\frac{p}{mcd(a,p)})\}_{n\in\mathbb{Z}}$$

luego, en este conjunto están todas las soluciones ■

Es directo ver que

$$x_o \equiv x_o + mcd(a,p)\frac{p}{mcd(a,p)}(mod p)$$

de donde las únicas soluciones eventualmente no equivalentes son:

$$\{x_o, x_o + \frac{p}{mcd(a,p)}, ..., x_o + (mcd(a,p) - 1)\frac{p}{mcd(a,p)}\}. \tag{3.40}$$

Efectivamente, si

$$x_o + k\frac{p}{mcd(a,p)} \equiv x_o + k'\frac{p}{mcd(a,p)}(mod p)$$

$$0 \leq k' \leq k \leq mcd(a,p),$$

obtenemos:

$$(k-k')\frac{p}{mcd(a,p)} = \alpha p,$$

de donde,

$$\frac{k-k'}{mcd(a,p)} = \alpha,$$

pero

$$k - k' \leq mcd(a,p) \Rightarrow k = k' \quad \blacksquare$$

Ejemplo:

Resolvamos la ecuación en $x : (16x+1) \equiv 9(mod 4)$. Escribámosla de la forma $ax \equiv b(mod p)$:

$$\begin{aligned} & 16x + 1 \equiv 9(mod 4) \\ \Longleftrightarrow & (16x+1) - 9 = k \cdot 4, \text{para algún } k + \mathbb{Z} \\ \Longleftrightarrow & 16x - 8 = k \cdot 4, \text{para algún } k \in \mathbb{Z} \\ \Longleftrightarrow & 16x \equiv 8(mod 4). \end{aligned}$$

Del teorema que caracteriza la existencia de soluciones para este tipo de ecuación, se tiene:

1) Como $mcd(16,4) = 4 | b = 8$, la ecuación tiene solución.
2) Encontraremos 4 soluciones no congruentes entre ellas.

Podemos determinar una solución particular de la ecuación probando $k = 1, 2, ...,$ en $16x - 8 = k \cdot 4$. Vemos que si $k = 2, x = 1$. En el sentido de nuestro interés, $x = 1 (\in \mathbb{Z})$ es solución, pues $16 \equiv 8(mod 4)$. Luego, el conjunto solución es $\{1+n\}_{n \in \mathbb{N}}$ (ver (3.38)) y las soluciones no congruentes (ver (3.40)) serán

$$\{1, 1+1, 1+2, 1+3\} = \{1, 2, 3, 4\}.$$

Ejercicios.

1) Encuentre, si es posible, la solución de las siguientes ecuaciones:
   (a) $12x \equiv 42(mod 6)$
   (b) $(17x+3) \equiv 8(mod 5)$,
   (c) $(5n)y \equiv (n^5 - n)(mod 5)$, si $n = 1, 2, 3$ y 4.

2) (a) Pruebe que las soluciones no congruentes de la ecuación "homogénea" $ax \equiv 0(mod p), a \neq 0$, son

$$\{0, \frac{p}{mcd(a,p)}, \frac{2p}{mcd(a,p)}, ..., (mcd(a,p)-1)\frac{p}{mcd(a,p)}\}.$$

   (b) Deduzca de (3.40) que toda solución del conjunto de soluciones no congruentes entre si de la ecuación $ax \equiv b(mod p)$ se escribe como la suma de una solución particular y una solución de la ecuación "homogénea" $ax \equiv 0(mod p)$.

* 3) (a) ¿Se atrevería a caracterizar las soluciones de un sistema de congruencias

$$(ax + by) \equiv e(mod p_1)$$
$$(cx + dy) \equiv f(mod p_2)$$

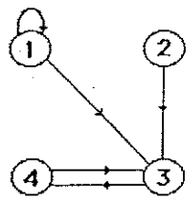
para $p_1, p_2 \in \mathbb{N} \setminus \{0\}$?
   (b) Puede ayudarle resolver el sistema particular:

$$(x + 2y) \equiv 6(mod 2)$$
$$(3x + y) \equiv 6(mod 3).$$

4. Grafos y matrices.

Sea $G = (U, V)$ un grafo, donde $U = \{1, ..., n\}$ es el conjunto de nodos y $V \subset U \times U$ es el conjunto de arcos.

Ejemplo: $G = (\{1,2,3,4\}, \{(1,1),(1,3),(2,3),(3,4),(4,3)\})$



Obviamente G define una relación trivial sobre U:
$i\mathcal{R}j \Leftrightarrow (i,j) \in V$. Además las matrices asociadas a G y $\mathcal{R}$ son las siguientes:

$$M(G) = M(\mathcal{R}) = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

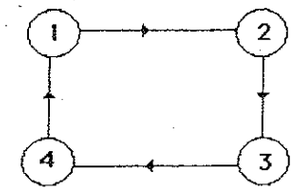
Por otra parte dada una matriz $A \in M_{nn}(\{0,1\})$, siempre es posible asociarle una relación y un grafo:

$$i\mathcal{R}j \Leftrightarrow a_{ij} = 1 \Leftrightarrow \text{ existe el arco } i \to j.$$

Claramente, el dominio de esta relación es $R = \{(i,j)/a_{ij} = 1 \quad 1 \leq i,j \leq n\}$.

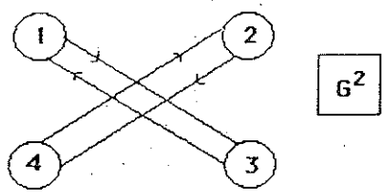
La matriz asociada a un grafo se denomina la *matriz de incidencia* de G.

Ejemplo: Sea $G^1 = (U, V_1)$.



$$M(G) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

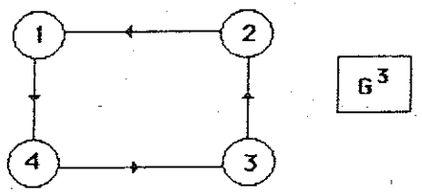
Construyamos a partir de G^1 el grafo $G^2 = (U, V_2)$ con nodos $U = \{1,2,3,4\}$ tal que $(i,j) \in V_2 \Leftrightarrow \exists$ un camino orientado de largo dos entre i y j en el grafo $G^1 \Leftrightarrow \exists k \in U$ tal que $(i,k) \in V_1 \wedge (k,j) \in V_1$.



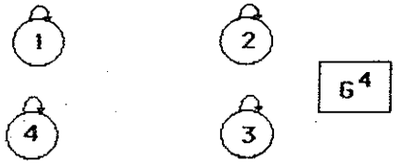
De manera análoga: $G^3 = (U, V_3)$

$(i,j) \in V_3 \Leftrightarrow \exists k_1, k_2 \in U$ tales que $(i,k_1) \in V_1 \wedge (k_1,k_2) \in V_1 \wedge (k_2,j) \in V_1$

$\Leftrightarrow \exists$ algún camino de largo 3 entre i y j.



De manera análoga G^4:



En general: dado $G = (U, V)$, definimos $G^m = (U, V_m)$ tal que $(i, j) \in V_m \Leftrightarrow$ existe un camino de largo m entre i y j, donde

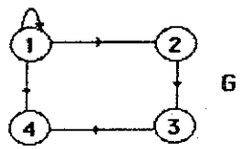
$$(i, k_1), (k_1, k_2), (k_2, k_3), ..., (k_{m-1}, j)$$

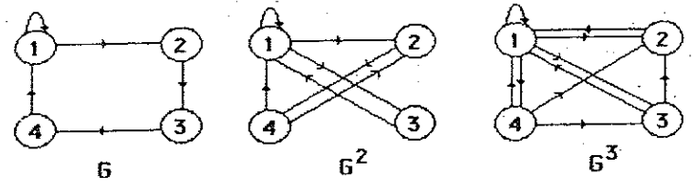
son arcos del grafo inicial.

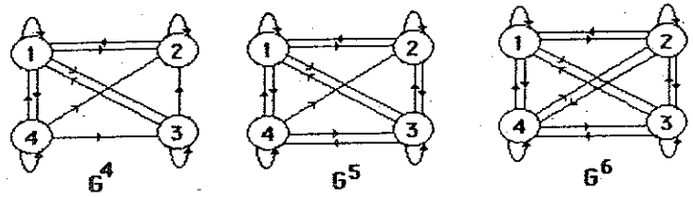
Del mismo ejemplo anterior es fácil ver que $G^5 = G^1, G^6 = G^2$, $G^7 = G^3$, $G^8 = G^4$,... Es decir, engendramos la sucesión de grafos que se repiten periódicamente de 4 en 4.

$$G = G^1, G^2, G^3, G^4, G^1, G^2, G^3, G^4, G^1, G^2, G^3, G^4, ...$$

Si hacemos lo mismo para el siguiente grafo G:







Grafo Completo contiene todos los arcos

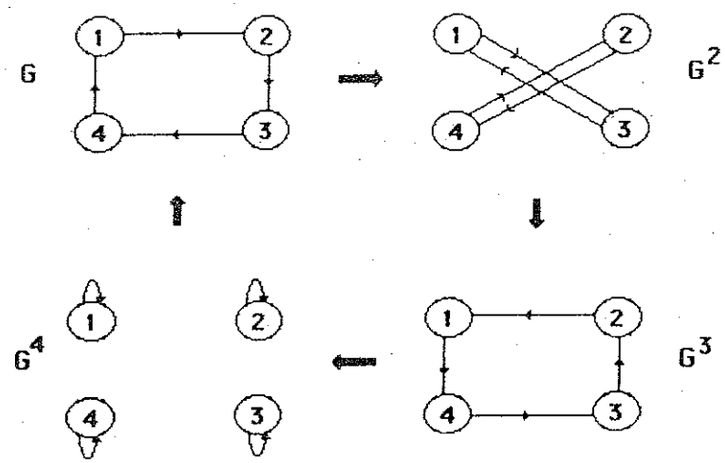
es fácil ver que, como existen caminos de largo 6 entre cualquier par de nodos y como necesariamente todos pasan por el nodo 1, existen caminos de largo arbitrario.

En el ejemplo, la sucesión de grafos es:

$$G = G^1, G^2, G^3, G^4, G^5, G^6 = K_6, K_6, K_6....$$

donde K_6 denota el grafo completo (están todos los arcos posibles).

Esta manera de calcular G^k es incómoda. Tratemos de utilizar la notación matricial; en el primer ejemplo se tiene:



y las matrices

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

$$M^2 = M \cdot M = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

$y...G(M^2) = G^2$ (donde $G(M)$ es el grafo asociado a la matriz M);
$M^2 = M(G^2)$ (¡¡¡ resultados notables !!!).

Sigamos con el cubo de la matriz M:

$$M^3 = M^2 M = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$= M(G^3)$$

$$M^4 = M^3 M = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = I = M(G^4).$$

Es decir, dado $G = (U, V)$),

$$M(G^p) = M^p(G) \qquad \forall p \geq 1.$$

Formalmente, si $M^p(G) = (m_{ij}^{(p)})$,

$$m_{ij}^{(p)} = 1 \Leftrightarrow \exists \textit{ al menos un camino de largo } p \textit{ en el grafo } G = (U, V). \tag{3.41}$$

Demostraremos esto por inducción, sobre p, la potencia de la matriz.
Es cierto para $p = 1$:

$$M(G) = (m_{ij})$$
y $m_{ij} = 1 \Leftrightarrow \exists$ arco $i \to j$ (camino de largo 1).

Supongamos que es cierto para p y demostremos para $p + 1$.

$$M^{p+1}(G) = M^p(G) \cdot M(G)$$

luego $\forall i, j = 1, ..., p$:

$$m_{ij}^{(p+1)} = \sum_{k=1}^{n} m_{ik}^{(p)} \cdot m_{kj},$$

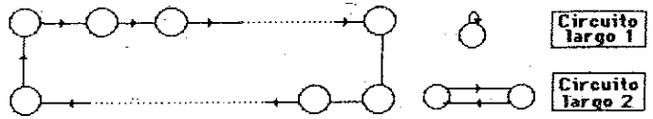
por lo tanto, $m_{ij}^{(p+1)} = 1 \Leftrightarrow \sum_k m_{ik}^{(p)} m_{kj} = 1 \Leftrightarrow \exists \ell \in \{1, ..., p\}$
tal que $m_{i\ell}^{(p)} m_{\ell j} = 1 \Leftrightarrow m_{i\ell}^{(p)} = 1 \wedge m_{\ell j} = 1$.

Por hipótesis de inducción:
$\Leftrightarrow$ ($\exists$ camino de largo p entre i y ℓ)$\wedge$ (un arco entre ℓ y j).

$\Leftrightarrow \exists$ camino de largo $p+1$ entre i y j ■

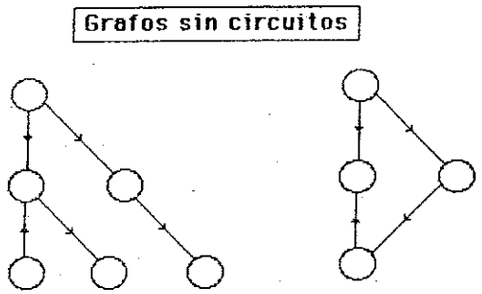
Ejercicios.

1. Diremos que el grafo G, con n nodos, tiene circuitos si existe al menos un nodo que admite un camino circular:



Demuestre que:

$$G \text{ no tiene circuitos } \Leftrightarrow M^n(G) = 0$$



2. Demuestre que si en el grafo existe un camino entre cualquier par de nodos y si además $M(G) \geq I$ entonces:

$$\text{existe un natural } q, \text{ tal que } M^q(G) = \begin{pmatrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{pmatrix}$$

Dé alguna cota superior para q.

3. Dado $G = (U, V), U = \{1, ..., n\}$ y $V \subseteq U \times X$, tal que

$$(\forall j \in U)[(\exists! k \in U)((j,k) \in V) \wedge (\exists! i \in U)(i,j) \in V].$$

Se define sobre U la relación $\mathcal{R}$ como:
$i\mathcal{R}j \Longleftrightarrow (\exists i_1, i_2, ..., i_{p-1} \in U)\ (\{(i,i_1),(i_1,i_2),...,(i_{p_1},i_p),(i_p,j)\} \subseteq V)$.
(a) Dé una interpretación para $\mathcal{R}$.
(b) Demuestre que $\mathcal{R}$ es relación de equivalencia.

4. Un grafo $G = (U, V)$ se llama conexo si todo par de nodos $i, j \in U$ están conectados, es decir si existe un camino de i a j (o viceversa).
(a) ¿Cuál es la relación asociada a un grafo que no es conexo?
(b) Si $|U| = n$, ¿cuál es el número mínimo de arcos en V, si G es conexo?

5. Dado $G = (U, V)$ con matriz de incidencia $M = M(G)$ y $|U| = n$, diremos que hay un camino desde el nodo i hasta el nodo j si y sólo si $(\exists k \geq 0)\ (m_{ij}^{(k)} = 1)$. Además, diremos que i y j están en el mismo circuito si y sólo si existe un camino desde i hasta j y uno de j hasta i. Considere la relación, $\mathcal{R}$, definida sobre U, donde $i\mathcal{R}j$ si y sólo si i está en el mismo circuito que j.
(a) Pruebe que $i\mathcal{R}j \Leftrightarrow \sum_{k=0}^{n} m_{ij}^{(k)} = \sum_{k=0}^{n} m_{ji}^{(k)} = 1$ (donde la sumatoria actúa en $\mathbb{R}$).
(b) Pruebe que $\mathcal{R}$ es relación de equivalencia.

* 6. Sean $M \in M_{nn}(\{0,1)\})$ tal que en cada fila y en cada columna de M hay exactamente un 1 (y el resto es 0). Pruebe que existe $k > 1, k \in \mathbb{N}$, tal que $M^k = M$.

5. Agencia matrimonial "La Solución".

Supongamos dos conjuntos finitos:

$$H = \{H_1, ..., H_n\}$$

$$M = \{m_1, ..., m_n\}$$

de n hombres y n mujeres respectivamente (la elección de mayúsculas y minúsculas no implica ningún machismo).

Definiremos como un "casorio" la celebración de n matrimonios entre los varones del conjunto H y las damas de M.

Como se trata de nuestra sociedad, supondremos un estricto cumplimiento de la monogamia y nos limitaremos a matrimonios entre dos individuos de sexo opuesto.

Supongamos también que nuestra "sociedad", de $2n$ individuos, es lo suficientemente "cuadrada" como para que:

Cada hombre o mujer tenga clasificados, por orden de preferencia, a todos los elementos de sexo contrario.

Por ejemplo. Sean $H = \{A, B, C, D\}$ y $M = \{a, b, c, d\}$ y consideremos las siguientes tablas de preferencia:

	1	2	3	4
A	c	b	d	a
B	b	a	c	d
C	b	d	a	c
D	c	a	d	b

Tabla de preferencias de varones.

	1	2	3	4
a	A	B	D	C
b	C	A	D	B
c	C	B	D	A
d	B	A	C	D

Tabla de preferencias de damas.

Desde la prehistoria, la inestabilidad acecha a toda pareja, ergo, es realista introducir en nuestro modelo una noción de "emparejamiento o casorio" inestable.

Supongamos que se tienen los n matrimonios legales entre los conjuntos H y M. Diremos que este "casorio" es *inestable* si y sólo si:

"Un hombre y una mujer no casados entre ellos se prefieren mutuamente, en lugar de sus respectivos conyuges legales"

En términos formales, diremos que el casorio es *inestable* si y sólo si:

$$(\exists X, Y \in H) \wedge (x, y \in M),$$

tales que

Xx, Yy son dos parejas legales, de manera que:

$$\begin{array}{l} X \text{ prefiere } y \text{ a su esposa } x \\ y \text{ prefiere } X \text{ a su esposo } Y. \end{array} \tag{3.42}$$

En caso contrario, es decir si no existen parejas disconformes, diremos que el casorio es *estable.*

De las tablas anteriores tenemos que el casorio:

$$Aa \quad Bb \quad Cc \quad Dd \quad \text{es inestable.}$$

En efecto: A prefiere b antes que a, b prefiere A antes que B.

Con respecto a este problema, algunas preguntas astutas y no triviales son las siguientes:

Dadas las tablas de preferencia ¿existe siempre un casorio estable?
Si la respuesta es afirmativa,
¿existe algún procedimiento para determinar uno de ellos?
Si existe algún casorio estable, ¿es éste único?
Si existen varios casorios estables, ¿cuántos son?

Aquí responderemos afirmativamente a la primera pregunta. Para ello construiremos una solución mediante un procedimiento aplicable a cualquier par de tablas de preferencia. Es decir; ¡mataremos dos pájaros de un tiro!

Esto no siempre es usual en matemáticas. En ocasiones demostramos que un problema tiene solución, pero no se tiene manera de explicitar una solución...

Ejercicio: Dé algún ejemplo donde se demuestre la existencia de una solución y ésta no sea explícita.

Antes de dar este procedimiento analicemos un método basado en el sentido común. Para ello tomemos las tablas de preferencia:

A	c	b	d	a
B	b	a	c	d
C	b	d	a	c
D	c	a	d	b

a	A	B	D	C
b	C	A	D	B
c	C	B	D	A
d	B	A	C	D

Supongamos que inicialmente se tiene el casorio Aa, Bb, Cc, Dd.

Claramente:

A prefiere b a su esposa a

b prefiere A a su esposo B.

Luego el sentido común diría:

"pues, que se divorcien y se casen".

Si a esto agregamos que a menudo los mutuos despechados en amor suelen curar sus penas en el amor mutuo, diríamos

"pues, que se casen también".

Tendríamos entonces la siguiente dinámica de casamientos y divorcios:

$$\begin{array}{cccc} \underline{A}a & B\underline{b} & Cc & Dd \\ A\underline{b} & Ba & \underline{C}c & Dd \end{array}$$

Pero b aún no está conforme con su media naranja A: ella prefiere a C y, cosas del amor, C también la prefiere:

"pues, que todo se desarme y se casen de nuevo".

Siguiendo el cruel devenir de los corazones solitarios

$$\begin{array}{cccc} \underline{A}a & B\underline{b} & Cc & Dd \\ A\underline{b} & Ba & \underline{C}c & Dd \\ A\underline{c} & Ba & Cb & \underline{D}d \\ Ad & Ba & Cb & Dc \end{array}$$

y este último es un casorio estable.

En efecto.

Listamos la lista de parejas que cada hombre o mujer prefiere a la suya:

A	c, b		a	A
B	b		b	óptimo
C	óptimo	(hizo su mejor elección)	c	C, B
D	óptimo		d	B;

ahora bien,

$$\begin{cases} \text{Si } A \text{ hace "avances" a } c, \\ c \text{ lo ignora pues prefiere a su marido } D. \end{cases}$$

$$\begin{cases} \text{Si } A \text{ hace "avances" a } b, \\ b \text{ lo ignora pues } C \text{ es su príncipe azul} \\ \text{(el primero de su lista)}, \end{cases}$$

luego, A no puede divorciarse.

$$\begin{cases} \text{Si } B \text{ le guiña el ojo a } b, \\ b \text{ le da filo ya que } C \text{ es su príncipe azul.} \end{cases}$$

En cuanto a C y D, éstos se casaron con la mejor de sus preferencias, luego, no miran a nadie.

De manera análoga, ninguna mujer podrá divorciarse (¡verifíquelo!), ergo, el casorio en cuestión es estable ■

Pero el éxito de nuestro procedimiento en un ejemplo no implica su éxito en otras situaciones. En efecto, esta estrategia de sentido común puede provocar el caos. Tomemos las tablas de preferencia:

$A\ b\ a\ c$	$a\ A\ C\ B$
B arbitraria	$b\ C\ A\ B$
$C\ a\ b\ c$	c arbitraria;

"arbitrario" significa que cualquier orden que se tome no altera la situación siguiente:

$$\begin{array}{cccl} \underline{A}a & B\underline{b} & Cc & \\ A\underline{b} & Ba & \underline{C}c & \\ Ac & B\underline{a} & \underline{C}b & \\ \underline{A}c & Bb & C\underline{a} & \\ Aa & Bb & Cc & \text{situación inicial.} \end{array}$$

Luego, nuestro procedimiento nos llevó a un ciclo indefinido de casamientos y divorcios, en el cual cada cuatro períodos regresamos a los brazos de nuestra amada Dulcinea o amado Amadis.

Conclusión: el procedimiento no sirve. Lo cual no implica que el problema no tenga solución...

Seamos más astutos, tan astutos que no sólo confiamos en resolver el problema, sino que instalamos una agencia matrimonial para "ayudar" a estas parejas:

Agencia Matrimonial "La Solución".

Algoritmo:

1. En un salón están las n damas esperando los avances de eventuales novios o pololos.
2. Los varones entran al salón uno a uno y eligen, según la disponibilidad, la mejor polola según el criterio de su lista de preferencias.
3. Las elegidas aceptan el pretendiente si:

3.1. Están solteras.

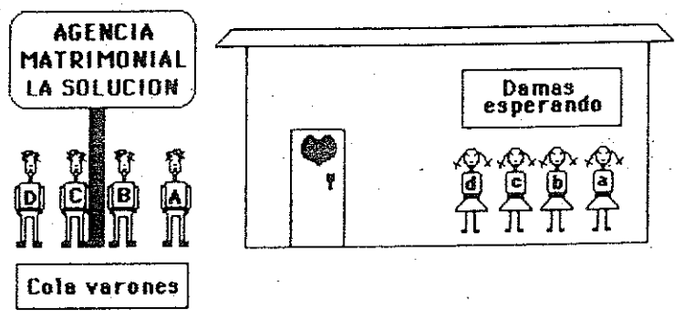
3.2. Están pololeando pero prefieren al pretendiente (según su clasificación).

3.2.1. En este caso abandonan al pololo y se emparejan con el pretendiente. El abandonado, sin salirse del salón borra a la ex-polola de su lista y aplica la estrategia del punto 2.

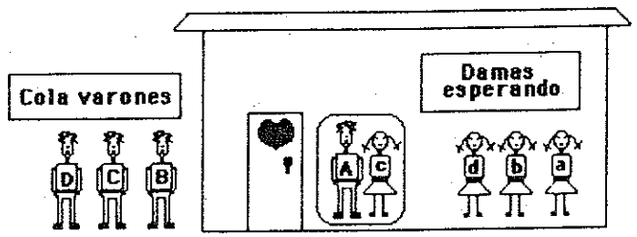
3.2.2. De no aceptarlo (la chica que está pololeando), el pretendiente la borra de su lista y aplica la estrategia del punto 2.

Realicemos un ejemplo según las tablas iniciales:

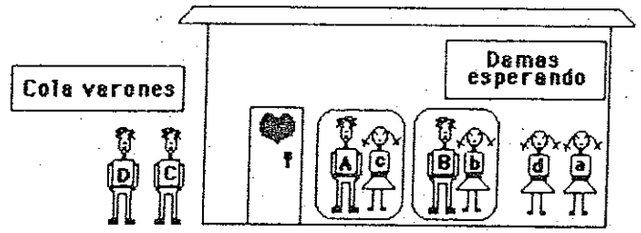
A	c	b	d	a	a	A	B	D	C
B	b	a	c	d	b	C	A	D	B
C	b	d	a	c	c	C	B	D	A
D	c	a	d	b	d	B	A	C	D



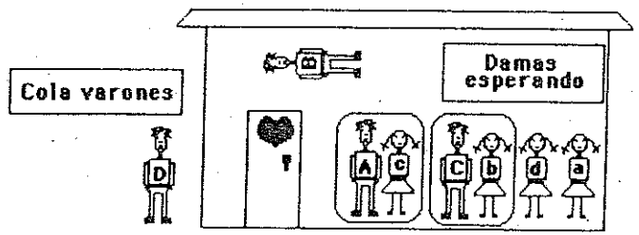
Entra A y elige la mejor de su lista:



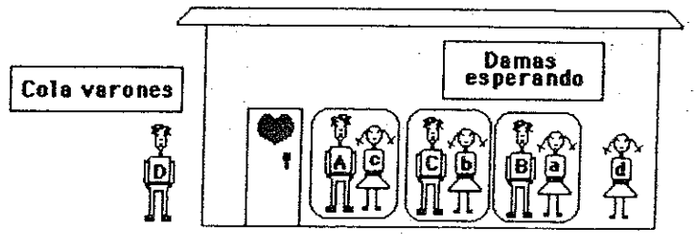
Entra B y elige la mejor de su lista:



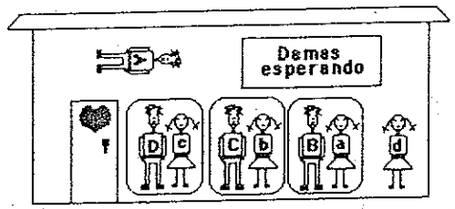
Entra C y el drama pasional estalla: C prefiere a b ... pero b está pololeando con B y ... prefiere a C. La malvada abandona a B y se pone a pololear con C:



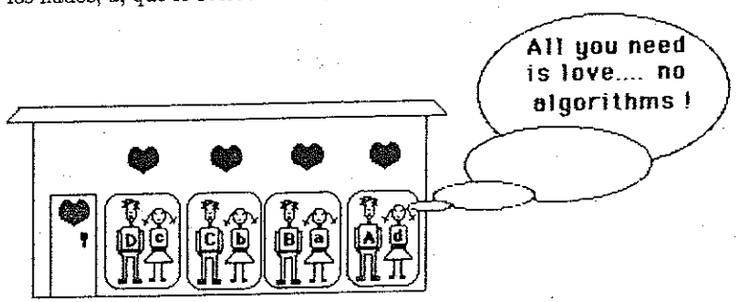
B botado y despechado, aunque práctico, realiza dos acciones: borra a la pérfida b de su lista (lista de B actualizada $\{a, c, d\}$) y busca el difícil consuelo en la mejor Dulcinea que puede abordar de acuerdo a su lista:



Ahora entra D y ... ¡otro drama! D prefiere a la chica c y ella, pololа de A, en estricto apego a sus intereses, abandona al malogrado A y se pone a pololear con D.



Pero, la vida sigue igual ... y la agencia ineluctablemente impone sus criterios: A ahoga sus penas en ... los ejercicios propuestos en el capítulo, quema el daguerrotipo de c y la borra de su lista (lista de A: $\{b, d, a\}$). Más aún, trata de conquistar a b, pero ella prefiere a su novio y lo deja. A borra b de su libreta telefónica y de su lista (le quedan sólo ($\{d, a\}$) y elige la olvidada de los hados, d, que lo recibe con los brazos abiertos.



El encargado de la agencia constata que éste es un emparejamiento estable y procede a realizar un casorio colectivo ¡¡¡ Happy End !!!

Pero aún no hemos demostrado que este procedimiento funciona siempre. Como buenos ingenieros, vale la pena tratar de asegurarnos de esto,

para evitar futuras pérdidas por eventuales demandas de los clientes de "La Solución".

Algunas observaciones inteligentes sobre nuestra estrategia son las siguentes:

1. El algoritmo es finito (termina en un número finito de pasos). En cada paso, o bien la cola de hombres disminuye en uno, o bien se acorta alguna lista de preferencias en uno.
   Como ambos objetos (cola y listas) son finitos, el algoritmo se detiene en algún momento ■

2. Dos mujeres no pueden compartir el mismo novio.
   En efecto, al entrar un varón, digamos X:
   o bien se empareja con una soltera,
   o bien levanta la polola a otro individuo, digamos Y, el cual borra su ex-polola de su lista.

3. La lista de un individuo nunca queda vacía. Si así fuera, significaría que lo han rechazado o dejado la totalidad de las damas. Es decir todas tienen novio y él está soltero. Lo cual contradice el hecho que el número de hombres y mujeres es el mismo, n.

4. La elección de una mujer nunca empeora (en cuanto a su lista). En efecto, si x pololea con X y decide dejar a X por Y es porque prefiere Y a X, ergo, mejora su elección.

5. Si al finalizar el algoritmo se tiene una pareja Xx tal que X prefiere la dama y, entonces:
   y no lo aceptó nunca,
   o bien,
   y lo abandonó en alguna oportunidad.

En efecto, si en el transcurso del algoritmo se tuvo Xy, como al final se tiene Xx, entonces entró a la agencia otro individuo al cual y prefirió, abandonando a X.

La otra situación que pudo ocurrir es que cuando X tuvo oportunidad de hacer avances a y (que pololeaba con otro individuo), ella no lo aceptó ■

De las observaciones anteriores se tiene:

El emparejamiento que entrega "La Solución" es estable. (3.43)

Demostración: Sabemos que el algoritmo se detiene (propiedad 1).

Supongamos que en el emparejamiento obtenido al finalizar el procedimiento existan parejas Xx e Yy tales que:

$$X \text{ prefiere } y \text{ a } x.$$

Del punto 5 concluímos que:

$$y \text{ lo rechazó en alguna oportunidad.}$$

Es decir, dado que la elección de y no empeora (punto 4) ésta prefiere su actual pololo Y a X,
o bien y lo abandonó en alguna oportunidad;luego, prefirió a otro pololo. De 5 se tiene que y prefiere Y a X.

De lo anterior se concluye que el "casorio" propuesto por "La solución" es estable ■

Ejercicios.

1. Dado un conjunto de n varones y n damas. ¿ Cuántas tablas de preferencia de varones pueden construirse? ¿De damas? ¿ Pares de tablas de damas y varones?
2. Determine "casorios estables" en las listas de preferencia con $n = 3$ dados en el texto.
   Verifique, en este mismo caso, que las soluciones no son únicas.
   Idea: aplique el algoritmo a dos órdenes distintos en la cola de varones que acuden a "La Solución".
3. Determine un algoritmo "feminista" para determinar un "casorio estable"
   (donde las mujeres tengan la iniciativa). Aplique ambos algoritmos a todos las posibles colas (de hombres y mujeres en el ejemplo de $n = 3$).
4. Demuestre que no existe siempre un casorio estable donde cada individuo se case con su preferencia óptima. Dé una condición suficiente para que se verifique lo anterior.
5. ¿ Qué se le ocurre en el caso en que en cada columna de las preferencias de damas y varones no se repiten letras?
   Estudie con ejemplos pequeños, aplique el algoritmo, etcétera, etcétera... y sobre todo, lo estamos esperando en "La Solución".
6. Dé una cota superior del número de pasos que requiere el algoritmo de "La Solución" para obtener un casorio estable en una población de $2n$ individuos.
7. Programe el algoritmo de "La Solución".

6. Ordenes son órdenes.

Dado un natural $n \in I\!N \setminus \{0\}$, definimos el conjunto de las *particiones ordenadas* de n:

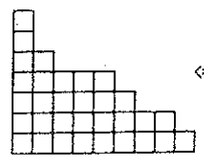
$$D_n = \{w = (w_1, ..., w_n) / \sum_{j=1}^{n} w_j = n, w_j \geq w_{j+1}, \forall j \in \{1, ..., n-1\}, w_j \in I\!N\}.$$

Por ejemplo, para $n = 6$, los elementos de D_6 son los siguientes:

$$(6,0,0,0,0,0), (5,1,0,0,0,0), (4,2,0,0,0,0), (3,3,0,0,0,0), (3,2,1,0,0,0)$$

$$(2,2,2,0,0,0), (3,1,1,1,0,0), (2,2,1,1,0,0), (2,1,1,1,1,0), (1,1,1,1,1,1).$$

Constatamos que la suma de las componentes es $n = 6$ y que su valor decrece de izquierda a derecha. Como notación gráfica utilizaremos la siguiente: asociamos un cuadrado al número 1 y por cada componente w_i, dibujaremos una pila de w_i cuadrados:



$\Longleftrightarrow$ **w= (7,5,4,4,4,3,2,2,1)**

Definamos en D_n la relación de orden, $\leq$, como sigue:

$$\forall v, w \in D_n : \qquad (w \leq v) \Longleftrightarrow (\sum_{j=i}^{n} w_j \geq \sum_{j=i}^{n} v_j)(\forall i \in \{1, ..., n\}) \qquad (3.44)$$

Verifiquemos que es relación de orden:

1. Es trivialmente *refleja*: $\forall w \in D_n, \sum_{j=i}^{n} w_j = \sum_{j=i}^{n} w_j \Leftrightarrow w \leq w$.
2. Es *antisimétrica*: supongamos $(w \leq v) \wedge (v \leq w)$.
   Es directo que:

$$\sum_{j=i}^{n} w_j = \sum_{j=i}^{n} v_j \qquad i \in \{1, ..., n\}$$

Tomando $i = n$, se obtiene $w_n = v_n$.
Tomando $i = n-1 : w_{n-1} + w_n = v_{n-1} + v_n \Rightarrow w_{n-1} = v_{n-1}$.
Por recurrencia, concluímos $v = w$.

3. Es *transitiva*: sea $(w \leq v) \wedge (v \leq u)$, entonces

$$(\forall i \in \{1, ...n\})(\sum_{j=i}^{n} w_j \geq \sum_{j=i}^{n} v_j) \wedge (\sum_{j=i}^{n} v_j \geq \sum_{j=i}^{n} u_j);$$

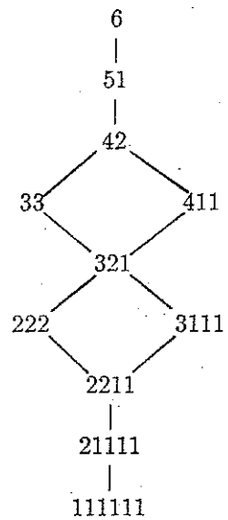
por transitividad en $\mathbb{N}$, concluímos

$$(\forall i \in \{1, .., n\})(\sum_{j=i}^{n} w_j \geq \sum u_j) \Longleftrightarrow w \leq u \quad \blacksquare$$

Diremos que, dados $v, w \in D_n, v$ es *hijo* de w (o w es *padre* de v) si y sólo si:

$$(v \leq w, v \neq w) \wedge (\nexists u \in D_n \text{ tal que } v \leq u \leq w, u \neq v, u \neq w). \qquad (3.45)$$

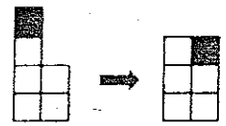
Una verificación empírica para el caso $n = 6$, arroja la siguiente distribución familiar:



donde el trazo vertical indica que el elemento del nivel inferior es "menor" que el del nivel superior (o es hijo de). Vemos acá que 42 tiene dos hijos: 33 y 411. Además, 321 no es hijo de 42 (entre él y 42 existe otra partición).

Analicemos con atención el diagrama anterior para ver cuáles son las "operaciones" para producir hijos.

$$42 \rightarrow 33$$



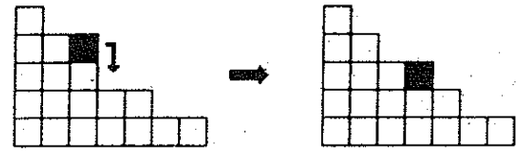
Un cuadrado, "cae" de la pila 1 a la pila 2.

$$321 \rightarrow 222$$

Un cuadrado cae de la pila 1 a la pila 3.

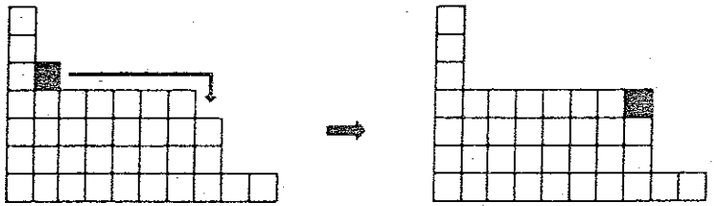
Si usted repite este análisis para todos los elementos de D_6, comprobará que son las únicas maneras de producir hijos. De esto, y con un cierto grado de "patudez" afirmamos que, cualquiera sea el $n \in \mathbb{N} \setminus \{0\}$ los hijos "nacen" de la manera siguiente:

(a)



o bien

(b)

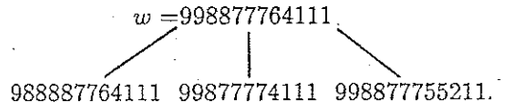


Es decir:

(a) Si dos pilas consecutivas tienen una diferencia de altura ≥ 2, se crea un hijo, enviando un cubo a la siguiente pila.

(b) Si, entre dos pilas, cuya diferencia de altura es exactamente 2, existe una "meseta" entonces el cuadrado de la pila de más a la izquierda se desliza hasta la de más a la derecha, produciendo una meseta mayor.

Ejemplo:

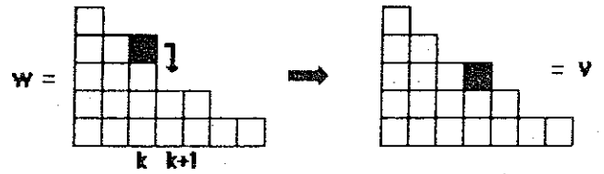


Formalmente se tiene el Teorema:

Dada una partición $w \in \mathcal{D}_n$,un hijo, $v \in D_n$,de w tiene la forma siguiente:

1. $\exists k \in \{1,...,n-1\}$, *tal que* $w_k - w_{k+1} \geq 2$ y:

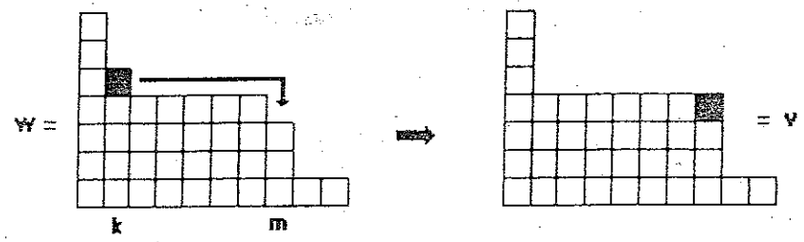
$$v_j = w_j \quad \forall j \in \{1,...,n\} \setminus \{k, k+1\}$$
$$v_k = w_k - 1, \quad v_{k+1} = w_k + 1$$



o bien,

2. $\exists k, m \in \{1,...,n-2\}, m > k+1$ *tales que*:

$$w_k = w_{k+1} + 1 = ... = w_{m-1} + 1 = w_m + 2$$



donde:

$$v_j = w_j \quad \forall j \in \{1,...,n\} \setminus \{k, m\}$$
$$v_k = w_k - 1, v_m = w_m + 1.$$

Demostración: Es suficiente probar que si se tiene una partición $u \leq w$, siempre es posible determinar otra, v, verificando (1) o (2), entre ambos (es decir $u \leq v \leq w, v \neq w$).

Sea entonces $u \leq w$, $u \neq w$, luego

$$\forall i \in \{1,...,n\} \qquad \sum_{j=i}^{n} u_j \geq \sum_{j=i}^{n} w_j. \tag{3.46}$$

De (3.46) es directo que existen componentes (al menos una) en u y w tales que la componente de u es estrictamente mayor que la de v (en caso contrario, si $\forall j, i \in \{1,...,n\}$, $u_j \leq w_j \Rightarrow \sum_{j=1}^{n} u_j \leq \sum_{j=1}^{n} w_j$ $\forall i \in = \{1,...,n\}$, lo cual es una contradicción con (1) pués $u \neq w$).

Sea $k \in \{1,...,n\}$ la primera componente, de izquierda a derecha, tal que $u_k > w_k$. Se tiene entonces

$$w = w_1 w_2 ... w_{k-2} w_{k-1} w_k ...$$
$$u = u_1 u_2 ..... u_{k-2} u_{k-1} u_k ...$$

tal que $w_j \geq u_j$ $j = 1,...,k-1$ y $u_k > w_k$.

Se tiene varios casos:

1. $w_{k-1} = w_k$, entonces: $w_{k-1} \geq u_{k-1} \geq u_k > w_k$, luego este caso es imposible.

2. $w_{k-1} - w_k \geq 2$. Se define la partición v, (entremedio de w y u) como sigue:

$$v_j = w_j \quad \forall j \in \{1,...,n\} \setminus \{k-1,k\}$$
$$v_{k-1} = w_{k-1} - 1, v_k = w_k + 1$$

Esquemáticamente:

$$\begin{array}{lccccc} w = w_1 & \cdots & w_{k-2} & w_{k-1} & w_k & \cdots \\ v = w_1 & \cdots & w_{k-2} & w_{k-1} - 1 & w_k + 1 & \cdots \\ u = u_1 & \cdots & u_{k-2} & u_{k-1} & u_k & \cdots \end{array}$$

Claramente $v \neq w$. Verifiquemos que, según el orden $\leq$, v está entre u y w. Es claro que:

$$\forall j \notin \{k-1,k\} \sum_{j=i}^{n} v_j = \sum_{j=i}^{n} w_j \leq \sum_{j=i}^{n} u_j$$

Para $j = k-1$:

$$\sum_{j=k-1}^{n} v_j = w_{k-1} - 1 + w_k + 1 + \sum_{j=k+1}^{n} v_j$$
$$= \sum_{j=k-1}^{n} w_j \leq \sum_{j=k-1}^{n} u_j$$

Para $j = k$:

$$\sum_{j=k}^{n} v_j = 1 + \sum_{j=k}^{n} w_j$$

pero

$$\sum_{j=k}^{n} w_j = w_k + \sum_{j=k+1}^{n} w_j < u_k + \sum_{j=k+1}^{n} w_j \leq u_k + \sum_{j=k+1}^{n} u_j$$

$$\Rightarrow \qquad \sum_{j=k}^{n} v_j = \sum_{j=k}^{n} w_j + 1 \leq \sum_{j=k}^{n} u_j$$

de donde concluímos que $v \leq u$ y, además, v es de la forma (1) dada en el teorema.

3. Si $w_{k-1} = w_k + 1$. En este caso

$$w_{k-2} \geq w_{k-1} = w_k + 1 \geq w_k$$
$$u_{k-2} \geq u_{k-1} \geq u_k$$

Recordando que $w_{k-1} \geq u_{k-1}, u_k > w_k$ se tiene $w_{k-1} = w_k + 1$ $\geq u_{k-1} \geq u_k > w_k$, concluyendo $u_{k-1} = u_k = w_k + 1$, obteniendo el esquema:

$$\begin{array}{lccccc} & & k-2 & k-1 & k & \\ w = w_1 \ldots & & w_{k-2} & w_k + 1 & w_k & \ldots \\ u = u_1 \ldots & & u_{k-2} & w_k + 1 & w_k + 1 & \ldots \end{array}$$

Aquí aparecen varios subcasos:

(3.1) Si $w_{k-2} - w_{k-1} = w_{k-2} - w_k - 1 \geq 2$, basta tomar $v \in D_n$ tal que

$$v_j = w_j, \ \forall j \in \{1,...,n\} \setminus \{k-2,k-1\}$$

$$v_{k-2} = w_{k-2} - 1, v_{k-1} = w_{k-1} + 1 = w_k + 2.$$

Claramente $v \neq w$ verifica la condición (1) del teorema. La prueba de que $v \geq u$, es análoga al caso anterior.

(3.2) Si $w_{k-2} - w_{k-1} = 1$, basta tomar $v \in D_n$ como sigue:

$$v_j = w_j \quad \forall j \in \{1,...,n\} \setminus \{k-2,k\}$$
$$v_{k-2} = w_{k-2} - 1, v_k = w_k + 1.$$

Esquemáticamente:

$$\begin{array}{lccccc} & & k-3 & k-2 & k-1 & k \\ w = w_1 & \ldots & w_{k-3} & w_{k-2} & w_k + 1 & w_k \ldots \\ v = w_1 & \ldots & w_{k-3} & w_{k-2} - 1 & w_k + 1 & w_k + 1 \ldots \\ u = u_1 & \ldots & u_{k-3} & u_{k-2} & w_k + 1 & w_k + 1 \ldots \end{array}$$

Es directo que $w \neq v$ y que v verifica la prioridad (2) del teorema para los índices $k-2$ y k. La prueba de que $v \geq u$ es análoga a los casos anteriores.

(3.3) Si $w_{k-2} - w_{k-1} = 0$. Recordando el esquema

$$\begin{array}{lccc} & k-2 & k-1 & k \\ w = w_1 \ldots & w_{k-2} & w_k + 1 & w_k \ldots \end{array}$$

$$\begin{array}{lccc} u = u_1 \ldots & u_{k-2} & w_k + 1 & w_k + 1 \ldots \end{array}$$

se tiene $w_{k-2} = w_{k-1} = w_k + 1 \geq u_{k-2} \geq w_k + 1$, de donde concluímos $u_{k-2} = w_k + 1$, obteniendo el nuevo esquema:

$$\begin{array}{lccccc} & & k-2 & k-1 & k & \\ w = w_1...w_{k-3} & & w_k+1 & w_k+1 & w_k & ... \\ u = u_1...u_{k-3} & & w_k+1 & w_k+1 & w_k+1 & ... \end{array}$$

Como el número de posiciones entre 1 y $k-3$ es finito y $\sum_{j=1}^{n} w_j = \sum_{j=1}^{n} u_j = n$, es fácil probar que, trasladándonos hacia la izquierda fatalmente encontraremos un índice $s \in \{1, ..., k-3\}$ tal que:

$$w_s - w_{s+1} \geq 2 \qquad \text{o bien}$$

$$w_s = w_{s+1} + 1 = ... = w_{k-1} + 1 = w_k - 1$$

En el primer caso construímos "el hijo" v según el punto (3.1). En el segundo caso:

$$\begin{array}{lccccccc} & s & s+1 & \cdots & k-1 & k & \\ w = w_1...w_{s-1} & w_k+2 & w_k+1 & \cdots & w_k+1 & w_k & ... \\ v = w_1...w_{s-1} & w_k+1 & w_k+1 & \cdots & w_k+1 & w_k+1 & ... \\ u = u_1...u_{s-1} & w_k+1 & w_k+1 & \cdots & w_k+1 & w_k+1 & ... \end{array}$$

Es decir,

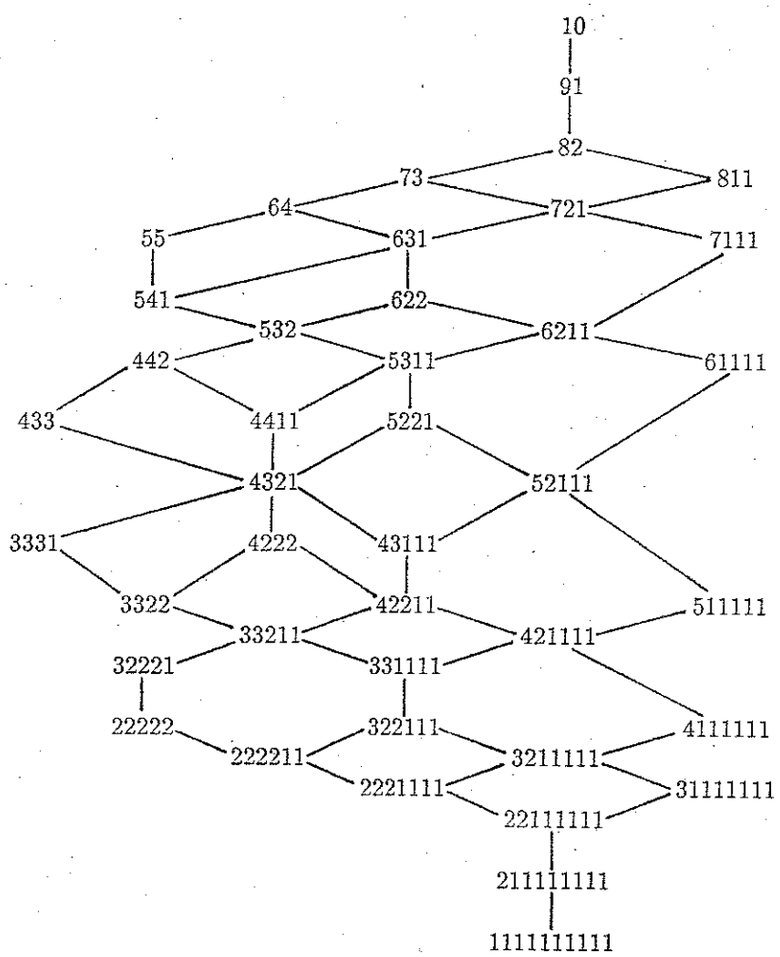
$$v_j = w_j, \forall j \in \{1, ..., n\} \setminus \{s, k\}$$

$$v_s = w_s - 1 = w_k + 1, v_k = w_k + 1.$$

Es directo que $v \neq w$ y verifica la condición (2) del teorema. Análogamente a los casos anteriores se prueba que $v \geq u$ ■

Las operaciones de enviar un cuadrado a la pila de la derecha o que éste se deslice en una meseta, las podemos interpretar como una avalancha de cubos de hielo. Por ejemplo, para $n = 10$, las diferentes maneras en que se produce el desmoronamiento de la pila de hielo se grafica en la página siguiente.

Lo que es físicamente interesante es la existencia de avalanchas que demoran más que otras y que <u>todas</u> llegan a un estado donde no se mueven más, $\bar{1} = (1, 1, ..., 1)$. ¿Puede demostrar alguna de estas afirmaciones?, ¿puede calcular exactamente el número de pasos de la avalancha más rápida (más lenta) entre $\bar{n} = (n, 0, ...)$ y $\bar{1} = (1, 1, ..., 1)$? La solución a estas preguntas y otros hechos curiosos puede consultarlos en el simpático trabajo "Games on line graphs and sand-piles" de los ilustrísimos investigadores privados M. Kiwi K. y un servidor.



CAPITULO IV

El mecanismo electoral ha sido establecido en funciòn de las municipales.
(acervo criollo)

FUNCIONES

4.1. Introducción.

Las funciones corresponden a un caso particular de relación. Dada una relación $\mathcal{R}$ definida por $R \subseteq A \times B$, diremos que $\mathcal{R}$ es una *función* si y sólo si

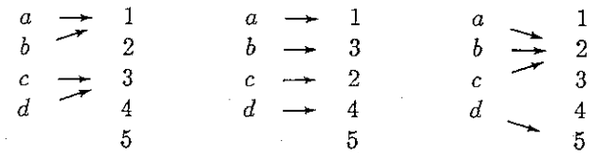
$$(\forall x \in A)(\exists! y \in B)\ (x\mathcal{R}y).$$

En tal caso notaremos esta relación por $f : A \to B$ tal que:

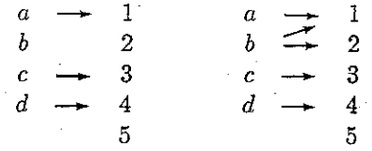
$$x\mathcal{R}y \Leftrightarrow y = f(x) \tag{4.1}$$

$$f : A \to B$$
$$x \to f(x)$$

y se denomina la imagen de x a través de f. Tomemos, por ejemplo, $A = \{a, b, c, d\}, B = \{1, 2, 3, 4, 5\}$.



son funciones.

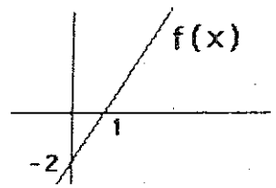


no son funciones.

Diremos que el conjunto A es el *dominio* y el conjunto B el *recorrido* de la función f.

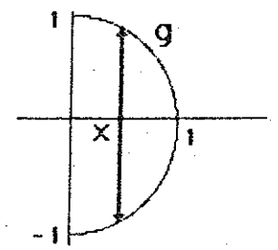
Con este lenguaje podemos decir que f es función si cualquier elemento del dominio tiene una y sólo una imagen en el recorrido. O bien de cada elemento del dominio sale una y sólo una flecha.

Al hacer el gráfico de una relación podemos verificar si es o no función, por ejemplo:



$f : \mathbb{R} \longrightarrow \mathbb{R}$
$x \longmapsto 2x - 2$

es función



no es función

f es función ya que cualquier elemento del dominio $\mathbb{R}$ tiene imagen y además ésta es única. g no es función ya que cada elemento de $[0,1]$ tiene dos imágenes.

Igualdad de funciones.

Dadas dos funciones, $f : A \to B$ y $g : C \to D$, diremos que $f = g$ si y sólo si

$$\begin{array}{c}(A = C) \wedge (B = D).\\ (\forall x \in A)(f(x) = g(x)).\end{array} \tag{4.2}$$

O bien, dos funciones son iguales si tienen idéntico dominio y recorrido y para cada elemento del dominio idénticas imágenes.

4.2 Funciones y Conjuntos.

Conjunto Imagen.

Sea una función $f : A \to B$, y sea $X \subseteq A$ definimos el *conjunto imagen* de X por f como la colección de todos los elementos del recorrido a los cuales llega una flecha con origen en un elemento de X:

$$f(X) = \{y \in B / \exists x \in X, y = f(x)\}; \tag{4.3}$$

de manera más breve:

$$f(X) = \{y \in B / y = f(x), x \in X\}.$$

También suele notarse $f(X)$ como $Im(X)$.

Por ejemplo, si f es la función:

$$\begin{array}{ccc}1 & \longrightarrow & 1\\ 2 & \longrightarrow & 2\\ 3 & \nearrow & 3\\ 4 & \longrightarrow & 4\end{array}$$

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

Obviamente, dada una función $f : A \to B$, la imagen de f verifica $f(A) \subseteq B$.

Imagen Recíproca o Pre-imagen.

Sea $Y \subseteq B$, definimos la *pre-imagen* o *imagen recíproca* de un conjunto Y como sigue:

$$\begin{array}{c}f^{-1}(Y) = \{x \in A / y = f(x), y \in Y\}\\ = \{x \in A / f(x) \in Y\}.\end{array} \tag{4.4}$$

Por ejemplo:

$$\begin{array}{ccc}1 & \nearrow & 1\\ 2 & \rightarrow & 2\\ 3 & \nearrow & 3\\ 4 & \longrightarrow & 4\end{array}$$

$$f^{-1}(\{1\}) = f^{-1}(\{3\}) = \phi$$
$$f^{-1}(\{2,4\}) = \{1,2,3,4\}.$$

4.2.1 Propiedades del conjunto imagen y pre-imagen.

Sea $f : A \to B$ una función, se tienen las propiedades siguientes:

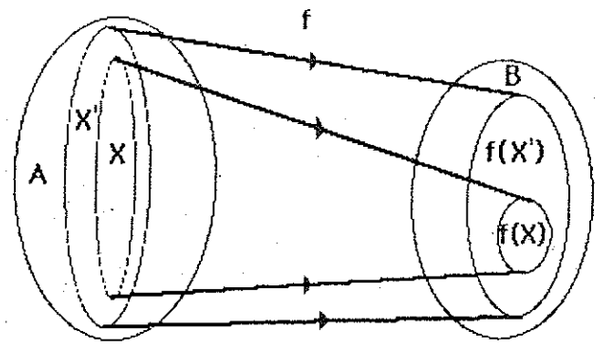
$$f^{-1}(B) = A. \tag{4.5}$$

En efecto, como f es función de cada elemento de A sale una flecha que llega a algún elemento de B. Formalmente: es claro que $f^{-1}(B) \subseteq A$. Probemos entonces que $A \subseteq f^{-1}(B)$:

Dado $x \in A$, $\exists! y \in B$ tal que $y = f(x)$; luego de la definición $x \in f^{-1}(B)$, entonces $A \subseteq f^{-1}(B)$, de donde se obtiene la igualdad ■

$$X \subseteq X' \Rightarrow f(X) \subseteq f(X'). \tag{4.6}$$

En efecto, $y \in f(X) \Leftrightarrow \exists x \in X, y = f(x)$.
Como $X \subseteq X' \Rightarrow \exists x \in X', y = f(x) \Leftrightarrow y \in f(X')$ ■



$$Y \subseteq Y' \subseteq B \Rightarrow f^{-1}(Y) \subseteq f^{-1}(Y'). \tag{4.7}$$

En efecto, $x \in f^{-1}(Y) \Leftrightarrow \exists y \in Y$ tal que $y = f(x)$. Como $Y \subseteq Y' \Rightarrow \exists y \in Y'$ tal que $y = f(x)$, de donde, por definición de pre-imagen $x \in f^{-1}(Y')$ ■

$$f(X \cup X') = f(X) \cup f(X') \tag{4.8}$$

$$f^{-1}(Y \cup Y') = f^{-1}(Y) \cup f^{-1}(Y') \tag{4.9}$$

$$f(X \cap X') \subseteq f(X) \cap f(X'). \tag{4.10}$$

Demostremos esta última propiedad. Sea $y \in f(X \cap X')$
$\Leftrightarrow (\exists x \in X \cap X')(y = f(x)) \Leftrightarrow (\exists x)\ (x \in X) \wedge (x \in X')(y = f(x))$ (ojo: se trata del mismo elemento x).
$\Rightarrow (\exists x \in X, y = f(x)) \wedge (\exists x \in X', y = f(x))$
$\Leftrightarrow (y \in f(X)) \wedge (y \in f(X')) \Leftrightarrow y \in f(X) \cap f(X')$.
¿Por qué la penúltima sentencia en la demostración es sólo una implicación y no una equivalencia?

La respuesta es que podríamos tener un elemento "y" común a ambos conjuntos, $f(X)$ y $f(X')$, proveniente en ambos casos de elementos distintos de los conjuntos X y X'. Sea, por ejemplo, $X = \{3,4\}$, $X' = \{1,2,3\}$ y la función:

$$\begin{array}{ccc} 1 & \rightarrow & 1 \\ 4 & \nearrow & 3 \\ 3 & \rightarrow & 2 \\ 2 & \rightarrow & 4 \end{array}$$

El 1 pertenece a ambas imágenes, $f(X)$, y $f(X')$, pero proviene de elementos distintos; se tiene

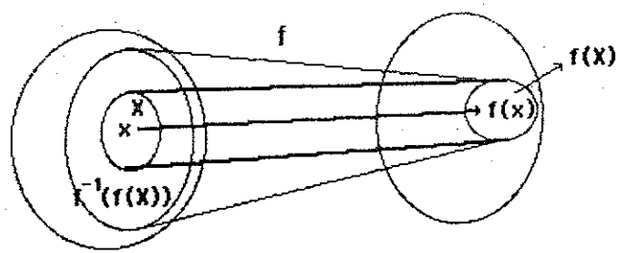
$$f(X) = \{1,2\}, \qquad f(X') = \{1,2,4\}$$
$$f(X \cap X') = \{2\}, \qquad f(X) \cap f(X') = \{1,2\}.$$

De lo anterior concluímos (a través de un contraejemplo) que no siempre se cumple $f(X \cap X') = f(X) \cap (X')$ ■

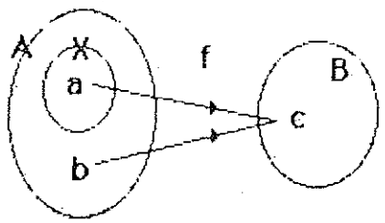
$$f^{-1}(Y \cap Y') = f^{-1}(Y) \cap f^{-1}(Y') \tag{4.11}$$

$$f^{-1}(f(X)) \supseteq X. \tag{4.12}$$

Lo que hacemos en (4.12) es tomar la imagen de un conjunto X (es decir determinamos $f(X)$ en B), luego, para ese conjunto, tomamos su pre-imagen y, sorpresa, no recuperamos necesariamente el conjunto inicial, sino uno que lo contiene. Analicemos esto: Sea $x \in X$, sea $y = f(x)$ su imagen por f. Luego $y \in f(X)$. Al tomar la imagen recíproca de $f(X)$, es decir $f^{-1}(f(X))$, como $y \in f(X)$, con $y = f(x)$ concluímos, por definición de imagen recíproca, $x \in f^{-1}(f(X))$ ■



Pero ¿por qué no hay igualdad? La respuesta es simple: podría existir un elemento, digamos $c \in B$ y al menos dos elementos $a, b \in A$ tales que $a \in X$ y $b \notin X$, tales que $f(a) = f(b) = c$:



Como $c \in f(X)$, al tomar la pre-imagen de $f(X)$ tendremos que ésta contiene al menos $X \cup \{b\} \supseteq X$. Sea, por ejemplo, $X = \{1, 2\}$ y la función f que figura a continuación. Se tiene $f(X) = \{2, 3\}$, $f^{-1}(f(X)) = \{1, 2, 3\}$.

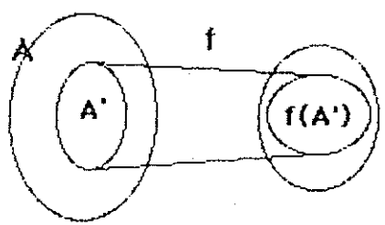
$$\begin{array}{ccc} 1 & & 1 \\ 2 & & 2 \\ 3 & \longrightarrow & 3 \\ 4 & \longrightarrow & 4 \end{array}$$

$$f(f^{-1}(Y)) \subseteq Y. \tag{4.13}$$

4.2.2 Restricción y extensión de funciones.

Sea $f : A \to B$ y sea $A' \subseteq A$, definimos la *restricción* de la función f al conjunto A' como

$$f|_{A'} : A' \to B;\ x \to f|_{A'}(x) = f(x)$$



se eliminan del dominio todos los elementos que no están en A' y todas las flechas que partían de $A \setminus A'$. Por ejemplo si $A = B = \{1, 2, 3, 4\}$, con $A' = \{2, 3\}$ se tiene:

$$\begin{array}{ccc} f & & \\ 1 & \longrightarrow & 1 \\ 2 & \longrightarrow & 2 \\ 3 & \longrightarrow & 4 \\ 4 & \longrightarrow & 3 \end{array} \qquad \begin{array}{ccc} f|_{A'} & & \\ & & 1 \\ 2 & \longrightarrow & 2 \\ 3 & \longrightarrow & 4 \\ & & 3. \end{array}$$

Sea ahora $A' \supseteq A$. Definimos una *extensión* de f al conjunto A' como una función g tal que coincida con f sobre el dominio A:

$$\begin{array}{l} g : A' \to B \\ \quad x \to g(x) \end{array}$$

tal que $\forall x \in A, g(x) = f(x)$.

Como el valor de $g(x)$ es arbitrario en $A' \setminus A$ pueden existir muchas extensiones. Por ejemplo:

$$\begin{array}{l} f : I\!P \to I\!N \\ \quad x \to x + 1 \end{array} \qquad \text{donde } I\!P \text{ es el conjunto de los números pares}$$

Una extensión sería

$$\begin{array}{l} g : I\!N \to I\!N \\ \quad x \to g(x), \end{array} \qquad g(x) = \begin{cases} x + 1 & \text{si } x \in I\!P \\ 0 & \text{si } x \notin I\!P. \end{cases}$$

Otra extensión sería $g(x) = x + 1$.

En este último caso, a cada número par le asociamos un impar y a cada impar un número par.

4.3. Clasificación y zoología funcionaria: epiyecciones, inyecciones, biyecciones.

Veremos aquí algunos tipos particulares de funciones que poseen interesantes propiedades algebraicas.

Dada una función $f : A \to B$, diremos que:

- Es *epiyectiva* si y sólo si $f(A) = B$ o bien:

$$(\forall y \in B)(\exists x \in A)(f(x) = y), \tag{4.14}$$

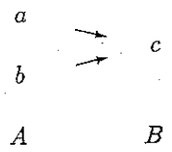
o bien "Todo elemento del recorrido admite al menos una pre-imagen". En términos de una ecuación, f es epiyectiva si y sólo si:

"$\forall b \in B$, la ecuación $f(x) = b$ admite solución en A".

- Es *inyectiva* si y sólo si:

$$(\forall y \in f(A))(\exists! x \in A)(f(x) = y). \tag{4.15}$$

En otras palabras, está prohibida la situación siguiente:



De manera equivalente, f es inyectiva si y sólo si

$$(\forall x_1, x_2 \in A)(f(x_1) = f(x_2) \Rightarrow x_1 = x_2). \tag{4.16}$$

Veamos que esta última sentencia es equivalente a la anterior:

(4.15)$\Rightarrow$ (4.16). Si se tuviese $f(x_1) = f(x_2) = c$ y además $x_1 \neq x_2$, se tendría que: $\exists c \in f(A)$, con al menos dos pre-imágenes, lo cual contradice la definición (4.15).
En el otro sentido, si aceptamos (4.16), se tiene una y sólo una pre-imagen $(\forall y \in f(A))(\exists! x \in A)(y = f(x))$ ■

En términos de una ecuación, la inyectividad se enuncia como sigue:

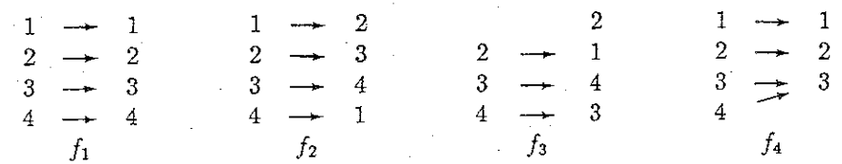
$\forall b \in f(A), f(x) = b$ tiene solución única en A.

- Diremos que f es *biyectiva* si y sólo si es epiyectiva e inyectiva:

$$(\forall y \in B)(\exists! x \in A)(f(x) = y) \tag{4.17}$$

o en términos de ecuación: $(\forall b \in B)(f(x) = b)$ tiene solución única en A.

Ejemplos.



Las funciones 1,2 son biyecciones. La función 3 es solamente inyección y la función 4 es solamente epiyección.

La función, $f : \mathbb{N} \to \mathbb{N}$, $n \to 2n$ es inyectiva, en efecto:

$$f(n) = f(m) \Leftrightarrow 2n = 2m \Leftrightarrow n = m,$$

pero no es epiyectiva: $\forall m = 2p + 1$, $p \geq 0$, no tiene pre-imagen.

Sin embargo, si tomamos $f : \mathbb{N} \to \mathbb{P}$, $n \to 2n$, obtenemos una biyección.

Sea ahora $f : \mathbb{Z} \to \mathbb{N}$,

$$f(n) = \begin{cases} 2n - 1 & \text{si } n > 0 \\ 0 & \text{si } n = 0 \\ -2n & \text{si } n < 0. \end{cases}$$

Es decir:

$$\begin{array}{rccccccccccc} \mathbb{Z}: & 0 & 1 & -1 & 2 & -2 & 3 & -3 & 4 & -4 & \ldots \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ \mathbb{N}: & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & \ldots \end{array}$$

Por inspección visual (no es una demostración) podemos "ver" que esta función f es biyectiva. Demostremos esto correctamente:

1) f es epiyectiva: Sea $m \in \mathbb{N}$.
si $m = 0$, se tiene la pre-imagen 0,
si $m = 2p$ (es decir es par) $m = f(-p)$,
si $m = 2p - 1, p \geq 1, m = f(p)$,
luego es epiyectiva.

2) f es inyectiva: Supongamos: $f(m_1) = f(m_2)$. Luego, ambos valores son nulos, negativos o positivos. Si ambos son nulos, es directo que $m_1 = m_2$.
Si m_1 y m_2 son enteros negativos se tiene $-2m_1 = -2m_2 \Rightarrow m_1 = m_2$.
Si ambos son positivos, tenemos $2m_1 - 1 = 2m_2 - 1 \Rightarrow m_1 = m_2$ ■

Es muy interesante notar que $\mathbb{N} \subseteq \mathbb{Z}$ y que hay una correspondencia uno a uno entre sus elementos. Esto desafía nuestra intuición, pues si tenemos un saco de peras y otro de manzanas estos tendrán igual número de frutos si y sólo si podemos hacer una correspondencia biunívoca entre sus elementos. El problema radica en que, tanto $\mathbb{N}$ como $\mathbb{Z}$ son conjuntos infinitos y allí hay que desconfiar de nuestra intuición. Analizaremos este tipo de problemas en el tema "Cantor, cardinalidad y otros resbaladeros".

En este mismo contexto, analicemos más en detalle lo que sucede en el caso de conjuntos finitos (A y B con cardinalidad finita).

4.4. Funciones sobre conjuntos finitos.

Sea $f : A \to B, |A| = m, |B| = n$. Si $m < n$ la función no puede ser epiyectiva, ya que necesitaríamos más flechas de las que permite la definición: una y sólo una de cada elemento de A.

$$\begin{array}{ccc} A & & B \\ X & \longrightarrow & X \\ X & \longrightarrow & X \\ X & \longrightarrow & X \\ X & \longrightarrow & X \\ & & X \quad \textit{falta una flecha} \end{array}$$

Si $m > n$, la función no puede ser inyectiva. Esto es muy trivial pero útil para asociar elementos. En combinatoria se conoce como el *principio del palomar*:

$$\begin{array}{l} \textit{Si se tienen } n \textit{ nidos y } m > n \textit{ palomas, entonces} \\ \textit{al menos dos palomas ocupan el mismo nido.} \end{array} \tag{4.18}$$

Por ejemplo, si tomamos un conjunto de 13 personas, al menos dos están de cumpleaños el mismo mes.

De las consideraciones anteriores se tiene que, cuando $|A| < \infty, |B| < \infty$,
$f : A \to B$ es biyectiva $\Rightarrow |A| = |B|$.
Además, si $|A| = |B| = n$; f epiyectiva $\Leftrightarrow$ f inyectiva.

En efecto, como f es epiyectiva, cada elemento de B recibe una flecha. Si no fuese inyectiva entonces algún elemento de B recibe dos flechas. Como $|A| = |B| = n$ y de cada punto de A sale una y sólo una flecha, existe algún elemento de B al cual no llega flecha (¡estamos aplicando el principio del palomar!), lo cual es una contradicción, ya que f es epiyectiva ■

La noción de biyección sirve para "contar" elementos en conjuntos finitos: podemos decir que dos conjuntos tienen igual número de objetos sin saber contar, basta asociarlos uno a uno. Consideremos el ejemplo siguiente:

Sea $I = \{1, ..., n\}$ y $B = \{a_1, ..., a_n\}$ tal que $a_i \neq a_j \quad \forall i \neq j$ y sea

$$\begin{array}{c} f : I \to A \\ i \to a_i. \end{array}$$

Claramente, f es biyectiva: es trivialmente epiyectiva. Veamos si es inyectiva: $f(i) = f(j) \Leftrightarrow a_i = a_j \Rightarrow i = j$ luego, es inyectiva, de donde concluímos $|A| = |I| = n$ ■

Consideremos la función:

$$\begin{array}{c} f : \mathcal{P}(I) \to \{0,1\}^n \\ \{i_1, i_2, ..., i_p\} \to x = (x_1, ..., x_n) \end{array}$$

donde $x_k = 1 \Leftrightarrow k \in \{i_1, i_2, ..., i_p\}$.

Por ejemplo, si $I = \{1, 2, 3\}$, la función f es la siguiente:

$\phi \to (0,0,0)$, $\{1\} \to (1,0,0), \{2\} \to (0,1,0), 3 \to (0,0,1)$,
$\{1,2\} \to (1,1,0), \{1,3\} \to (1,0,1)$, $\{2,3\} \to (0,1,1), \{1,2,3\} \to (1,1,1)$.

Volvamos al caso general. El resultado interesante es que f es una biyección.

En efecto: f es epiyectiva. Dado $x \in \{0,1\}^n, x = (x_1, ..., x_n)$ le asociamos el subconjunto de I:

$$X = \{i \in I / x_i = 1\}.$$

Claramente, $f(X) = x \in \{0,1\}^n$.

f es inyectiva: $x = f(\{i_1, ..., i_p\}) = f(\{j_1, ..., j_q\}) = y \Leftrightarrow x_i = y_i$, $\forall i = 1, ..., n$, de donde $p = q$, $i_i = j_i$, $\forall i = 1, ..., p$. Concluímos entonces que f es una biyección ■

Dado que f es biyectiva, obtenemos

$$|\mathcal{P}(I)| = |\{0,1\}^n| = 2^n = 2^{|I|}.$$

Por otra parte, vimos que un conjunto finito arbitrario, A, puede ser puesto en biyección con el conjunto finito, I, que tiene igual número de

elementos. De donde concluímos que, dado un conjunto finito arbitrario A : $|\mathcal{P}(A)| = 2^{|A|}$, o bien

el número de subconjuntos de un conjunto finito A es $2^{|A|}$. (4.19)

4.5. Funciones e identidades combinatoriales.

4.5.1 Número de funciones entre dos conjuntos finitos.

Supongamos que los conjuntos A y B son finitos. ¿Cuál es el número de funciones posibles del conjunto A en B? Tomemos por ejemplo $A = \{a, b\}$, $B = \{\alpha, \beta, \gamma, \delta\}$. Es posible elegir la imagen de a de 4 maneras y la de b de 4 maneras. Es decir, el número de funciones distintas es 16. En el caso general podemos razonar como sigue:

Asumiendo que $|A| = m, |B| = n$. Sea $\mathcal{F}(A, B)$ el conjunto de todas las funciones de A en B. Para calcular su cardinalidad (número de elementos), basta establecer una biyección entre $\mathcal{F}(A, B)$ y algún conjunto cuyo cardinal sea conocido. En este espíritu definamos:

$$\varphi : \mathcal{F}(A, B) \to B^m$$
$$f \to \varphi(f)$$

tal que, si $f(a_1) = b_{i_1}, ..., f(a_m) = b_{i_m}$, entonces

$$\varphi(f) = (b_{i_1}, ..., b_{i_m}) \in B^m.$$

Por ejemplo, si $m = 3$, $n = 4$:

$$f(a_1) = b_3 \ f(a_2) = b_3, \ f(a_3) = b_1 \implies \varphi(f) = (b_3, b_3, b_1)$$

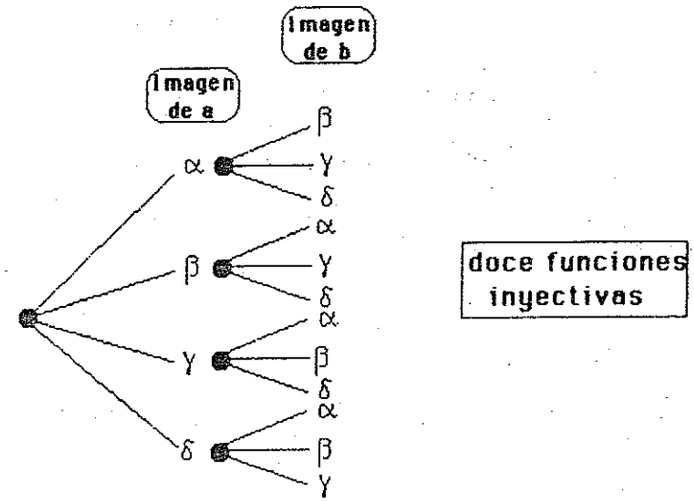
$$f(a_1) = b_2, \ f(a_2) = b_4, \ f(a_3) = b_3 \implies \varphi(f) = (b_2, b_4, b_3).$$

Es fácil verificar que φ es biyectiva, luego el número de funciones de A en B:

$$|\mathcal{F}(A, B)| = |B^m| = n^m \quad \blacksquare$$

4.5.2 Número de funciones inyectivas.

Hemos visto que para tener una inyección entre conjuntos finitos se requiere $|A| \leq |B|, (m \leq n)$. Para el caso particular $A = \{a, b\}$, $B = \{\alpha, \beta, \gamma, \delta\}$:



Constatamos que el número de inyecciones corresponde al número de pares ordenados con componentes distintas. En general para $|A| = m$, y $|B| = n$:

- la primera componente se elige de n maneras.
- la segunda de $n - 1$ ($\neq$ de la primera) maneras.

  ⋮ ⋮
- La m-ésima de $n - m + 1$ maneras.

Luego el número de funciones inyectivas es:

$$n \cdot (n-1) \cdot (n-2)...(n-m+1) = \frac{n!}{(n-m)!}$$

En el caso particular $|A| = |B| = n$, sabemos que una inyección es biyección, luego el número de funciones biyectivas es $n!$

4.5.3 Número de inyecciones con distinta imagen.

Veamos ahora el número de inyecciones con conjunto imagen distinto. Por ejemplo, las funciones $f : \{a, b\} \to \{1, 2, 3\}$ tal que $f(a) = 1, f(b) = 2$ y $f' : \{a, b\} \to \{1, 2, 3\}$ tal que $f'(a) = 2, f'(b) = 1$ son distintas pero de igual imagen: $f(\{a, b\}), = f'(\{a, b\})$. Veamos otro caso particular:

Sea $A = \{1, 2, 3\}, B = \{1, 2, 3, 4\}$. Las inyecciones que tienen imagen $\{1, 2, 3\}$ son las seis siguientes:

$$\begin{array}{ccccccccc} 1 & \to & 1 & 1 & \to & 1 & 1 & \to & 2 \\ 2 & \to & 2 & 2 & \to & 3 & 2 & \to & 1 \\ 3 & \to & 3 & 3 & \to & 2 & 3 & \to & 3 \\ & & 4 & & & 4 & & & 4 \\ 1 & \to & 2 & 1 & \to & 3 & 1 & \to & 3 \\ 2 & \to & 3 & 2 & \to & 1 & 2 & \to & 2 \\ 3 & \to & 1 & 3 & \to & 2 & 3 & \to & 1 \\ & & 4 & & & 4 & & & 4 \end{array}$$

número que coincide con todas las maneras de ordenar los elementos $1, 2, 3$ en el conjunto B.

Así, dada $f : A \to B$, existen $m!$ funciones inyectivas que tienen la misma imagen.

Luego:

Número total de Inyecciones $= m! \times$ (número de clases de inyecciones con $\neq$ imagen)

$$(\text{número de clases de inyecciones con } \neq \text{ imagen}) = \frac{n!}{(n-m)!m!} = C_n^m,$$

con lo cual interpretamos los coeficientes binomiales en términos de funciones.

4.6. Función inversa.

Otra noción importante es la de *función inversa*: Dada una función biyectiva $f : A \to B$ se tiene que:

$$(\forall y \in B)(\exists! x \in A)(y = f(x)).$$

Luego, podemos invertir el sentido de las flechas sin perder la propiedad característica de una función: de cada elemento parte una y sólo una flecha. Esta nueva función la denominaremos función inversa de f, y notaremos f^{-1}:

$$\begin{array}{ccc} A & f & B \\ a & \longrightarrow & 3 \\ b & \longrightarrow & 2 \\ c & \longrightarrow & 1 \\ d & \longrightarrow & 4 \end{array} \qquad \begin{array}{ccc} B & f^{-1} & A \\ 1 & \longrightarrow & c \\ 2 & \longrightarrow & b \\ 3 & \longrightarrow & a \\ 4 & \longrightarrow & d \end{array}$$

En términos formales:

$$f^{-1} : B \to A$$
$$y \to f^{-1}(y),$$

donde

$$f^{-1}(y) = x \Leftrightarrow f(x) = y. \tag{4.20}$$

Obviamente f^{-1} también es biyectiva y además es única. De la unicidad se concluye que $(f^{-1})^{-1} = f$ (verifique).

4.7. Composición de funciones.

Dadas las funciones f, g:

$$\begin{array}{ccccc} & & f & & g \\ A & \to & B & \to & C \\ a & \longrightarrow & 1 & \longrightarrow & \alpha \\ b & \longrightarrow & 3 & \longrightarrow & \gamma \\ d & \longrightarrow & 5 & \nearrow & \\ c & \longrightarrow & 2 & \longrightarrow & \beta \\ & & 4 & \longrightarrow & \delta. \end{array}$$

Podemos definir una tercera función, h, partiendo de cada elemento de A y siguiendo las flechas hasta llegar al conjunto C:

$$\begin{array}{ccc} & h & \\ a & \longrightarrow & \alpha \\ b & \longrightarrow & \gamma \\ d & \nearrow & \beta \\ c & & \delta. \end{array}$$

Anotemos $h = g \circ f : A \to C$, que denominaremos la *composición de* f y g. Es importante el hecho que la "primera" función f tiene como conjunto de "llegada" al dominio B, de la "segunda" función g. El conjunto B juega el papel de "puente" entre A y C.

Formalmente: dadas las funciones $f : A \to B$, $g : B \to C$ definimos la función "g *compuesta* con f" como:

$$\begin{aligned} g \circ f : & A \to C \\ & x \to g \circ f(x) = g(f(x)). \end{aligned} \tag{4.21}$$

Claramente, $g \circ f$ es función.

En efecto, si un elemento tiene dos imágenes:
$(g \circ f(x) = a) \ \wedge \ (g \circ f(x) = b) \Leftrightarrow (g(f(x)) = a) \ \wedge \ (g(f(x)) = b)$.
Notando $y = f(x)$ se tiene $(g(y) = a) \ \wedge \ (g(y) = b)$. Como g es función concluímos que $a = b$ ■

No siempre se tiene que $g \circ f$ y $f \circ g$ son iguales, más aún, en ocasiones es imposible definirlas. Por ejemplo:

$$\begin{aligned} f : & \mathbb{R} \to \mathbb{R} \\ & x \to 2x + 1 \end{aligned} \qquad \begin{aligned} g : & \mathbb{R} \to \mathbb{R} \\ & z \to z^2, \end{aligned}$$

luego,

$$\begin{aligned} g \circ f : & \mathbb{R} \to \mathbb{R} \\ & x \to (2x + 1)^2 \end{aligned} \qquad \begin{aligned} f \circ g : & \mathbb{R} \to \mathbb{R} \\ & x \to 2x^2 + 1. \end{aligned}$$

Obviamente $g \circ f \neq f \circ g$.

Sean las funciones:

$$\begin{aligned} f : & \mathbb{N} \to \mathbb{P} \\ & n \to 2n \end{aligned} \qquad \begin{aligned} g : & \mathbb{P} \to \mathbb{Z} \\ & k \to -k, \end{aligned}$$

es posible definir

$$\begin{aligned} g \circ f : & \mathbb{N} \to \mathbb{Z} \\ & n \to -2n. \end{aligned}$$

Pero no es posible definir $f \circ g$, pues $g(n) \in \mathbb{Z} \neq \mathbb{N}$, el dominio de f ■

Una función biyectiva importante, en relación a la composición de funciones, es la *identidad*. Dado un conjunto A definimos:

$$\begin{aligned} id_A : & A \to A \\ & x \to id_A(x) = x, \end{aligned} \tag{4.22}$$

correspondiente a la función cuya acción deja invariantes los elementos de A.

Si tomamos $f : A \to B$ y la composición $f \circ id_A : A \to B$ se tiene:

$$f \circ id_A = f.$$

Basta verificar que $(\forall x \in A)((f \circ id_A)(x) = f(x))$. En efecto:

$$(f \circ id_A)(x) = f(id_A(x)) = f(x) \quad ■$$

La función identidad juega, con respecto a la composición, el rol del "1" con respecto a la multiplicación en $\mathbb{R}$.

También, si tomamos $id_B : B \to B$ y la composición $id_B \circ f$ se obtiene el mismo resultado: $id_B \circ f = f$.

Recordemos que una función f es *invertible* si y sólo si es biyectiva. Veamos qué sucede con la composición de

$$A \xrightarrow{f} B \xrightarrow{f^{-1}} A \qquad f^{-1} \circ f = ?$$

$$B \xrightarrow{f^{-1}} A \xrightarrow{f} B \qquad f \circ f^{-1} = ?$$

Sea $f^{-1}(y) = x$, es decir $f(x) = y$ luego:
$f \circ f^{-1}(y) = f(f^{-1}(y)) = f(x) = y = id_B(y)$.
$f^{-1} \circ f(x) = f^{-1}(f(x)) = x = id_A(x)$. De donde concluímos:

$$(f \circ f^{-1} = id_B) \ \wedge \ (f^{-1} \circ f = id_A). \tag{4.23}$$

Además, dadas dos funciones biyectivas $f : A \to A, g : A \to A$

$$f \circ g = g \circ f = id_A \Leftrightarrow g = f^{-1}. \tag{4.24}$$

En efecto, $\Leftarrow$) si $g = f^{-1}$ es directo de lo anterior.
$\Rightarrow$) Debemos demostrar que $g = f^{-1}$. Esto es equivalente a probar que:

$$g(y) = x \Leftrightarrow f(x) = y.$$

Como f es inyectiva:

$$\begin{aligned} & g(y) = x \Leftrightarrow f(g(y)) = f(x) \\ \Leftrightarrow \quad & f \circ g(y) = f(x), \end{aligned}$$

pero $f \circ g = id_A$, luego

$$\Leftrightarrow id_A(y) = f(x) \Leftrightarrow y = f(x) \quad ■$$

Otras propiedades de la composición son las siguientes: dadas dos funciones $f : A \to B$ y $g : B \to C$

$$f, g \text{ inyectivas } \Rightarrow g \circ f \text{ inyectiva.} \tag{4.25}$$

$$f, g \text{ epiyectivas } \Rightarrow g \circ f \text{ epiyectiva.} \tag{4.26}$$

Verifiquemos (4.25):

Supongamos $g \circ f(x_1) = g \circ f(x_2) \Leftrightarrow g(f(x_1)) = g(f(x_2))$. Como g es inyectiva $\Leftrightarrow f(x_1) = f(x_2)$ y como f es inyectiva $\Leftrightarrow x_1 = x_2$ ■

¿Qué sucede si $g \circ f$ es inyectiva, con las funciones f, g? (Desarrolle).

La demostración de la propiedad (4.26) es simple:

$$f, g \text{ epiyectivas } \Leftrightarrow (f(A) = B) \wedge (g(B) = C).$$

Luego,

$$g \circ f(A) = g(f(A)) = g(B) = C;$$

luego, $g \circ f$ es epiyectiva ■

¿Qué sucede si $g \circ f$ es epiyectiva con las funciones f, g? (Desarrolle).

Otra propiedad importante es la *asociatividad* de la composición. Es decir, dadas $f : A \to B, g : B \to C, h : C \to D$ se tiene:

$$h \circ (g \circ f) = (h \circ g) \circ f. \tag{4.27}$$

En efecto:

$$(ho(gof))(x) = h((gof)(x)) = h(g(f(x))) = (hog)(f(x)) = ((hog)of)(x)$$ ■

Consideremos ahora dos funciones, $f : A \to B$ y $g : B \to C$, ambas invertibles (biyecciones):

$$f : A \to B, \qquad g : B \to C$$
$$f^{-1} : B \to A, \qquad g^{-1} : C \to B.$$

Se tiene la propiedad:

$$g \circ f \text{ es invertible. Además } (g \circ f)^{-1} = f^{-1} \circ g^{-1}. \tag{4.28}$$

La invertibilidad de $g \circ f$ es directa pues la composición de biyecciones es una biyección. Veamos la expresión de la inversa:

$$f^{-1} \circ g^{-1} : C \to A, \qquad g \circ f : A \to C.$$

Se tiene

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ g^{-1} = id_C.$$

Como la inversa es única, concluímos $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ ■

4.8. Permutaciones.

Vamos a estudiar una clase particular de funciones con dominio finito, donde la "composición" es muy útil. Sea el conjunto $A = \{1, ..., n\}$, denominaremos S_n el conjunto de todas las biyecciones sobre A:

$$S_n = \{f : A \to A / f \text{ es biyección }\}. \tag{4.29}$$

Sabemos que $|S_n| = n!$

Diremos que una función $f \in S_n$ es una *permutación*.

Pasemos revista a las notaciones más usuales para una permutación. Para ello consideremos el conjunto $A = \{1, 2, 3\}$, S_3 contiene las funciones:

$$f_1 = id: \quad 1 \longrightarrow 1,\ 2 \longrightarrow 2,\ 3 \longrightarrow 3$$
$$f_2: \quad 1 \longrightarrow 1,\ 2 \longrightarrow 3,\ 3 \longrightarrow 2$$
$$f_3: \quad 1 \longrightarrow 2,\ 2 \longrightarrow 1,\ 3 \longrightarrow 3$$
$$f_4: \quad 1 \longrightarrow 2,\ 2 \longrightarrow 3,\ 3 \longrightarrow 1$$
$$f_5: \quad 1 \longrightarrow 3,\ 2 \longrightarrow 1,\ 3 \longrightarrow 2$$
$$f_6: \quad 1 \longrightarrow 3,\ 2 \longrightarrow 2,\ 3 \longrightarrow 1.$$

Estas se notan como sigue:

$$f_1 = (123), f_2 = (132), f_3 = (213), f_4 = (231), f_5 = (312), f_6 = (321),$$

o bien,

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

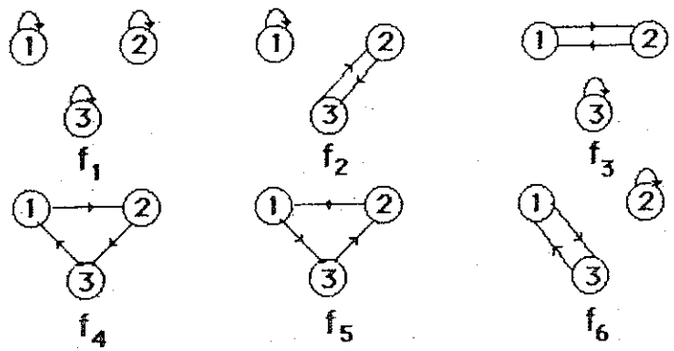
Conviene señalar que la alteración del orden de las columnas no varía la permutación, por ejemplo:

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 3 & 2 & 1 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

En el caso general, si f es una permutación sobre el conjunto $\{1, ..., n\}$, notaremos:

$$f = \begin{pmatrix} 1 & 2 & \dots & i & \dots & n \\ f(1) & f(2) & & f(i) & & f(n) \end{pmatrix}.$$

También es posible notar una permutación mediante un grafo:



Compongamos permutaciones:

$$f_2 \circ f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = f_5$$

$$f_4 \circ f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = f_2.$$

Podemos construir así la tabla de todas las composiciones posibles:

$\circ$	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_5	f_6	f_3	f_4
f_3	f_3	f_4	f_1	f_2	f_6	f_5
f_4	f_4	f_3	f_6	f_5	f_1	f_2
f_5	f_5	f_6	f_2	f_1	f_4	f_3
f_6	f_6	f_5	f_4	f_3	f_2	f_1

Esta tabla se denomina *tabla de Pitágoras* asociada a la operación $\circ$. Ella es sumamente útil para ver algunas propiedades de la composición de permutaciones. Veamos el caso particular S_3:

- Existe una identidad f_1:
- Cada elemento posee un inverso:

$$f_i^{-1} = f_i \qquad i = 1, 2, 3, 6$$

$$f_4^{-1} = f_5 \wedge f_5^{-1} = f_4.$$

- La tabla no es simétrica con respecto a la diagonal principal: $f_3 \circ f_2 \neq f_2 \circ f_3$.
- En cada fila (o columna) cada elemento aparece una y sólo una vez ■

4.8.1 Propiedades generales de las permutaciones en S_n.

- La permutación $id = \binom{12\dots n}{12\dots n}$ es la identidad en S_n, es decir,

$$\forall f \in S_n : f \circ \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix} \circ f = f. \qquad (4.30)$$

- La composición, es asociativa en S_n. (4.31)

La demostración es directa del caso general (propiedad (4.27)) por la asociatividad de la composición ■

- Dada la permutación

$$f = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$$

f admite un elemento inverso que es:

$$\begin{pmatrix} f(1) & f(2) & \dots & f(n) \\ 1 & 2 & \dots & n \end{pmatrix}. \tag{4.32}$$

En efecto:

$$\begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & & f(n) \end{pmatrix} \circ \begin{pmatrix} f(1) & f(2) & \dots & f(n) \\ 1 & 2 & \dots & n \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix} = id \quad \blacksquare$$

Se desprende de las propiedades anteriores que la *operación* $\circ$ dota al conjunto S_n de una *estructura*: los elementos del conjunto están "rígidamente" relacionados entre sí mediante esta operación.

Ejercicios.

1. Señale si las relaciones siguientes son o no funciones:
   (a) En $\mathbb{Q} \times \mathbb{Z}$, $(\frac{a}{b})R(a-b)$.
   (b) En $(\mathbb{N} \setminus \{0\}) \times \mathbb{R}$, $nR(\frac{1}{n})$.
   (c) En $\mathbb{R}^2$, $x\mathcal{R}y \iff xy^2 = 1$.
   (d) En $\mathcal{P}^2(E)$, $A\mathcal{R}C_E A$.
   (e) En $A = \{1,2,3,4\}$, $\mathcal{R}$ tal que

$$M(\mathcal{R}) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

2. Demuestre que $\mathcal{R}$, una relación definida en A^2 ($A = \{1,\dots,n\}$) es función si y sólo si, para $M(R) = (m_{ij})$, se tiene

$$\sum_{j=1}^{n} m_{ij} = 1 \quad \forall i = 1,\dots,n$$

   (donde $\sum$ indica la suma usual en $\mathbb{R}$, no en $\{0,1\}$).
3. Sea $f : \mathbb{R} \to \mathbb{R}$, $x \to x^2 + 2x + 1$, Determine:
   (a) $f(\mathbb{R}_+)$.
   (b) $f(\{1,-1\})$.
   (c) $f([-a,a])$, $a > 0$.
   (d) $f^{-1}(\{4,12,8\})$.
   (e) $f^{-1}([-a,a])$, $a > 0$.
4. Sea $f : A \to B$ una función. Considere en A la relación $a\mathcal{R}b \iff f(a) = f(b)$.
   (a) Pruebe que $\mathcal{R}$ es relación de equivalencia.
   (b) Para $A = \{1,2,\dots,n\}$ y

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

   encuentre $A/\mathcal{R}$ (El conjunto cuociente de A según $\mathcal{R}$).
5. Sea $f : \mathbb{R} \to \mathbb{R}$ tal que $\forall x,y \in \mathbb{R} \quad f(x+y) = f(x) + f(y)$.
   (a) Demuestre que

$$f(\sum_{i=1}^{n} x_i) = \sum_{i=1}^{n} f(x_i), \quad \begin{matrix} x_i \in \mathbb{R} \\ i = 1,\dots,n \end{matrix}$$

(Use Inducción).

(b) Demuestre que $f(0) = 0$ y deduzca que $f(x) = -f(x) \quad \forall x \in \mathbb{R}$.

(c) Demuestre que $f(n) = nf(1)\ \forall n \in \mathbb{N}$.

(d) Demuestre que $f(z) = zf(1)\ \forall z \in \mathbb{N}$. (Considere $z = n - m$, $n, m \in \mathbb{N}$).

6. Sea $f : X \to Y$, $g : Y \to Z$. Sea $A \subseteq X$, pruebe que: $(g \circ f)|_A = g \circ (f|_A)$.
7. Sea U un conjunto no vacío y $A, B \subseteq U$. Sea $f : \mathcal{P}(U) \to \mathcal{P}(U)$, $f(X) = A \cap (B \cup X)$, pruebe que $f^2 = f$.
8. Si el dominio de g es $A = \{0, ..., n\}$, encuentre un dominio de f en los casos siguientes, de manera de que $g \circ f$ está bien definida.
   (a) $f(x) = x(mod 2)$.
   (b) $f(x) = \begin{cases} x+3 & \text{si } x \text{ es par} \\ x & \text{si } x \text{ es impar.} \end{cases}$
   (c) $f(x) = 5x - 1$.
   (d) $f(x) = x \cdot (n - x)$.
9. Sea $f : A \to A$ (A no vacío) una función. Definimos $f^n : A \to A$ por medio de la recurrencia $f^\circ = f, f^{n+1} = f^n \circ f$. Pruebe que:
   (a) f es biyectiva $\Rightarrow f^n$ es biyectiva.
   (b) f es biyectiva $\Rightarrow (f^n)^{-1} = (f^{-1})^n$.
10. Sea $f : \mathbb{N} \to \mathbb{N}$ tal que:

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

    (a) Determine si f es inyectiva, epiyectiva, biyectiva.
    (b) Determine $f^2 = f \circ f$.
11. Sea $f : A \to B$, $g : C \to D$. Defina $h : A \times C \to B \times D$ tal que $h(a, c) = (f(a), g(c))$. Pruebe que h es biyectiva si y sólo si f y g son biyectivas.
12. Sean $f : A \to B$ y $A' \subseteq A$. Sea $f|_{A'}$ la restricción de f a A'.
    (a) Pruebe que si f es inyectiva, entonces $f|_A$ es inyectiva.
    (b) Dé un ejemplo en que $f|_{A'}$ sea inyectiva y no así f.
13. Para cada par de números reales a y b, se define $f_{ab} : \mathbb{R} \to \mathbb{R}$, $f_{ab}(x) = ax + b$.
    (a) Muestre que $f_{1b} \cdot f_{a0} = f_{ab}$.
    (b) Para $a \neq 0$ pruebe que f_{ab} es biyectiva.
    (c) Para $a \neq 0$ calcule f_{ab}^{-1}.

* 14. Sea $f : X \to Y$, pruebe que f es inyectiva si y sólo si $f(A \cap B) = f(A) \cap f(B),\ \forall A, B \subseteq X$.

* 15. Sea $f : X \to Y$ una función, X, Y no vacíos. Pruebe que:
    (a) $f(f^{-1}(B)) = B \quad \forall B \subseteq X$ si y sólo si f es epiyectiva.
    (b) Si f es inyectiva, $f(A \setminus C) = f(A) \setminus f(C), \forall A, C \subseteq X$.

(c) $C_y(f(A)) \subseteq f(C_x(A)) \forall A \subseteq X$ si f es epiyectiva.

(d) Si f es epiyectiva, entonces $C_y(f(A)) = f(C_x(A))$ si y sólo si f es también inyectiva.

* 16. Sea una relación $\mathcal{R}$ asociada a $R \subseteq A \times B$. Sea, además,

$$\tilde{\mathcal{R}} : \begin{array}{l} A \to \mathcal{P}(B) \\ x \to \mathcal{R}(\{x\}) \quad \text{con } \mathcal{R}(\{x\}) = \{y \in B / (x, y) \in \mathcal{R}\}. \end{array}$$

Demuestre que la función $H : \mathcal{P}(A \times B) \to \mathcal{F}(A, \mathcal{P}(B)), R \to \tilde{R}$, es inyectiva.

* 17. Sea $A = \{0, 1, ..., n-1\}$. Diremos que $f : A \to A$ es cíclica si y sólo si $f(0) \in A, f(i+1) = (f(i) + 1) \bmod(n), 0 \leq i < n - 1$.
    (a) Pruebe que f cíclica $\Rightarrow f$ biyectiva.
    (b) Determine el número de funciones cíclicas.

18. Dado un triángulo equilátero de lado 1, demuestre que, dados cinco puntos arbitrarios en el interior del triángulo, existen al menos dos a distancia $\leq \frac{1}{2}$ (aplique el principio del palomar).
19. Sea A un conjunto de 5 números naturales no nulos, tales que el máximo entre ellos es a lo más 9. Pruebe que entre las sumas de los elementos de los subconjuntos no vacíos de A, existen al menos dos sumas iguales (aplique el principio del palomar).
20. Si en un pueblo no hay dos habitantes con igual número de dientes ¿Cuál podría ser el número máximo de habitantes del pueblo? (El que posee más dientes, tiene 32) (aplique el principio del palomar).
21. Demuestre que existen dos personas en el mundo con el mismo número de cabellos. (Observación: estime la cantidad de cabellos de una persona y de habitantes del planeta) (aplique el principio del palomar).

* 22. Dado el conjunto $\mathcal{F} = \{f_1, f_2, ..., f_6\}$ de funciones en $A = \mathbb{R} \setminus \{0, 1\}$, definidas como

$$f_1 = \begin{array}{l} A \to A \\ x \to x \end{array} \qquad f_2 : \begin{array}{l} A \to A \\ x \to \frac{1}{x} \end{array} \qquad f_3 : \begin{array}{l} A \to A \\ x \to 1 - x \end{array}$$

$$f_4 = \begin{array}{l} A \to A \\ x \to \frac{1}{1-x} \end{array} \qquad f_5 : \begin{array}{l} A \to A \\ x \to \frac{x-1}{x} \end{array} \qquad f_6 : \begin{array}{l} A \to A \\ x \to \frac{x}{x-1}. \end{array}$$

Construya la tabla de Pitágoras para la composición de funciones en $\mathcal{F}$.

* 23. Sea $f \in S_n$ (el conjunto de las permutaciones de $A = \{1, ..., n\}$), llamamos; inversión a un par $i, j \in A, i < j$ que verifica $f(i) > f(j)$.

¿Cuántas inversiones es posible encontrar al recorrer todos los elementos de S_n?

* 24. Sea $f \in S_{20}$ que verifica:
(1) $\exists i, j \in \{1, ..., 10\}$ tal que:
$f(i) = 1, f(j) = 2$.
(2) $\exists k, \ell \in \{11, ..., 12\}$ tal que:
$f(k) = 3, f(\ell) = 4$ ¿Cuántas funciones como f existen en S_{20}?

* 25. ¿Cuántas permutaciones hay en S_n en las cuales dos imágenes i y j (fijos) no están "juntas"? Es decir

$$(\exists k \in \{1, ..., n\})([(f(k)=i) \wedge (f(k+1)=j)] \vee [(f(k)=i) \wedge (f(k-1)=j)])$$

* 26. (a) ¿Cuántas permutaciones de S_n verifican $f(i+1) = f(i) + 1$ $\forall i \in \{1, ..., n\}$?
(b) ¿Cuántas hay en S_n que verifican $f(i+1) \neq f(i)+1 \quad \forall i \in \{1, ..., n\}$?
(Observación: (b) no es el complemento de (a)).

* 27. Dado $p \geq 2, p \in \mathbb{N}$ fijo, y dado $a \in \mathbb{N}$ sabemos que existen elementos $u_p, v_p \in \mathbb{N}$, únicos, tales que: $a = u_p \cdot p + v_p, 0 \leq v_p < p$ (algoritmo de la división). Se define $f_p : \mathbb{N} \to \mathbb{N}, a \to f_p(a) = u_p$.
(a) Probar que, dados $a = u_p \cdot p + v_p, b = u'_p \cdot p + v'_p$, descomposiciones de a y b, se tiene:

$$f_p(a+b) = f_p(a) + f_p(b) \iff v_p + v'_p < p.$$

(b) ¿Es f_p inyectiva?, ¿es f_p epiyectiva?
(c) Probar que, dados $p < p' \in \mathbb{N} \Rightarrow f_{p'}(a) \leq f_p(a), \forall u \in \mathbb{N}$.

28. Si para toda función $f : X \to X$, existe $A \in \mathcal{P}(X) \setminus \{X, \phi\}$ tal que $f(A) \subseteq A$, pruebe que X no puede ser finito.

* 29. Sea $\mathbb{Z}_p$ el conjunto cociente de las congruencias módulo p. Estudie para $p = 2, 3, 4, 5$, la función $f_r : \mathbb{Z}_p \to \mathbb{Z}_p, [x] \mapsto f_r([x]) = [r] \cdot [x]$, donde $1 \leq r < p$.
Demuestre que: $\forall 1 \leq r < p, f_r$ es biyectiva si y sólo si p es primo.

* 30. (a) Sea $f_r : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p \times \mathbb{Z}_p, ([x], [y]) \to ([x] \cdot [r], [y] + [r])$, donde $[x] \cdot [r] = [x \cdot r]$ y $[y] + [r] = [y + r]$. Pruebe que f_r es biyectiva $\forall 1 \leq r \leq p$ si y sólo si p es primo.
(Indicación: use los resultados de Ejercicios 11 y 29).
(b) Sea $g : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p([x], [y]) \to \max\{[x], [y]\}$, donde

$$\max\{[x], [y]\} = [\max\{\hat{x}, \hat{y}\}] \text{ con } \hat{x} \in [x], \hat{y} \in [y], 0 \leq \hat{x}, \hat{y} < p.$$

Encuentre $A \subset \mathbb{Z}_p \times \mathbb{Z}_p$ tal que $g \circ f_r|_A$ es biyectiva $(1 \leq r \leq p)$.
(Indicación: Analice el caso $[x] = [0] \in \mathbb{Z}_p$ o bien $[y] = [p - r] \in \mathbb{Z}_p$).

TEMAS CAPITULO IV

1. Cantor, cardinalidad y otros resbaladeros.

2. Sobre parentela, casorios y tribus.

1. Cantor, cardinalidad y otros resbaladeros.

Recordemos acá el apócrifo cuento del pastor Cardenio (El Ingenioso Hidalgo, episodio del príncipe Etíope) que no sabía contar y para no perder su rebaño de ovejas, cada vez que partía con ellas al monte realizaba la operación siguiente:

Por cada oveja que salía del corral, dejaba un piedra en un canasto. Al regresar, por cada oveja que entraba al corral sacaba una piedra del canasto.

Obviamente lo que hacía Cardenio era una biyección entre dos conjuntos: el de ovejas y el de piedras. Esta idea simple se le ocurrió a Cantor (matemático del siglo pasado) para "contar" elementos y comparar conjuntos de acuerdo a si es posible o no establecer una biyección entre ellos. Lo interesante de esta idea es que ella es aplicable tanto a conjuntos finitos como infinitos ya que es posible establecer biyecciones entre algunos conjuntos infinitos. Esto permitió a Cantor comparar conjuntos infinitos entre sí y de alguna manera atacar el problema de la existencia de infinitos "más grandes que otros".

Formalicemos lo anterior. Dados dos conjuntos A, B (no necesariamente finitos) diremos que tienen igual *cardinalidad* si existe una función biyectiva $f : A \to B$. En tal caso notamos $A \equiv B$.

Obviamente si A y B son finitos y existe una biyección entre ellos, tenemos que su cardinal (que definimos en (1.37)) es el mismo, es decir, tienen el mismo número de elementos.

En el caso infinito el asunto es más resbaloso. Por ejemplo, existe una biyección entre $\mathbb{N}$ y su subconjunto propio, $\mathbb{P}$, de los números pares:

$$\begin{aligned} f : \mathbb{N} &\to \mathbb{P} \\ n &\to 2n \end{aligned}$$

$$\begin{array}{cccccc} 0 & 1 & 2 & \ldots & n & \ldots \\ \downarrow & \downarrow & \downarrow & \ldots & \downarrow & \ldots \\ 0 & 2 & 4 & \ldots & 2n & \ldots \end{array}$$

luego $\mathbb{N} \equiv \mathbb{P}$. Es decir comparten el mismo tipo de infinito aunque $\mathbb{P}$ está estrictamente contenido en $\mathbb{N}$.

La relación entre conjuntos $\equiv$, *tener igual cardinal* es de equivalencia. En efecto:

Es refleja: $\forall A, A \equiv A$. Basta tomar $id : A \rightarrowtail A$.

Es simétrica: Si $A \equiv B, \exists f : A \to B$ biyección, luego existe la inversa que también es biyectiva, $f^{-1} : B \to A$ de donde $B \equiv A$.

Es transitiva: Si $(A \equiv B) \wedge (B \equiv C), \exists f : A \to B, g : B \rightarrowtail C$ biyectivas, luego $g \circ f : A \rightarrowtail C$ es biyectiva, de donde $A \equiv C$ ■

Esta equivalencia, $\equiv$, permite clasificar todos los conjuntos en clases, según exista o no una biyección entre ellos. Por ejemplo, una clase sería todos los conjuntos finitos con 10.000 elementos. Otra, que representamos por $[\mathbb{N}]$ contiene $\mathbb{P}$, los impares, etcétera.

La clase $[\mathbb{N}]$ es importante ya que la infinitud de $\mathbb{N}$ es la más fácil de "entender".

En tal sentido, diremos que un conjunto X es *enumerable* si y sólo si X es finito o bien $X \equiv \mathbb{N}$.

Notaremos el cardinal de $\mathbb{N}$ como $|\mathbb{N}| = \mathcal{X}_o$ (aleph-cero).

Como ejemplos, tenemos que $\mathbb{P}$ y $\mathbb{Z}$ son enumerables. Otros conjuntos enumerables no triviales se construyen aplicando la propiedad siguiente:

Dada una familia de conjuntos $\{A_i\}_{i\in\mathbb{N}}$ tal que cada A_i es enumerable,

$$\textit{entonces } \bigcup_{i\in\mathbb{N}} A_i \textit{ también es enumerable.} \qquad (4.33)$$

La demostración es simple. Hagamos una lista de los elementos de estos conjuntos (los cuales podemos enumerar, ya que cada uno de ellos está en biyección con $\mathbb{N}$):

$$\begin{array}{lcl} A_0 & = & \{\ a_{00} \quad a_{01} \quad a_{02} \quad a_{03} \quad \ldots \\ A_1 & = & \{\ a_{10} \quad a_{11} \quad a_{12} \quad a_{13} \quad \ldots \\ A_2 & = & \{\ a_{20} \quad a_{21} \quad a_{22} \quad a_{23} \quad \ldots \\ \vdots & & \vdots \quad \vdots \quad \vdots \quad \vdots \end{array}$$

además, podemos suponer, sin pérdida de generalidad, que $A_i \cap A_j = \phi$ para $i \neq j$ (¿¿por qué??). Asociamos la siguientes biyección, φ, entre $\bigcup_{i\in\mathbb{N}} A_i$ y $\mathbb{N}$.

$a_{00} \to 0$ (suma de índices es 0)
$a_{01} \to 1,\ a_{10} \to 2$ (suma de índices es 1)
$a_{02} \to 3,\ a_{11} \to 4,\ a_{20} \to 5$ (suma de índices es 2)
$a_{03} \to 6,\ a_{12} \to 7,\ a_{21} \to 8,\ a_{30} \to 9$ (suma de índices es 3).

Un corolario de esta propiedad es que el conjunto de los racionales, Q, es enumerable.

En efecto, $Q = \bigcup_{q\in\mathbb{N}_+} Q_q$, donde:

$$Q_1 = \{\ldots, \frac{-3}{1}, \frac{-2}{1}, \frac{-1}{1}, \frac{0}{1}, \frac{1}{1}, \frac{2}{1}, \frac{3}{1}, \ldots\}$$
$$Q_2 = \{\ldots, \frac{-3}{2}, \frac{-2}{2}, \frac{-1}{2}, \frac{0}{2}, \frac{1}{2}, \frac{2}{2}, \frac{3}{2}, \ldots\}$$
$$\vdots$$
$$Q_q = \{\ldots, \frac{-3}{q}, \frac{-2}{q}, \frac{-1}{q}, \frac{0}{q}, \frac{1}{q}, \frac{2}{q}, \frac{3}{q}, \ldots\}.$$

Claramente $\forall q \in \mathbb{N}_+, Q_q$ es enumerable.

$$\begin{array}{rccccccccc} \mathbb{N}: & 0 & 1 & 2 & 3 & 4 & 5 & 6\ldots \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ Q_q: & \frac{0}{q} & \frac{1}{q} & \frac{-1}{q} & \frac{2}{q} & \frac{-2}{q} & \frac{3}{q} & \frac{-3}{q} \ldots \end{array}$$

Se tiene entonces la biyección $\Psi : \mathbb{N} \to Q_q, n \to \Psi(n)$:

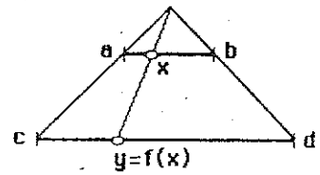
$$\Psi(n) = \begin{cases} \frac{k}{q} & \text{si } n = 2k-1, \quad k \in \mathbb{N}_+ \\ \frac{-k}{q} & \text{si } n = 2k, \quad k \in \mathbb{N}. \end{cases}$$

Como la unión de conjuntos enumerables es enumerable, concluímos que Q es enumerable ■

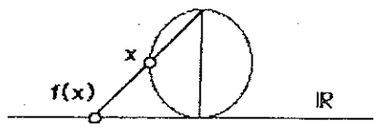
Tenemos entonces que $|\mathbb{N}| = |Q| = \mathcal{X}_o$ y $Q \in [\mathbb{N}]$.

Se deduce también de (4.33) que $\bigcup_{n\geq 1} \{0,1\}^n$ es enumerable (¡Justifique!).

Estudiemos conjuntos infinitos más complejos. Por ejemplo, dados $a < b,\ c < d \in \mathbb{R}$ los intervalos son equivalentes: $[a,b] \equiv [c,d]$.



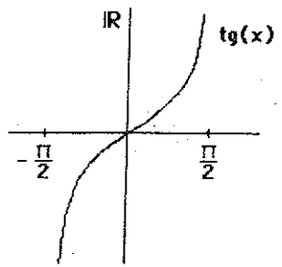
Los puntos sobre una circunferencia de radio $r > 0$ son equivalentes a la recta $\mathbb{R}$:



En particular, no es difícil demostrar que $\mathbb{R}$ está en biyección con el intervalo abierto $]-\frac{\pi}{2},\frac{\pi}{2}[=\{x\in\mathbb{R}|\frac{-\pi}{2}<x<\frac{\pi}{2}\}$. En efecto:

$$\begin{aligned} tg:\ ]-\frac{\pi}{2},\frac{\pi}{2}[&\to \mathbb{R} \\ x &\to tg(x) \end{aligned}$$

es biyectiva (verifique).



También es fácil ver que los intervalos abiertos están todos en la misma clase de equivalencia (tienen igual cardinal):

En efecto, $\forall a,b\in\mathbb{R}, a<b$, la aplicación

$$\begin{aligned} \varphi:]0,1[&\to]a,b[\\ x &\to a+(b-a)x \end{aligned}$$

es biyectiva (verifique).

Luego $(]0,1[\equiv\ ]-\frac{\pi}{2},\frac{\pi}{2}[\ )\wedge\ (]-\frac{\pi}{2},\frac{\pi}{2}[\equiv\ \mathbb{R})$. Como $\equiv$ es transitiva:

$$]0,1[\ \equiv\ \mathbb{R}.$$

Hemos probado entonces que $\mathbb{R}$ y el intervalo abierto $]0,1[$ tienen el mismo cardinal, que denotaremos c, denominado cardinal del *continuo*:

$$|\ ]0,1[\ |\ =|\mathbb{R}|=c.$$

El gran resultado de Cantor fue el Teorema que lleva su nombre:

Teorema de Cantor.

$$\mathbb{R}\ \textit{no es enumerable}\ (c\neq\chi_0). \tag{4.34}$$

Demostración:

Basta demostrar esto para el intervalo $]0,1[$ ya que éste es equivalente a $\mathbb{R}$. El método de demostración se denomina *proceso de diagonalización de Cantor*.

Supongamos que $]0,1[$ sea enumerable, luego $\exists f:\mathbb{N}\to]0,1[$ biyectiva. Es decir, $]0,1[=\{f(0),f(1),f(2).,...\}$. Claramente $\forall n\in\mathbb{N}, f(n)$ es un número entre 0 y 1.

$$\begin{aligned} f(0) &= 0.\mathbf{a_{00}}a_{01}a_{02}a_{03}....a_{0n}... \\ f(1) &= 0.a_{10}\mathbf{a_{11}}a_{12}a_{13}.....a_{1n}... \\ f(2) &= 0.a_{20}a_{21}\mathbf{a_{22}}a_{23}.....a_{2n}... \\ &\vdots\quad\ \vdots\qquad\qquad\vdots \\ f(n) &= 0.a_{n0}a_{n1}a_{n2}a_{n3}.....\mathbf{a_{nn}}... \\ &\vdots\quad\ \vdots \end{aligned}$$

construyamos $\epsilon\in]0,1[$ de la manera siguiente:

$$\epsilon = 0.\epsilon_0\epsilon_1\epsilon_2\epsilon_3...\epsilon_n....$$

tal que $\forall n \in \mathbb{N}\ \epsilon_n \neq a_{nn}$.

Por ejemplo:

$$\epsilon_n = \begin{cases} 1 & \text{si } a_{nn} \neq 1 \\ 0 & \text{si } a_{nn} = 1. \end{cases}$$

Es trivial, entonces, que:

$$\epsilon \neq f(n) \quad \forall n \in \mathbb{N},$$

luego, ϵ no tiene pre-imagen por f, que es supuestamente biyectiva, concluyendo que $]0,1[$ no es enumerable.

Como $\mathbb{R}$ está en la clase de $]0,1[$, hemos demostrado que $\mathbb{R}$ no es enumerable ■

Hemos detectado entonces dos tipos de infinitud: la fácil o enumerable, asociada a los números naturales, y un infinito más complejo asociado al conjunto de los reales. La pregunta es: ¿ hay otras clases entremedio?. Si tiene una respuesta contáctese inmediatamente con el autor (¡no le cuente a nadie en el camino!).

Para terminar, daremos otro resultado, también conocido como Teorema de Cantor. Probaremos que *un conjunto X y el conjunto de sus partes, $\mathcal{P}(X)$, no tienen igual cardinal.* Este resultado es trivial cuando X es finito, ya que $|X| = n$ y $|\mathcal{P}(X)| = 2^n$. Veamos lo que sucede en el caso infinito:

Supongamos que existe una biyección entre ambos conjuntos:

$$\varphi : X \to \mathcal{P}(X).$$

Sea $C = \{x \in X | x \notin \varphi(x)\}$ Como $C \subseteq X \Rightarrow C \in \mathcal{P}(X)$. Como φ es epiyectiva, existe $c \in X$, tal que $\varphi(c) = C$.

Ergo,

$$c \in C \Rightarrow c \notin \varphi(c) = C$$
$$c \notin C \Rightarrow c \in \varphi(c) = C.$$

Luego la biyección φ no existe ■

Este resultado tiene algún parecido con la Paradoja de Rusell (ver Tema 2, capítulo I). Más aún, podemos concluir de él que U, el "conjunto de todos los conjuntos", ¡no existe! De existir se tendría que $\varphi : U \to \mathcal{P}(U)$, donde

$\varphi(u) = u$ es una biyección. En efecto, dado $u \in \mathcal{P}(U) \Rightarrow u \subseteq U \Rightarrow$ (como U es el conjunto de todos los conjuntos) $u \in U$, luego φ es epiyectiva. Además, $\varphi(x) = \varphi(y) \Rightarrow x = y$. De donde se tiene la contradicción pues sabemos, del resultado anterior, que tal biyección no existe.

Este último resultado es de gran sanidad ya que, de existir el conjunto, U, de todos los conjuntos, existe en particular el conjunto de la Paradoja de Russell $\{x \in U / x \notin x\}$ que, como vimos en el Tema 2, del capítulo I, conduce a una contradicción ■

Ejercicios.

1. (a) Dé una fórmula explícita de $\varphi(a_{ij})$ para, $\varphi : \bigcup_{i \in \mathbb{N}} A_i \to \mathbb{N}$, en función de los índices (i,j).
   (b) Pueden existir conjuntos finitos en la familia $\{A_i\}_{i \in \mathbb{N}}$.
2. (a) Pruebe que, si $\{A_i\}_{i=1}^n$ es una familia finita de conjuntos enumerables, entonces $\times_{i=1}^n A_i$ es enumerable.
   (b) Sea A tal que $|A| = p < \infty$. Pruebe que $U = \bigcup_{n \in \mathbb{N}} A^n$ es enumerable, donde $A^n = \times_{i=1}^n A$.
3. Todo conjunto infinito incluye un conjunto enumerable.
4. Diremos que $|A| \leq |B|$ si el conjunto A tiene igual cardinal que algún subconjunto de B. Además, si $|A| \neq |B|$ y $|A| \leq |B|$ se anota $|A| < |B|$.
   (a) Deduzca que $\chi_0 < c$.
   (b) Pruebe que $|A| \leq 2^{|A|}$. (Use el Teorema de Cantor)
5. Pruebe que $F = \{A \subseteq \mathbb{N} / A \text{ es finito }\}$ es enumerable.
6. Todo subconjunto de un conjunto enumerable es enumerable.
7. Asuma que si p es primo, entonces $\sqrt{p} \in I$ (es un número irracional). Recuerde, además, que $\mathbb{R} = Q \cup I$. Pruebe: $|Q| < |I|$. (Indicación: puede servirle también el Ejercicio 5).

2. Sobre parentela, casorios y tribus.

En plena Amazonía, en la confluencia de los ríos Napo y Tapajóz, habita la tribu Tupinamba, la cual hasta hace apenas sesenta años, practicaba el canibalismo (cf. "Aventuras de Hans Staden, Monteiro Lobato, 1951 y colección de La Decouverte, París 1985). El Dr. Charleston, antropólogo titular de la Universidad de Oxford, nos ha dejado, luego de su muerte (en circunstancias más bien picantes y condimentadas), este texto que describe el análisis estructuralista "chez les Tupinambas" (dado que el francés es la lengua por excelencia del estructuralismo), que es, sin duda alguna, una de las cumbres pedagógicas para todo estructuralista iniciático. Dejemos entonces la palabra al malogrado Charleston:

"Durante mi larga convivencia con los Tupinambas, aparte de idear sinnúmero de actos mágicos para evitar la amenazante olla, comencé a modelar los aspectos principales de las relaciones de parentesco y por ende matrimonios y tabúes incestuosos del pueblo de los dientos puntudos, como suelen referirse a sí mismos. Para cumplir este cometido fue vital la formación matemática y muy particularmente algebraica que recibí del ilustre profesor Golesdric durante mis estudios universitarios (sic)...."

Pero vamos al grano.

La sociedad Tupinamba está dividida en Clases o Clanes Matrimoniales. La población se reparte en un número finito de clases matrimoniales disjuntas dos a dos. Las reglas de parentesco y matrimonio se formulan en términos de estas clases.

Una clase matrimonial tiene la propiedad de *Exogamia*: si un miembro de la clase X debe buscar esposa al exterior de la clase X.

Cualquier violación de esta regla es castigada severamente y los culpables son sacrificados y pasan directamente a la olla de la clase X.

Pero la exogamia es insuficiente para explicar la ya compleja sociedad Tupinamba pues no define a qué clase (o clases) debe dirigirse un miembro de X para contraer matrimonio, ni tampoco lo que sucede una vez casados: ¿dónde se quedan?, ¿en la clase de la esposa o del esposo?, ¿forman otra clase? ¿en qué clan viven los hijos?, etc., etc.

Para aclarar un poco nuestras inquietudes introduciremos alguna notación:

Sea $C = \{X_1, ..., X_n\}$ el conjunto de clases matrimoniales o clanes de la tribu Tupinamba (conviene señalar que durante su estadía Charleston contabilizó 4 clanes, con aproximadamente 250 miembros cada uno). Definimos también la función conyugal como la biyección:

$$f : C \to C,$$

donde $f(X)$ es la clase en la cual un individuo de X debe buscar esposa. La exogamia se traduce entonces:

$$f(X) \neq X \qquad \forall X \in C.$$

Observemos que en este modelo la clase donde un individuo puede buscar esposa es única.

Introduzcamos ahora una biyección $p : C \to C$ tal que, si un varón $x \in X$ entonces sus hijos deben estar en la clase $p(X)$.

p se denomina la función de *filiación paternal.*

De manera análoga, sea la biyección $m : C \to C$ tal que, si una mujer $x \in X$ entonces sus hijos deben estar en la clase $m(X)$.

m se denomina función de *filiación maternal.*

Para que esto tenga sentido, como los hijos de una pareja deben estar en una sola clase:

$$p(X) = m(f(X)).$$

Es decir, los hijos de un varón del clan X deben estar en la clase asociada por la filiación maternal (clase $m \circ f(X)$).

Con esto estamos en condiciones de definir una estructura elemental de parentesco.

Denominamos estructura elemental de parentesco en C al conjunto de las tres biyecciones (f, m, p) que verifican los axiomas:

$$\begin{array}{ll} (F) & p = m \circ f. \\ (EXO) & f(X) \neq X \qquad \forall X \in C. \end{array} \tag{4.35}$$

Las funciones f, m, p se denominan conyugal, maternal y paternal respectivamente.

Este simple modelo coincide con las observaciones de Charleston (rip) en la tribu Tupinamba:

1. Dos individuos de clanes distintos no pueden tomar esposa en un mismo clan.
2. Los hijos de dos mujeres de clanes distintos pertenecen a clanes distintos.
3. Los hijos de dos hombres de clanes distintos pertenecen a clanes distintos.
4. Toda clase X aporta mujeres (clase $f^{-1}(X)$) para matrimonios.
5. Toda clase X recibe niños de padre por $p^{-1}(X)$ y de madre por $(m^{-1}(X))$.

Veamos un ejemplo con dos clanes: $C = \{A, B\}$ y las permutaciones

$$f = \begin{pmatrix} A & B \\ B & A \end{pmatrix}, m = \begin{pmatrix} A & B \\ A & B \end{pmatrix}; p = m \circ f = \begin{pmatrix} A & B \\ B & A \end{pmatrix} = f.$$

Una sociedad con esta estructura se denomina de *partes exogámicas maternales*.

Vemos que en esta estructura:

- Toda clase es exogámica: los individuos del clan A se casan con una mujer de B y los de B con una de A.
- Los hijos quedan en la clase de la madre. De aquí viene el adjetivo "maternal".

Veamos lo que podemos deducir de este modelo.

Supongamos dos hermanos: hombre y mujer, ¿en qué clase están los hijos de la hermana?

Los hermanos están en la misma clase, digamos A (ya que los hijos están en la clase de la madre ya sean hombres o mujeres). Como la sociedad es maternal, los hijos de la hermana siguen en A.

Es decir los hijos de la hermana de un padre (hombre casado y con hijos) están en la clase del padre.

¿ Dónde están los hijos de un hermano de una madre?

Ejercicio: Defina, de manera equivalente, una sociedad paternal (línea paterna).

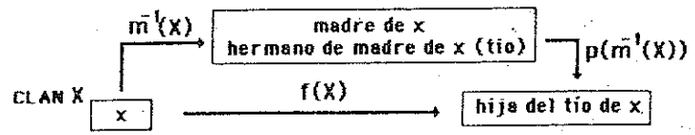
Hay sociedades, como la Tupinamba, donde la formación de parejas es recíproca: si un individuo del clan X debe buscar mujer en Y entonces un individuo de Y debe buscar mujer en X. Diremos que (C, f, m, p) es una estructura de *intercambio recíproco* si y sólo si

$$(RE) \qquad f^2 = f \circ f = id \qquad \text{(función identidad)}. \tag{4.36}$$

La estructura exogámina maternal anterior es de intercambio recíproco (verifique).

Casamiento con primos.

Sea un individuo $x \in X$: su madre es de la clase $m^{-1}(X)$, el hermano de su madre está aún en $m^{-1}(X)$ y los hijos del hermano de su madre están en la clase $p(m^{-1}(X))$:



Más simple, un individuo de la clase X puede casarse con su prima por parte de madre si y sólo si $f(X) = p(m^{-1}(X))$.

Si esto sucede $\forall X \in C$ se tiene $f = p \circ m^{-1}$ y diremos que la sociedad permite el casamiento con la prima por parte de madre:

$$(PM) \qquad f = p \circ m^{-1} \tag{4.37}$$

Como sabemos que $p = m \circ f$:

$$(PM) \qquad f \circ m = m \circ f \quad (m \text{ y } f \text{ conmutan}). \tag{4.38}$$

De manera análoga, un individuo de la clase X puede casarse con su prima por parte de padre (es decir la hija de la hermana del padre) ssi $f(X) = m(p^{-1}(X))$ (verifique).

Si esto sucede $\forall X \in C$ se dice que la sociedad permite el casamiento con la prima por parte de padre:

$$(PP) \qquad f = m \circ p^{-1} \tag{4.39}$$

o de manera equivalente

$$(PP) \qquad f \circ m = m \circ f^{-1}. \tag{4.40}$$

Se tiene la propiedad estructural siguiente:

cada una de las condiciones

$$(RE) \quad f^2 = id, \ (PM) \quad f \circ m = m \circ f, \ (PP) \quad f \circ m = m \circ f^{-1}$$

implica la equivalencia de las otras dos:

$$(RE) \Rightarrow (PP) \Leftrightarrow (PM)$$
$$(PM) \Rightarrow (RE) \Leftrightarrow (PP)$$
$$(PP) \Rightarrow (RE) \Leftrightarrow (PM) \qquad \text{(verifique)}.$$

Un ejemplo interesante es el de los tupinambas cuya estructura (de 4 clanes) es la siguiente:

$$f = \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix}, m = \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix}, p = \begin{pmatrix} A & B & C & D \\ D & C & A & B \end{pmatrix}$$

Teorema tupinamba:

La sociedad Tupinamba es de intercambio recíproco y permite el matrimonio con las primas. (Demuéstrelo).

Ejercicios.

1. Construya sociedades con 4 clanes que verifiquen sólo una de las tres propiedades (RE) o (PP) o (PM).
2. Analice la estructura de 8 clanes:

$$f = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 & B_1 & B_2 & B_3 & B_4 \\ B_1 & B_2 & B_3 & B_4 & A_1 & A_2 & A_3 & A_4 \end{pmatrix}$$

$$m = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 & B_1 & B_2 & B_3 & B_4 \\ A_2 & A_3 & A_4 & A_1 & B_4 & B_1 & B_2 & B_3 \end{pmatrix}$$

$$p = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 & B_1 & B_2 & B_3 & B_4 \\ B_4 & B_1 & B_2 & B_3 & A_2 & A_3 & A_4 & A_1 \end{pmatrix}.$$

* 3. Dada una biyección arbitraria $\psi : C \rightarrowtail C$ (C finito) demuestre que la relación

$\forall X, Y \subseteq C : X \sim Y \Leftrightarrow \exists n \in I\!N$ tal que $\psi^n(X) = Y$,

es de equivalencia.

Demuestre que la clase de $X \in C$:

$$[X] = \{X, \psi(X), ..., \psi^{k-1}(X)\}$$

donde $k > 0$ es el primer natural tal que $\psi^k = id$ (función identidad).

En base a esta relación de equivalencia y en el contexto de una estructura de parentesco definimos:

pares como el conjunto cociente $C/\sim$ con respecto a f.

ciclos, el conjunto cociente $C/\sim$ con respecto a m.

parejas, el conjunto cociente $C/\sim$ con respecto a p.

Determine los pares, ciclos y parejas asociados a la sociedad Tupinamba y la sociedad del ejercicio 2 (con 8 clases).

CAPITULO V

La naturaleza de lo verdadero
se trasluce ya en el cuidado
que pone en ocultarse.
Tristes Trópicos, C. Lévi-Strauss.

ESTRUCTURAS ALGEBRAICAS

5.1 Introducción.

Comencemos con un juego muy simple: dado un número real $x \in \mathbb{R}\backslash\{0\}$, tomemos las siguientes operaciones que nos son cotidianas:

$$x \longrightarrow -x$$
$$x \longrightarrow \frac{1}{x}.$$

Claramente, si partiendo del elemento x, aplicamos cada una de ellas dos veces consecutivas, recuperamos x :

$$x \longrightarrow -x \longrightarrow -(-x) = x$$
$$x \longrightarrow \frac{1}{x} \longrightarrow \frac{1}{(\frac{1}{x})} = x.$$

Es decir, estas dos reglas generan una ley idéntica:

Aplicar dos veces consecutivas la operación nos lleva a la situación inicial.

Es importante el hecho de que ambas operaciones, aritméticamente hablando, son de naturaleza distinta; sin embargo su arquetipo es el mismo, "la doble aplicación no altera la situación inicial". Es como si no se hubiera hecho nada.

Ahora bien, podemos combinar ambas reglas: dado $x \neq 0$

1) Aplicamos
$$x \longrightarrow -x.$$
2) Aplicamos el inverso
$$-x \longrightarrow -\frac{1}{x}$$

Si lo hacemos al revés

1) Aplicamos

$$x \longrightarrow \frac{1}{x}$$

2) Aplicamos el inverso

$$\frac{1}{x} \longrightarrow -\frac{1}{x}$$

Constatamos que no importa el orden, ya que el resultado es el mismo.

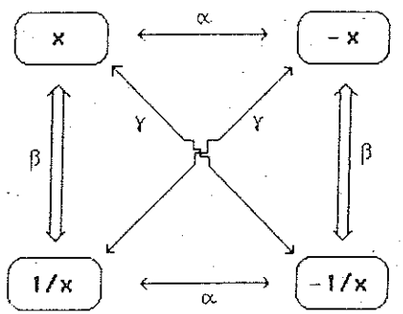
Notemos "x pasa a $-x$" por una flecha, "$\longrightarrow$", y "x pasa a $\frac{1}{x}$" por doble flecha, "$\Longrightarrow$".

Con esta notación, lo que hemos demostrado es:

$$\Longrightarrow\longrightarrow \;=\; \longrightarrow\Longrightarrow$$

Definamos ahora una tercera operación que consiste en aplicar las dos anteriores sucesivamente, la cual notamos "$\rightsquigarrow$". Como no importa el orden en que se apliquen $\Longrightarrow$ y $\longrightarrow$, la nueva operación está bien definida.

Con estas tres operaciones podemos establecer el siguiente diagrama:



Por ejemplo, partiendo de $x \neq 0$:

$$x \longrightarrow -x \Longrightarrow -\frac{1}{x} \equiv x \rightsquigarrow -\frac{1}{x};$$

ahora,

$$-\frac{1}{x} \longrightarrow \frac{1}{x} \Longrightarrow x \equiv -\frac{1}{x} \rightsquigarrow x.$$

Demos nombre a estos objetos en vez de trabajar con jeroglíficos. Sean

e : la operación que consiste en no hacer nada:

α : cambiar el signo de x

β : pasar al inverso de x

γ : cambiar el signo y luego pasar al inverso.

Construyamos una tabla con las posibles combinaciones de estos objetos:

	e	α	β	γ
e	e	α	β	γ
α	α	e	γ	β
β	β	γ	e	α
γ	γ	β	α	e

Por ejemplo,

$\alpha\gamma$ significa, dado $x \neq 0$

1) pasar de x a $-x$ (operación α)
2) pasar de $-x$ a $\frac{1}{x}$ (operación γ).

Pero ir de x a $\frac{1}{x}$ corresponde a la operación β, luego $\alpha\gamma = \beta$.

Mediante flechas:

$$x \longrightarrow -x \rightsquigarrow \frac{1}{x}$$

o bien:

$$x \longrightarrow -x \Longrightarrow -\frac{1}{x} \longrightarrow \frac{1}{x}.$$

Vemos que en la diagonal de la tabla siempre aparece el operador e (no hacer nada) y que el aplicar dos veces cualquier operador es equivalente a aplicar e. En otras palabras, la segunda aplicación deshace el camino o es el camino inverso.

Veamos ahora lo que sucede al aplicar las operaciones en el orden distinto $\alpha(\beta\gamma)$.

1) Aplicamos $\beta\gamma$:

$$x \Longrightarrow \frac{1}{x} \rightsquigarrow -x.$$

2) Aplicamos α :

$$-x \longrightarrow x.$$

Concluyendo, $\alpha(\beta\gamma) = e$.

Desarrollemos ahora $(\alpha\beta)\gamma$

1) Aplicamos $\alpha\beta$:

$$x \longrightarrow -x \Longrightarrow -\frac{1}{x}$$

2) Aplicamos γ :

$$\frac{1}{x} \rightsquigarrow x.$$

Es decir, $(\alpha\beta)\gamma = e$.
De donde

$$\alpha(\beta\gamma) = (\alpha\beta)\gamma$$

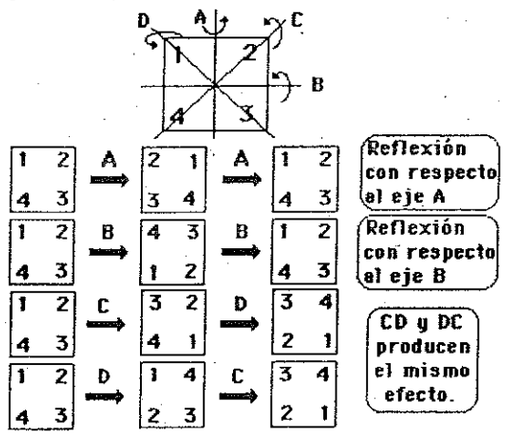
¡no importa el orden de los paréntesis en la aplicación de los operadores!

Vimos anteriormente que $\alpha\beta = \beta\alpha$. En general, de la simetría de la tabla con respecto a la diagonal, vemos que no importa si partimos por la izquierda o por la derecha en la aplicación de los operadores.

Vemos entonces que en este ejemplo tan simple, el conjunto de operadores $\{e, \alpha, \beta, \gamma\}$ satisface cinco propiedades:

1) El resultado de la composición de estas operaciones siempre es un elemento del conjunto de operadores.
2) Existe un elemento que "no hace nada", e, y que denominamos *elemento neutro.*
3) No importa cómo realizamos la operación entre diversos elementos. Esto lo denominamos *asociatividad.*
4) No importa el orden en que realizamos las operaciones. Propiedad llamada *conmutatividad.*
5) Cada elemento tiene asociado otro (en este caso el mismo) que lleva a la situación inicial. Este elemento lo denominamos *inverso.*

Veamos ahora un ejemplo geométrico. Tomemos un cuadrado cuyos vértices están etiquetados con los números $\{1, 2, 3, 4\}$ y permitamos las siguientes operaciones, también denominadas *reflexiones*:



Sean $\{e, \alpha, \beta, \gamma\}$ los operadores siguientes:

e : no realizar ninguna reflexión
α : reflexión con respecto al eje A
β : reflexión con respecto al eje B
γ : reflexión con respecto a los ejes C y D.

Se obtiene la tabla

	e	α	β	γ
e	e	α	β	γ
α	α	e	γ	β
β	β	γ	e	α
γ	γ	β	α	e

que es idéntica a la del ejemplo anterior. De donde concluimos que posée las mismas propiedades.

Tomemos, finalmente, las permutaciones sobre el conjunto $\{1, 2, 3, 4\}$:

$$f_0 = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}, \quad f_1 = \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}, \quad f_2 = \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}, \quad f_3 = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$$

Si formamos la tabla con respecto a la composición de funciones se obtiene:

$\circ$	f_0	f_1	f_2	f_3
f_0	f_0	f_1	f_2	f_3
f_1	f_1	f_0	f_3	f_2
f_2	f_2	f_3	f_0	f_1
f_3	f_3	f_2	f_1	f_0

que es exactamente la misma tabla anterior, si identificamos

$$e \longleftrightarrow f_0, \alpha \longleftrightarrow f_1, \beta \longleftrightarrow f_2, \gamma \longleftrightarrow f_3.$$

De las tres situaciones anteriores vemos que: objetos de naturaleza distinta se estructuran de manera idéntica a un cierto nivel de abstracción. En este sentido, la tabla anterior es "representante" de una serie de fenómenos que son equivalentes entre ellos. Podríamos decir que se trata de tres edificios de aspecto exterior diferente, pero con una estructura común.

Aunque estamos frente a objetos distintos, la manera de relacionarse entre ellos es idéntica. En tal sentido, nuestro estudio ha revelado la estructura

interna de elementos de variada índole y por lo mismo, porque esta estructura es común, nos permite comparar realidades y/o conjuntos de objetos distintos.

De lo anterior podríamos decir que una *estructura* corresponde a las relaciones existentes entre los objetos de un conjunto, donde estas relaciones se definen a partir de operaciones. Estas operaciones imponen propiedades sobre las relaciones entre los elementos y permiten extraer leyes que rigen su comportamiento. También podemos ver que, a partir de la tabla que define la relación entre los elementos, los tres ejemplos anteriores son equivalentes.

5.2 Ley de composición interna.

Sea X un conjunto no vacío, diremos que una función

$$\begin{aligned} * : X \times X &\longrightarrow X \\ (x, y) &\longrightarrow x * y \end{aligned} \tag{5.1}$$

es una *ley de composición interna* (u operación) sobre el conjunto X.

Dado un par de elementos en X, le aplicamos esta "multiplicación" abstracta de modo que el resultado esté también en X.

Un conjunto dotado de una (o varias) leyes de composición interna, se denomina *Estructura Algebraica.*

Como, por definición, $*$ es una función se tiene que:

$$(\forall a, x, y \in X)(x = y) \Longrightarrow \begin{array}{l} x * a = y * a \\ a * x = a * y, \end{array} \tag{5.2}$$

ya que como $*$ es función, las imágenes de (x, a) e (y, a) coinciden cuando x es igual a y. Para la otra igualdad el razonamiento es análogo.

Algunos ejemplos de leyes de composición interna (ℓci) son los siguientes:

- La multiplicación en $\mathbb{R}$.
- La suma en $\mathbb{R}$.
- La unión y la intersección de conjuntos.
- La diferencia simétrica de conjuntos.
- La multiplicación de matrices en $M_{nn}\{0, 1\}$.
- El *mcd* en $\mathbb{N}$.
- La multiplicación en $\mathbb{N}$.

- La conjunción y disyunción en $\{F, V\}$.

No son leyes de composición interna:

- La división en $\mathbb{N}$.
- La resta en $\mathbb{N}$.
- La suma en $\{1, 2, 3\}$.

Las propiedades importantes de una ℓci (que ya vimos en los ejemplos del párrafo anterior, son):

Asociatividad. Una ℓci $*$ en X es asociativa si y sólo si

$$(\forall x, y, z \in X)[x * (y * z) = (x * y) * z]. \tag{5.3}$$

Conmutatividad. Una ℓci $*$ en X es conmutativa si y sólo si

$$(\forall x, y \in X)(x * y = y * x). \tag{5.4}$$

Distributividad. Dadas dos ℓci, $*$ y Δ sobre X, $*$ distribuye con respecto a Δ si y sólo si $\forall x, y, z$

$$x * (y \Delta z) = (x * y) \Delta (x * z) \text{ (distributividad por la izquierda).} \tag{5.5}$$

$$(x \Delta y) * z = (x * z) \Delta (y * z) \quad \text{(distributividad por la derecha).} \tag{5.6}$$

Elemento neutro. Una $\ell.c.i.$ $*$ sobre X admite un elemento neutro si y sólo si

$$(\exists e \in X)(\forall x \in X)(e * x = x * e = x). \tag{5.7}$$

Elemento "cero" o absorbente. Una $\ell.c.i.$ $*$ sobre X admite un elemento absorbente si y sólo si

$$(\exists z \in X)(\forall x \in X)(z * x = x * z = z). \tag{5.8}$$

Idempotencia. Diremos que un elemento $x \in X$ es idempotente si y sólo si

$$x * x = x. \tag{5.9}$$

Elemento inverso. Dado $x \in X$, diremos que $y \in X$ es inverso de x si y sólo si

$$x * y = y * x = e, \tag{5.10}$$

donde e es el neutro. Notaremos, cuando el inverso sea único, $y = x^{-1}$ (notación multiplicativa) o bien $y = -x$ (notación aditiva).

Claramente, un inverso de x^{-1} es $(x^{-1})^{-1} = x$ (justifique).

Ejemplos:

1) Tomemos $(\mathbb{R}, +, \cdot)$. Ambas operaciones son conmutativas, asociativas, existen neutros (0 y 1 respectivamente), elementos inversos, (excepto el 0 para $\cdot$) un elemento absorbente (el 0) para la multiplicación, y la multiplicación distribuye con respecto a la suma.

2) Proposiciones lógicas. En el conjunto de las proposiciones lógicas con las operaciones $(\wedge, \vee)$. Ambas son *ℓ.c.i.* conmutativas y asociativas, ambas distribuyen, existen neutros $(p \vee F \iff p \quad , p \wedge V \iff p)$, no existen inversos y existen elementos absorbentes $(p \vee V \iff V, p \wedge F \iff F)$. Todas las proposiciones son idempotentes $(p \vee p \iff p, \quad p \wedge p \iff p)$.

3) $(\mathcal{P}(X), \cap, \cup)$. Ambas operaciones son asociativas y conmutativas, $\cap$ distribuye con respecto a $\cup$, existe elemento neutro $(A \cap X = A, \ A \cup \phi = A)$, $\forall A \in \mathcal{P}(X), A$ es idempotente $(A \cap A = A \cup A = A)$, no existen inversos.

4) Sea $X = \{1, ..., n\}$ y la estructura algebraica $(S_n, \circ)$ de las permutaciones (o biyecciones) de n elementos. Hemos visto que $\circ$ es asociativa, no es conmutativa, existe un elemento neutro:

$$id : X \longrightarrow X \quad \text{(función identidad)}$$
$$x \longrightarrow x,$$

o bien

$$id = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

Cada permutación p admite un inverso:

$$p = \begin{pmatrix} 1 & 2 & \cdots & n \\ p(1) & p(2) & & p(n) \end{pmatrix}, \quad p^{-1} = \begin{pmatrix} p(1) & p(2) & \cdots & p(n) \\ 1 & 2 & & n \end{pmatrix}.$$

Es directo que $p \circ p^{-1} = p^{-1} \circ p = id$.

No hay elementos idempotentes distintos de id.

Si $p \circ p = p \iff \forall x \in X, \quad p(p(x)) = p(x)$, pero p es una biyección, en particular es inyectiva, luego,

$$\forall x \in X, \quad p(x) = x \iff p = id \quad \blacksquare$$

5) Sea $(\mathbb{R}, *)$ donde $*$ está definida por

$$a * b = a + b + ab \qquad \forall a, b \in \mathbb{R}.$$

Es directo que $*$ es *ℓ.c.i.*

Es asociativa:

$$\begin{aligned} a * (b * c) &= a * (b + c + bc) = \\ &= a + b + c + bc + a(b + c + bc) \\ &= a + b + c + ab + ac + bc + abc. \end{aligned}$$

Por otra parte,

$$\begin{aligned} (a * b) * c &= (a + b + ab) * c = a + b + ab + c + (a + b + ab)c \\ &= a + b + c + ab + ac + bc + abc; \end{aligned}$$

luego, $\qquad a * (b * c) = (a * b) * c.$

Es conmutativa:

$$a * b = a + b + ab = b + a + ba = b * a.$$

Elemento neutro:

$$\begin{aligned} a * x = a &\iff a + x + ax = a \iff \\ &\iff a + x(a + 1) = a \iff x(a + 1) = 0. \end{aligned}$$

El real $x = 0$ verifica la ecuación anterior, de donde,

$$a * 0 = a + 0 + a \cdot 0 = a.$$

Además $0 * a = 0 + a + a \cdot 0 = a$. Luego, 0 es el neutro.

5.3 Propiedades de estructuras.

Sea $(X, *)$ una estructura algebraica, entonces,

Si existe un elemento neutro $e \in X$, este es único. (5.11)

Si $*$ es asociativa y posee un elemento neutro e, entonces

Si existe el inverso de $a \in X$, éste es único. (5.12)

Si a^{-1} es el inverso de a y b^{-1} el de b, entonces $a*b$ tiene inverso y:

$$(a*b)^{-1} = b^{-1} * a^{-1}. \tag{5.13}$$

Demostración.

(5.11) Supongamos que $e, e' \in X$ son neutros, entonces

$$e' = e * e', \quad e = e * e' \Longrightarrow e = e'.$$

(5.12) Supongamos que $y_1, y_2 \in X$ son inversos de $a \in X$

$$y_1 = y_1 * e = y_1 * (a * y_2),$$

como $*$ es asociativa

$$y_1 = (y_1 * a) * y_2 = e * y_2 = y_2.$$

(5.13) Sean a^{-1}, b^{-1} los inversos de a y b respectivamente:

$$\begin{aligned}(b^{-1} * a^{-1}) * (a * b) &= b^{-1} * (a^{-1} * a) * b \\ &= b^{-1} * e * b = b^{-1} * b = e,\end{aligned}$$

por la derecha:

$$\begin{aligned}(a * b) * (b^{-1} * a^{-1}) &= a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} \\ &= a * a^{-1} = e,\end{aligned}$$

luego, por unicidad del inverso concluímos $(a*b)^{-1} = b^{-1} * a^{-1}$ ∎

Hemos visto que la noción de "inverso" requiere la existencia de neutro. En algunas ocasiones se tiene una propiedad más débil que es similar a la de inverso, con la ventaja que no requiere de la existencia de un neutro.

Diremos que un elemento $x \in X$ es *cancelable* con respecto a la *ℓ.c.i.* $*$ si y sólo si $\forall y_1, y_2 \in X$

$$(x * y_1 = x * y_2 \Rightarrow y_1 = y_2) \wedge (y_1 * x = y_2 * x \Longrightarrow y_1 = y_2). \tag{5.14}$$

Un ejemplo en $(\mathbb{Z}, \cdot)$ es el siguiente:

$$\begin{aligned}5 \cdot y_1 &= 5 \cdot y_2 \\ y_1 \cdot 5 &= y_2 \cdot 5\end{aligned} \quad \Longrightarrow \quad y_1 = y_2 \text{ en } \mathbb{Z}.$$

Y acá no existe elemento inverso para la multiplicación en $\mathbb{Z}$.

Una propiedad que liga las nociones de elemento inverso y cancelable es la siguiente: sea $(X, *)$, con $*$ asociativa y elemento neutro e, entonces

un elemento invertible es cancelable. (5.15)

Prueba. Sea $a \in X$, invertible, con inverso a^{-1};

$$\begin{aligned}&y_1 * a = y_2 * a \\ &\Longleftrightarrow (y_1 * a) * a^{-1} = (y_2 * a) * a^{-1} \\ &\Longleftrightarrow y_1 * (a * a^{-1}) = y_2 * (a * a^{-1}) \\ &\Longleftrightarrow y_1 * e = y_2 * e \Longleftrightarrow y_1 = y_2.\end{aligned}$$

Por la izquierda, la demostración es análoga ∎

Consideremos la tabla de Pitágoras:

$*$	1	2	3	4
1	4	2	3	2
2	1	1	3	4
3	4	2	2	1
4	4	1	2	3

acá no hay elemento neutro (¿por qué?), luego, no podemos hablar de inverso. La pregunta es si hay elementos cancelables.

El criterio es el siguiente: si una fila (columna) contiene dos o más elementos iguales, entonces, el elemento que define la fila (columna) de la tabla no es cancelable

$*$		α		β	
		⋮		⋮	
a	⋯	b	⋯	b	⋯
		⋮		⋮	

ya que: $a * \alpha = b = a * \beta$ pero $\alpha \neq \beta$ ∎

Luego, por simple inspección de la tabla anterior, se tiene:

1 no es cancelable $\quad (1*2 = 1*4)$
2 no es cancelable $\quad (2*1 = 2*2)$
3 no es cancelable $\quad (3*2 = 3*3)$.

El único candidato es 4, el cual es cancelable ya que tanto la fila como la columna asociada a él no contienen elementos repetidos.

Notemos que cada fila (columna) de la tabla precedente, puede verse como una función del conjunto $\{1,2,3,4\}$ en sí mismo. Las filas serían:

$$\begin{pmatrix}1&2&3&4\\4&2&3&2\end{pmatrix}\quad\begin{pmatrix}1&2&3&4\\1&1&3&4\end{pmatrix}\quad\begin{pmatrix}1&2&3&4\\4&2&2&1\end{pmatrix}\quad\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}$$

y por columnas

$$\begin{pmatrix}1&4\\2&1\\3&4\\4&4\end{pmatrix}\quad\begin{pmatrix}1&2\\2&1\\3&2\\4&1\end{pmatrix}\quad\begin{pmatrix}1&3\\2&3\\3&2\\4&2\end{pmatrix}\quad\begin{pmatrix}1&2\\2&4\\3&1\\4&3\end{pmatrix}.$$

En esta óptica podemos decir que:

Un elemento $x \in X$ es cancelable si y sólo si su fila y columna en la tabla define dos funciones biyectivas (o permutaciones de los elementos de X). (5.16)

5.4 Subestructuras.

Es interesante preguntarse qué sucede si dada una estructura algebraica $(X,*)$ tomamos $A \subseteq X$ y aplicamos $*$ entre los elementos de A. Por ejemplo, dado $(\mathbb{Z},+)$, tomemos $(\{0,1,2\},+)$.

Claramente, $+$ no es una *ℓ.c.i.* para el conjunto $\{0,1,2\}$, ya que $1+2=3 \notin \{0,1,2\}$. Obviamente, lo que nos interesa es cuando la aplicación de $*$ sobre $A \subseteq X$ deja el resultado al interior de A.

Diremos que $*$ es *cerrada* (o estable) en A si y sólo si

$$\forall x,y \in A \Longrightarrow x*y \in A. \tag{5.17}$$

Un ejemplo de esto último sería $(\mathbb{N},*)$ donde $x*y=\max\{x,y\}$. Sea $(\{0,1,...,n\},*)$. Se tiene

$$\forall x,y \in \{0,1,...n\}, \qquad 0 \leq \max\{x,y\} \leq n,$$

luego $*$ es cerrada en $\{0,1,...,n\}$.

Además, supongamos que $*$ es cerrada en un conjunto $A \subseteq X$, ¿ qué propiedades de $*$ pasan "heredadas" a la subestructura $(A,*)$?

Es directo verificar que

$$*\ \textit{asociativa en } X \Longrightarrow *\ \textit{asociativa en } A. \tag{5.18}$$

$$*\ \textit{conmutativa en } X \Longrightarrow *\ \textit{conmutativa en } A. \tag{5.19}$$

$$a \textit{ cancelable en } X \Longrightarrow a \textit{ cancelable en } A. \tag{5.20}$$

Si, además, se tiene en X se tiene otra *ℓ.c.i.* Δ :

$$*\ \textit{distribuye con respecto a } \Delta \textit{ en } X \Longrightarrow *\ \textit{distribuye con respecto a } \Delta \textit{ en } A. \tag{5.21}$$

Volveremos sobre "subestructuras" más adelante.

5.5 Estructura de congruencias.

Vimos en el Capítulo III el conjunto cociente $\mathbb{Z}_n$, de las clases de congruencia de la suma módulo n :

$$a \equiv b(mod n) \Longleftrightarrow a-b=kn, \quad k \in \mathbb{Z}.$$

Las clases son:

$$[s]=\{x \in \mathbb{Z}/x=kn+s, k \in \mathbb{Z}\} \quad 0 \leq s \leq n-1,$$

luego,

$$\mathbb{Z}_n=\{[0],[1],...,[n-1]\}.$$

Definamos en $\mathbb{Z}_n$ la operación siguiente: $\forall [a],[b] \in \mathbb{Z}_n$

$$[a] \oplus [b] := [a+b]. \tag{5.22}$$

Donde la suma de la derecha es la suma usual en $\mathbb{Z}$.

La definición (5.22) establece que la suma de dos clases de equivalencia corresponde a la clase de equivalencia determinada por la suma (en $\mathbb{Z}$) de sus representantes.

Obviamente $\oplus$ es una ley de composición interna en el conjunto cociente $\mathbb{Z}_n$ ya que $[a+b] \in \mathbb{Z}_n$. Veamos, por ejemplo, lo que sucede para $n=4$. La tabla de Pitágoras es:

$\oplus$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

En efecto,

$$\begin{aligned}
&[0] \oplus [2] = [0+2] = [2] \\
&[2] \oplus [1] = [2+1] = [3] \\
&[2] \oplus [2] = [2+2] = [4] = [2 \cdot 2] = [2k] = [0] \\
&[2] \oplus [3] = [2+3] = [5] = [2 \cdot 2 + 1] = [2k+1] = [1] \\
&[3] \oplus [3] = [3+3] = [6] = [2 \cdot 3] = [2k] = [0], \text{ etc.}
\end{aligned}$$

Recordemos que, en general, $\forall s \geq n$, podemos escribir $s = qn + r$, $0 \leq r < n$, de donde

$$[s] = [qn + r] = [r].$$

Veamos las propiedades de $(\mathbb{Z}_n, \oplus)$:

$\oplus$ es asociativa : es directo de la asociatividad de $+$ en $\mathbb{Z}$

$$\begin{aligned}
[a] \oplus ([b] \oplus [c]) &= [a] \oplus [b+c] = [a+b+c] \\
&= [a+b] \oplus [c] = ([a] \oplus [b]) \oplus [c].
\end{aligned} \tag{5.23}$$

$\oplus$ es conmutativa : es directo de la conmutatividad de $+$ en $\mathbb{Z}$

$$[a] \oplus [b] = [a+b] = [b+a] = [b] \oplus [a]. \tag{5.24}$$

$[0]$ es el elemento neutro:

$$[0] \oplus [a] = [0+a] = [a] = [a+0] = [a] \oplus [0]. \tag{5.25}$$

$\forall [a] \in \mathbb{Z}_n$ existe inverso:

$$\begin{aligned}
[a] \oplus [x] = [0] &\iff [a+x] = [0] \\
&\iff a + x \equiv 0 (\bmod n) \\
&\iff a + x = kn, \quad k \in \mathbb{Z} \\
&\iff x = kn - a, \quad k \in \mathbb{Z}.
\end{aligned} \tag{5.26}$$

En efecto,

$$[a] \oplus [kn - a] = [kn] = [0].$$

Basta, entonces, tomar como representante del inverso de a el elemento $x = -a$ $(k = 0)$, o bien $x = n - a$. Es decir, el inverso de $[a]$, que notamos $-[a]$, (notación aditiva), es $[-a] = [n - a]$.

Introduzcamos ahora una "multiplicación" en $\mathbb{Z}_n$:

$$\forall [a], [b] \in \mathbb{Z}_n : \quad [a] \cdot [b] = [ab]. \tag{5.27}$$

Para $n = 4$:

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

Por ejemplo:

$$[3] \cdot [2] = [3 \cdot 2] = [6] = [4 \cdot 1 + 2] = [2]$$

$$[3] \cdot [3] = [9] = [4 \cdot 2 + 1] = [1].$$

Veamos las propiedades de $\cdot$ en $\mathbb{Z}_n$:

1. La multiplicación $\cdot$, es asociativa y conmutativa, ya que la multiplicación en $\mathbb{Z}$ lo es.
2. Existe elemento neutro; la clase $[1]$.
3. No existe necesariamente inverso. Para $n = 4$, los elementos $[0]$ y $[2]$ no tienen inverso. Sí lo tienen $[1]$ y $[3]$:

$$[1]^{-1} = [1], \quad [3]^{-1} = [3].$$

4. No siempre un elemento es cancelable. Para $n = 4$ los únicos elementos cancelables son $[1], [3]$.
5. Existe un elemento absorbente, $[0]$.
6. La operación $\cdot$ distribuye con respecto a $+$:

$$\begin{aligned}
[a] \cdot ([b] \oplus [c]) &= [a] \cdot [b+c] = [a(b+c)] \\
&= [ab + ac] = [ab] \oplus [ac] = ([a] \cdot [b]) \oplus ([a] \cdot [c]).
\end{aligned}$$

De lo anterior concluímos que la estructura algebraica $(\mathbb{Z}_n, \oplus, \cdot)$ verifica:

$$\oplus \begin{cases} \text{asociativa} \\ \text{conmutativa} \\ \text{admite neutro} \\ \text{cada elemento tiene inverso.} \end{cases} \tag{5.28}$$

$$\cdot \begin{cases} \text{asociativa} \\ \text{conmutativa} \\ \text{admite neutro.} \end{cases} \tag{5.29}$$

$\cdot$ distribuye con respecto a $\oplus$. (5.30)

Veamos a continuación, en un contexto abstracto, los diversos tipos de estructuras, de acuerdo a las propiedades que posean sus leyes de composición interna.

5.6. Clasificación de estructuras.

Dada una estructura algebraica $(X, *)$ diremos que tiene *estructura de grupo* (o que es un grupo), si y sólo si la ley de composición interna $*$ verifica los axiomas siguientes:

$$\begin{array}{l} * \text{ es asociativa} \\ * \text{ admite un elemento neutro} \\ \text{cada elemento de } X \text{ tiene un inverso con respecto a } *. \end{array} \quad (5.31)$$

Cuando, además de estas propiedades, se tiene la conmutatividad, diremos que $(X, *)$ es un *grupo conmutativo o abeliano.*

Supongamos una estructura $(X, *, \Delta)$, con dos leyes de composición interna. Diremos que $(X, *, \Delta)$ un *anillo* si y sólo si

$$\begin{array}{l} (X, *) \text{ es un grupo abeliano} \\ \Delta \text{ es asociativa} \\ \Delta \text{ distribuye con respecto a } * \end{array} \quad (5.32)$$

Diremos que $(X, *, \Delta)$ es un *anillo conmutativo,* si además Δ es conmutativa. Diremos que $(X, *, \Delta)$ es un anillo con *unidad*, si existe elemento neutro para la operación Δ.

Diremos que $(X, *, \Delta)$ es un *cuerpo* si y sólo si

$$\begin{array}{l} (X, *, \Delta) \text{ es un anillo} \\ (X \setminus \{e\}, \Delta) \text{ es un grupo abeliano} \end{array} \quad (5.33)$$

donde el elemento $e \in X$ es el neutro del grupo $(X, *)$.

De las definiciones anteriores vemos que hay una complejidad creciente entre los tres tipos de estructuras, siendo la más "simple" la de *grupo* y la más "compleja" la de *cuerpo.*

Veamos algunos ejemplos de las diversas estructuras:

1) Tenemos que $(S_n, \circ)$ es un grupo, en general, no abeliano, $(Z_n, \oplus)$ es un grupo abeliano.

2) Del parráfo 5.1 tenemos que la tabla de los tres ejemplos es la misma y $(\{e, \alpha, \beta, \gamma\}, \cdot)$ tiene estructura de grupo abeliano (denominado *grupo de Klein*).

3) $(\mathbb{Z}_n, \oplus, \cdot)$ tiene estructura de anillo conmutativo con unidad, pero, en general, no tiene estructura de cuerpo. En efecto, $(\mathbb{Z}_n \setminus \{[0]\}, \cdot)$ en general no es grupo, ya que hay elementos que no tienen inverso para la multiplicación. Al final del capítulo veremos en qué condiciones $(\mathbb{Z}, \oplus, \cdot)$ es un cuerpo.

4) $(\mathbb{R}, +, \cdot)$ es un cuerpo ya que:
$(\mathbb{R}, +)$ es grupo abeliano
$(\mathbb{R} \setminus \{0\}, \cdot)$ es grupo abeliano
$\cdot$ distribuye con respecto a $+$.

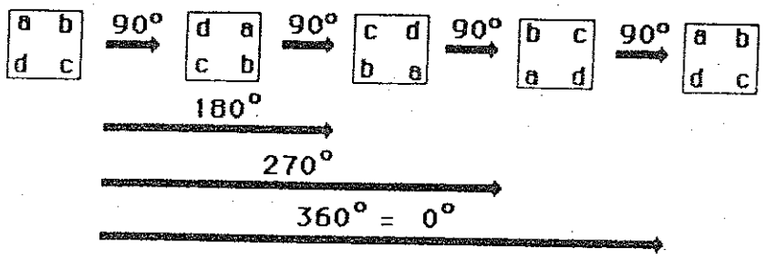
5.7 Morfismos.

En los tres primeros ejemplos del capítulo (signos e inversos en $\mathbb{R}$, reflexiones de un cuadrado y permutaciones) vimos que, aunque la naturaleza de los conjuntos y de las operaciones en cada caso era distinta (significado diferente), a nivel de operatoria compartían exactamente las mismas propiedades (idéntica tabla de Pitágoras). De esto es lógico concluir que estas estructuras, haciendo abstracción de la naturaleza de los objetos que la componen, son iguales. Formalizaremos aquí esta noción de igualdad entre estructuras, que llamaremos *isomorfía.* Tomemos, por ejemplo, el grupo abeliano $(\mathbb{Z}_4, \oplus)$:

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

(se entiende que el entero s corresponde a la clase $[s]$. Omitimos los paréntesis por comodidad.)

Tomemos ahora las rotaciones de múltiplos de 90° de un cuadrado con respecto a su centro en la dirección de los punteros del reloj:



sea

e : rotación de 0°

α : rotación de 90°

β : rotación de 180°

γ : rotación de 270°

Se obtiene la tabla de Pitágoras:

$\bullet$	e	α	β	γ
e	e	α	β	γ
α	α	β	γ	e
β	β	γ	e	α
γ	γ	e	α	β

Ahora, si identificamos mediante una función las tablas de las estructuras $(\mathbb{Z}_4, \oplus)$ y $(\{e, \alpha, \beta, \gamma\}, \bullet)$, se obtiene

$$\begin{aligned} \varphi : \mathbb{Z}_4 &\longrightarrow \{e, \alpha, \beta, \gamma\} \\ 0 &\longrightarrow e \\ 1 &\longrightarrow \alpha \\ 2 &\longrightarrow \beta \\ 3 &\longrightarrow \gamma \end{aligned}$$

que es, obviamente, una biyección.

Además, al hacer la identificación ambas tablas se confunden. Es decir, la composición de dos elementos en $\mathbb{Z}_4$ mediante $\oplus$ es lo mismo, vía la identificación, que tomar la composición de sus imágenes con la operación $\bullet$:

$$\varphi(x \oplus y) = \varphi(x) \bullet \varphi(y). \tag{5.34}$$

Por ejemplo:

$$\begin{array}{ccccc} 1 & \oplus & 2 & = & 3 \\ \varphi \downarrow & & & & \uparrow \varphi^{-1} \\ \alpha & \bullet & \beta & = & \gamma \end{array}$$

Es claro que la situación anterior no siempre se da. Un ejemplo es la tabla del grupo de Klein y la anterior:

$\cdot$	e	α	β	γ
e	e	α	β	γ
α	α	e	γ	β
β	β	γ	e	α
γ	γ	β	α	e

$\neq$

$\bullet$	e	α	β	γ
e	e	α	β	γ
α	α	β	γ	e
β	β	γ	e	α
γ	γ	e	α	β

Si, por ejemplo, en el grupo de Klein calculamos

$$\alpha \cdot \alpha = e = \text{ neutro.}$$

En el otro grupo se tiene $\alpha \bullet \alpha = \beta \neq$ neutro . Más aún, en el grupo de Klein todos los elementos son su propio inverso, lo que no sucede en la otra estructura. Es posible demostrar que no existe una biyección entre los elementos de manera que se satisfaga la igualdad (5.34) (verifique).

Formalicemos lo anterior. Dadas dos estructuras algebraicas $(X, *)$, (Y, Δ), una función $f : X \longrightarrow Y$ se denomina un *homomorfismo* si y sólo si

$$(\forall x_1, x_2 \in X)(f(x_1 * x_2) = f(x_1) \Delta f(x_2)). \tag{5.35}$$

Además, diremos que:

f es un *isomorfismo* si y sólo si f es biyectiva (5.36)

f es un *automorfismo* si y sólo si $X = Y$ y f es *isomorfismo.* (5.37)

Diremos que dos estructuras algebraicas $(X, *), (Y, \Delta)$ son *isomorfas* si existe un isomorfismo entre ellas. En tal caso notaremos $(X, *) \cong (Y, \Delta)$.

La relación $\cong$ entre estructuras algebraicas es de equivalencia.

Prueba:

- Refleja: $(X, *) \cong (X, *)$, basta tomar $f =$ id $: X \to X$.

- Simétrica: $(X,*) \cong (Y,\Delta) \iff \exists f : X \to Y$ isomorfismo, luego $f^{-1} : Y \to X$ es biyectiva. Calculemos $f^{-1}(a\Delta b) =?$

Como f es epiyectiva $\Longrightarrow \exists x_1, x_2 \in X$ tales que $a = f(x_1), b = f(x_2)$. Luego,

$$a\Delta b = f(x_1)\Delta f(x_2) = f(x_1 * x_2),$$

de donde

$$f^{-1}(a\Delta b) = f^{-1}(f(x_1 * x_2)) = x_1 * x_2$$
$$= f^{-1}(a) * f^{-1}(b),$$

luego, f^{-1} es un isomorfismo, de donde concluímos $(Y,\Delta) \cong (X,\Delta)$.

- Transitiva:

$$[(X,*) \cong (Y,\Delta)] \wedge [(Y,\Delta) \cong (Z,\sqcup)] \iff$$

$\exists f : X \to Y, g : Y \to Z$ ambos isomorfismos, luego $g \circ f : X \to Z$ es biyectiva (ver propiedades de la composición de biyecciones en el capítulo IV). Además, como f, g son homomorfismos

$$(g \circ f)(x_1 * x_2) = g(f(x_1 * x_2)) = g(f(x_1)\Delta f(x_2))$$

$$= g(f(x_1)) \sqcup g(f(x_2)).$$

Concluímos entonces que $g \circ f : X \to Z$ es un isomorfismo, ergo $(X,*) \cong (Z,\sqcup)$ ■

De lo anterior se tiene que $\cong$ induce una partición del conjunto de estructuras en clases de equivalencia. En tal sentido los tres ejemplos iniciales del capítulo están en la misma clase de equivalencia.

Aunque intuitivamente es claro que dos estructuras isomorfas tienen propiedades análogas, precisémoslo mediante las proposiciones siguientes:

Sea $(X,*) \cong (Y,\Delta)$, donde $f : X \to Y$ es un isomorfismo entre ambas estructuras.

$*$ *es asociativa* $\iff \Delta$ *asociativa.* (5.38)

$*$ *es conmutativa* $\iff \Delta$ *conmutativa.* (5.39)

e *neutro de* $X \iff f(e)$ *neutro de* Y (5.40)

x *invertible en* $X \iff f(x)$ *invertible en* Y, (5.41)

además $(f(x))^{-1} = f(x^{-1})$.

x *cancelable en* $X \iff f(x)$ *cancelable en* Y. (5.42)

Prueba:

(5.38), Sean $x_1, x_2, x_3 \in X$ tales que $f(x_1) = y_1, \quad f(x_2) = y_2, \quad f(x_3) = y_3$.

$$\Longrightarrow \quad y_1\Delta(y_2\Delta y_3) = f(x_1)\Delta(f(x_2 * x_3)) =$$
$$= f(x_1 * (x_2 * x_3));$$

como $*$ es asociativa:

$$= f((x_1 * x_2) * x_3) =$$
$$= f(x_1 * x_2)\Delta f(x_3) = (f(x_1)\Delta f(x_2))\Delta f(x_3)$$
$$= (y_1\Delta y_2)\Delta y_3.$$

En el otro sentido se demuestra de manera análoga.

(5.40) $\Longrightarrow$) Sea $y \in Y$, luego $\exists x \in X, y = f(x)$.

$$f(e)\Delta y = f(e)\Delta f(x) = f(e * x) = f(x) = y,$$

análogamente $y\Delta f(e) = y$.

(5.41) $f(x)\Delta f(x^{-1}) = f(x * x^{-1}) = f(e)$ que es neutro de Y ■

En el caso de estructuras con dos operaciones, $(X,*_1,\Delta_1),(Y,*_2,\Delta_2)$, diremos que son isomorfas si existen isomorfismos para ambas operaciones. Es decir, dos biyecciones $\varphi : X \to Y, \psi : X \to Y$, tales que:

$$\varphi(a *_1 b) = \varphi(a) *_2 \varphi(b)$$
$$\psi(a\Delta_1 b) = \psi(a)\Delta_2\psi(b).$$

La noción de isomorfía entre estructuras es muy útil. En particular, en ella se basa el computador al cual alimentamos con números en $\mathbb{Q}$ con las operaciones usuales. Este los convierte (vía una biyección φ) en expresiones binarias en el conjunto $\{0,1\}$, operando con ellas mediante otra suma y multiplicación para, finalmente, "decodificarlas", vía φ^{-1}, y presentarnos el resultado racional (y... compresible) que vemos en la pantalla.

5.8 Grupos.

Recordemos que un *grupo* es una estructura algebraica $(\mathcal{G},*)$ que verifica los axiomas siguientes: $*$ es asociativa, existe un elemento neutro y cada elemento posee inverso. Si, además, $*$ es conmutativa se dice que el grupo es *abeliano*.

Como ejemplos de grupo podemos citar el de Klein $(\{e,\alpha,\beta,\gamma,\},\bullet)$, $(S_n,\circ)$, $(\mathbb{Z}_n,\oplus)$, $(\mathbb{R},+)$, $(\mathbb{Z},+)$, $(\mathbb{R}\setminus\{0\},\cdot)$.

Diremos que el *orden* de un grupo $(\mathcal{G},*)$, es el cardinal de $\mathcal{G}$.

5.8.1. Propiedades elementales de un grupo.

Sea $(\mathcal{G},*)$ un grupo:

$$\forall a,b\in\mathcal{G}, \textit{la ecuación } a*x{=}b \textit{ tiene solución única en } \mathcal{G}. \tag{5.43}$$

$$\forall a\in\mathcal{G}, \textit{ es cancelable.} \tag{5.44}$$

Si el orden de $(\mathcal{G},*)$ es finito, cada línea (o columna) de la tabla de Pitágoras es una permutación de los elementos de $\mathcal{G}$. (5.45)

Demostración. (5.43) Existencia:

$$\begin{aligned} a*x=b &\iff a^{-1}*(a*x)=a^{-1}*b\\ &\iff (a^{-1}*a)*x=a^{-1}*b\\ &\iff e*x=a^{-1}*b \iff x=a^{-1}*b. \end{aligned}$$

Unicidad : Supongamos $x_1,x_2\in G$ son soluciones de la ecuación

$$\begin{aligned} (a*x_1=b)\wedge\ (a*x_2=b) &\iff a*x_1=a*x_2\\ &\iff a^{-1}*(a*x_1)=a^{-1}*(a*x_2)\\ &\iff (a^{-1}*a)*x_1=(a^{-1}*a)*x_2\\ &\iff e*x_1=e*x_2 \iff x_1=x_2. \end{aligned}$$

(5.44) Tomemos $a*b_1=a*b_2\iff(a^{-1}*a)*b_1=(a^{-1}*a)*b_2\iff b_1=b_2$. De manera análoga $b_1*a=b_2*a\iff b_1=b_2$.

(5.45) Del parráfo anterior sabemos que un elemento es cancelable si y sólo si su fila y columna en la tabla de Pitágoras no tienen elementos repetidos. Luego, concluímos el resultado directamente de (5.44).

Para ver cuál es el grado de restricción que imponen los axiomas de un grupo sobre la estructura, veamos cuántos grupos no isomorfos hay para conjuntos $\mathcal{G}$ de cardinal pequeño.

Sea $\mathcal{G}=\{a_0,a_1\}$ con una *ℓ.c.i.* $*$. Para que sea grupo, uno de los elementos debe ser el neutro. Sea éste a_0. Se tiene entonces:

$$\begin{array}{ccc} * & a_0 & a_1\\ a_0 & a_0 & a_1\\ a_1 & a_1 & ? \end{array} \Longrightarrow \begin{array}{ccc} * & a_0 & a_1\\ a_0 & a_0 & a_1\\ a_1 & a_1 & a_0 \end{array}$$

Ya que cada elemento debe tener inverso, necesariamente $a_1*a_1=a_0$. Es decir, para $|\mathcal{G}|=2$ existe una sola clase de equivalencia de grupos de orden 2. Todos son isomorfos. Además, los grupos de orden 2 son abelianos.

Analicemos ahora los grupos de orden 3. De manera análoga, sea a_0 el neutro:

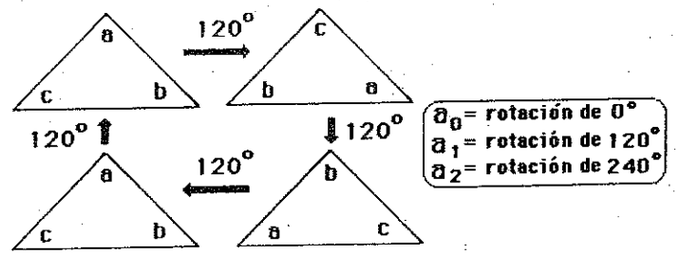
$$\begin{array}{cccc} * & a_0 & a_1 & a_2\\ a_0 & a_0 & a_1 & a_2\\ a_1 & a_1 & ? & ?\\ a_2 & a_2 & ? & ? \end{array}$$

Si $a_1*a_1=a_0$, como cada fila y columna de un grupo finito es una permutación de sus elementos, se obtiene $a_2*a_1=a_2$. Lo cual es una contradicción, pues se repetiría a_2 en la tercera fila. Luego, necesariamente: $a_1*a_1=a_2$, $\quad a_1*a_2=a_0$ y en la tercera fila $a_2*a_1=a_0$ y $a_2*a_2=a_1$. Concluímos entonces que la tabla de Pitágoras de un grupo de orden 3 es la siguiente:

$$\begin{array}{cccc} * & a_0 & a_1 & a_2\\ a_0 & a_0 & a_1 & a_2\\ a_1 & a_1 & a_2 & a_0\\ a_2 & a_2 & a_0 & a_1 \end{array}$$

Ergo, todos los grupos de orden 3 son isomorfos y además abelianos.

Un grupo de orden 3, que da una representación geométrica de la tabla de Pitágoras anterior, es el de las rotaciones de un triángulo equilátero en torno a su centro, de manera que, luego de cada rotación, coincida consigo mismo:



Es directo ver que éste es un grupo de orden 3.

Veamos ahora qué sucede para $|\mathcal{G}| = 4$. Sabemos, de los ejemplos anteriores, que al menos existen 2 grupos de orden 4 no isomorfos; el de Klein y el de las rotaciones de un cuadrado. No es difícil probar, siguiendo el esquema del caso anterior, que no existe otra clase de isomorfía para este orden (cualquier tabla de un grupo con cuatro elementos es equivalente a una de los dos anteriores) y además que cualquier grupo de orden 4 es abeliano (demuéstrelo).

Para órdenes superiores, el análisis se complica. Veremos más adelante que todavía para el orden 5 todos los grupos son abelianos. Para el orden 6 esto ya no se verifica; basta recordar el grupo de las permutaciones $(S_3, \circ)$, que no es abeliano.

5.8.2 Subgrupos.

Dado un grupo $(\mathcal{G}, *)$, diremos que $(\mathcal{H}, *)$ es un *subgrupo* de $\mathcal{G}$ si y sólo si

$$\begin{aligned} &\phi \neq \mathcal{H} \subseteq \mathcal{G} \\ &(\mathcal{H}, *) \text{ es grupo.} \end{aligned} \tag{5.46}$$

La segunda propiedad nos indica que $*$ debe ser cerrada en $\mathcal{H}$ (si nó no sería *ℓ.c.i.* y luego, $\mathcal{H}$ no sería grupo). Además, si $x \in \mathcal{H}$ necesariamente su inverso x^{-1} debe estar en $\mathcal{H}$.

La asociatividad no es problema, ya que, dado que ésta se verifica en $\mathcal{G}$, se verifica en cualquiera de sus subconjuntos.

De las consideraciones anteriores podemos caracterizar un subgrupo como sigue: dado $\phi \neq \mathcal{H} \subseteq \mathcal{G}$ entonces

$$\mathcal{H} \text{ es subgrupo de } \mathcal{G} \Longleftrightarrow (\forall h_1, h_2 \in \mathcal{H} \Longrightarrow h_1 * h_2^{-1} \in \mathcal{H}). \tag{5.47}$$

En efecto:

$\Longrightarrow$) si $\mathcal{H}$ es subgrupo de $\mathcal{G}$, luego $*$ es una *ℓ.c.i.* cerrada en $\mathcal{H}$ y además, dados
$h_1, h_2 \in \mathcal{H} \Longrightarrow h_2^{-1} \in \mathcal{H}$ y por la cerradura $h_1 * h_2^{-1} \in \mathcal{H}$.
$\Longleftarrow$) La asociatividad no es problema, ya que es heredada del grupo $(\mathcal{G}, *)$.
Tomando $h_1 = h_2 \Longrightarrow e = h_1 * h_1^{-1} \in \mathcal{H}$.
Tomando $e, h_1 \Longrightarrow e * h_1^{-1} \in \mathcal{H} \Longleftrightarrow h_1^{-1} \in \mathcal{H}$. Finalmente, $*$ es cerrada en $\mathcal{H}$: $h_1 * h_2 = h_1 * (h_2^{-1})^{-1} \in \mathcal{H}$ (pues $h_1, h_2^{-1} \in \mathcal{H}$ y aplicamos la hipótesis).

Concluímos entonces que $(\mathcal{H}, *)$ es un subgrupo de $(\mathcal{G}, *)$ ■

Diremos que $(\mathcal{H}, *)$ es un subgrupo *propio* de $\mathcal{G}$ si $\mathcal{H} \subseteq \mathcal{G}$ y $\mathcal{H} \neq \mathcal{G}$.

Ejemplos de subgrupos:

1. En el grupo de Klein de orden cuatro, $(\{e, \alpha\}, \bullet)$ es un subgrupo propio.
2. $(\mathbb{Z}, +)$ es un subgrupo de $(\mathbb{R}, +)$.
3. $(\{e\}, *), (\mathcal{G}, *)$ son subgrupos triviales de $(\mathcal{G}, *)$.

Más adelante veremos subgrupos interesantes de $(S_n, \circ)$ y en los ejercicios se propone el estudio de los subgrupos de las rotaciones y reflexiones de un cuadrado.

Una propiedad que relaciona un subgrupo $(\mathcal{H}, *)$ con el grupo $(G, *)$ es la siguiente:

$$\textit{El neutro y los inversos coinciden en } (\mathcal{H}, *) \textit{ y } (\mathcal{G}, *). \tag{5.48}$$

En efecto, notemos por $e_\mathcal{H}, e_\mathcal{G}$ los neutros de $\mathcal{H}$ y $\mathcal{G}$, respectivamente. Se tiene

$$\forall h \in \mathcal{H} : e_\mathcal{H} * h = h * e_\mathcal{H} = h$$

$$\forall x \in \mathcal{G} : e_\mathcal{G} * x = x * e_\mathcal{G} = x,$$

de donde:

$$h * e_\mathcal{H} = h * e_\mathcal{G} \quad \forall h \in \mathcal{H}. \tag{5.49}$$

Además:

$$e_\mathcal{H} = e_\mathcal{G} * e_\mathcal{H}.$$

Como $e_\mathcal{G}$ es neutro de $\mathcal{G} \supseteq \mathcal{H}$:

$$\begin{aligned} e_\mathcal{H} &= (h^{-1} * h) * e_\mathcal{H} \\ &= h^{-1} * (h * e_\mathcal{H}), \end{aligned}$$

de la identidad (5.49) :

$$\begin{aligned} &= h^{-1} * (h * e_\mathcal{G}) \\ &= (h^{-1} * h) * e_\mathcal{G}. \end{aligned}$$

Como $e_\mathcal{G}$ es neutro de $\mathcal{G} \supseteq \mathcal{H}$:

$$e_\mathcal{H} = e_\mathcal{G} * e_\mathcal{G} = e_\mathcal{G}.$$

Supongamos ahora que los inversos de h son $x_1 \in \mathcal{H}$ y $x_2 \in \mathcal{G}$. Luego, estos elementos verifican:

$$h * x_1 = x_1 * h = e$$
$$h * x_2 = x_2 * h = e.$$

Tomando la igualdad $h * x_1 = e$ y aplicando x_2 por la izquierda se obtiene:

$$x_2 * (h * x_1) = x_2 * e$$
$$\Longleftrightarrow (x_2 * h) * x_1 = x_2 \Longleftrightarrow e * x_1 = x_2 \Longleftrightarrow x_1 = x_2 \quad \blacksquare$$

5.8.3 Representación de Cayley.

Hemos visto en el párrafo anterior que en la tabla de Pitágoras de un grupo finito, las filas y columnas son permutaciones de los elementos del grupo. Esto nos lleva a preguntarnos si existe un procedimiento que permita establecer un isomorfismo entre un grupo finito y un grupo de permutaciones. La respuesta está establecida en el **teorema de Cayley**:

Todo grupo finito es isomorfo a un grupo de permutaciones. (5.50)

Verificaremos este resultado a través de un ejemplo. Posteriormente daremos una demostración formal.

Tomemos el grupo de Klein, K_4 :

$*$	a_0	a_1	a_2	a_3		
a_0	a_0	a_1	a_2	a_3	$\longleftarrow$	fila 0
a_1	a_1	a_0	a_3	a_2	$\longleftarrow$	fila 1
a_2	a_2	a_3	a_0	a_1	$\longleftarrow$	fila 2
a_3	a_3	a_2	a_1	a_0	$\longleftarrow$	fila 3.

Como ya sabemos, cada fila de la tabla de Pitágoras es una permutación de los elementos $\{a_0, a_1, a_2, a_3\}$. Tomemos entonces, como candidatos a formar un grupo de permutaciones, isomorfo a K_4, las permutaciones dadas por las filas de la tabla asociada a K_4 :

$$p_0 = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ a_0 & a_1 & a_2 & a_3 \end{pmatrix} \quad \text{permutación asociada a fila 0}$$

$$p_1 = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ a_1 & a_0 & a_3 & a_2 \end{pmatrix} \quad \text{permutación asociada a fila 1}$$

$$p_2 = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ a_2 & a_3 & a_0 & a_1 \end{pmatrix} \quad \text{permutación asociada a fila 2}$$

$$p_3 = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{pmatrix} \quad \text{permutación asociada a fila 3.}$$

Veamos si $(\{p_0, p_1, p_2, p_3\}, \circ)$ es grupo. Ya sabemos que $\circ$ es asociativa. Construyamos la tabla de Pitágoras de esta estructura:

$\circ$	p_0	p_1	p_2	p_3
p_0	p_0	p_1	p_2	p_3
p_1	p_1	p_0	p_3	p_2
p_2	p_2	p_3	p_0	p_1
p_3	p_3	p_2	p_1	p_0

A partir de ella verificamos que $(\{p_0, p_1, p_2, p_3\}, \circ)$ es grupo abeliano y, además, estableciendo la función

$$\varphi : p_0 \to a_0, \quad p_1 \to a_1 \quad p_2 \to a_2, \quad p_3 \to a_3$$

las tablas se confunden, con lo cual probamos la isomorfía en este caso particular ■

Demostración del teorema de Cayley:

Sea $(\mathcal{G}, *)$ el grupo finito, donde $\mathcal{G} = \{a_0, a_1, ..., a_{n-1}\}$ tiene orden n. Sin pérdida de generalidad, supongamos que el neutro de $\mathcal{G}$ es a_0 y escribamos la tabla de Pitágoras asociada a $\mathcal{G}$:

$*$	a_0	a_1	$\cdots$	a_j	$\cdots$	a_{n-1}	
a_0	a_0			a_j		a_{n-1}	fila 0
$\vdots$	$\vdots$			$\vdots$		$\vdots$	
a_i	$a_i * a_0$	$a_i * a_1$	$\cdots$	$a_i * a_j$	$\cdots$	$a_i * a_{n-1}$	fila i
$\vdots$	$\vdots$			$\vdots$			
a_{n-1}	a_{n-1}		$\cdots$	$a_{n-1} * a_j$	$\cdots$	$a_{n-1} * a_{n-1}$	fila $n-1$
				columna j			

De manera análoga al ejemplo, tomemos las permutaciones:

$$p_{a_o} = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_0 & a_1 & \cdots & a_{n-1} \end{pmatrix}$$

$$p_{a_1} = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_1 * a_0 & a_1 * a_1 & \cdots & a_1 * a_{n-1} \end{pmatrix}$$

$$p_{a_i} = \begin{pmatrix} a_0 & a_1 & \cdots & a_j & \cdots & a_{n-1} \\ a_i * a_0 & a_i * a_1 & \cdots & a_i * a_j & \cdots & a_i * a_{n-1} \end{pmatrix}$$

$$p_{a_{n-1}} = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1} * a_0 & a_{n-1} * a_1 & \cdots & a_{n-1} * a_{n-1} \end{pmatrix}.$$

Sea $\mathcal{P} = \{p_{a_i}\}_{i=1}^{n}$ probaremos que $(\mathcal{G}, *) \cong (\mathcal{P}, \circ)$. Para ello debemos establecer una biyección que sea un homomorfismo entre ambas estructuras.

Sea la función canónica (¡la obvia!):

$$\varphi : \mathcal{G} \to \mathcal{P}$$
$$a_i \to p_{a_i} \quad 0 \leq i \leq n-1.$$

Claramente, φ es una biyección. Veamos si es un homomorfismo:

$$\varphi(a_i * a_j) = p_{a_i * a_j} = \begin{pmatrix} a_0 & \cdots & a_s & \cdots & a_{n-1} \\ (a_i * a_j) * a_0 & \cdots & (a_i * a_j) * a_s & \cdots & (a_i * a_j) * a_{n-1} \end{pmatrix}$$

Como $*$ es asociativa:

$$= \begin{pmatrix} a_0 & \cdots & a_s & \cdots & a_{n-1} \\ a_i * (a_j * a_0) & \cdots & a_i * (a_j * a_s) & \cdots & a_i * (a_j * a_{n-1}) \end{pmatrix}$$

Ahora bien:

$$p_{a_j} = \begin{pmatrix} a_0 & \cdots & a_s & \cdots & a_{n-1} \\ a_j * a_0 & \cdots & a_j * a_s & \cdots & a_j * a_{n-1} \end{pmatrix}$$

corresponde a la j-ésima fila de la tabla asociada a $\mathcal{G}$ y se tiene el esquema

$$\forall s \in \{0, \cdots, n-1\} : \quad a_s \overset{p_{a_j}}{\longrightarrow} a_j * a_s \overset{p_{a_i}}{\longrightarrow} a_i * (a_j * a_s).$$

Es decir:

$$\varphi(a_i * a_j) = p_{a_i * a_j}$$
$$= \begin{pmatrix} a_0 & \cdots & a_{n-1} \\ a_i * a_0 & \cdots & a_i * a_{n-1} \end{pmatrix} \circ \begin{pmatrix} a_0 & \cdots & a_{n-1} \\ a_j * a_0 & \cdots & a_j * a_{n-1} \end{pmatrix}$$
$$= p_{a_i} \circ p_{a_j} = \varphi(a_i) \circ \varphi(a_j).$$

Luego, φ es un isomorfismo, de donde $(\mathcal{G}, *) \cong (\mathcal{P}, \circ)$ ■

De lo anterior podemos extraer algunas conclusiones:

1. $(S_n, \circ)$ admite subgrupos propios. Por ejemplo, para $n = 4$, el grupo de permutaciones isomorfo al grupo de Klein, K_4, es un subgrupo propio

de $(S_4, \circ)$. Sucede lo mismo con el grupo de permutaciones isomorfo a las rotaciones de un cuadrado.

2. Cada vez que se trabaja con un grupo finito, podemos "pasar", vía la isomorfía anterior, a un subgrupo de permutaciones, lo que muchas veces simplifica el trabajo.

5.8.4 Grupo de matrices isomorfo a $(S_n, \circ)$.

Dado el grupo $(S_n, \circ)$, definimos el conjunto de *matrices de permutación*, $MP_n(\{0,1\})$, con elementos 0's, 1's, tal que cada matriz tiene sólo un uno por fila y columna. Por ejemplo, para $n = 3$:

$$MP_3(\{0,1\}) = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \right.$$
$$\left. \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \right\}.$$

Formalmente:

$$MP_n(\{0,1\}) = \{M \in M_{nn}(\{0,1\}) / \sum_{j=1}^{n} m_{ij} = \sum_{i=1}^{n} m_{ij} = 1 \ \forall i, j\} \qquad (5.51)$$

Es importante señalar que en la caracterización anterior la sumatoria se entiende con la suma usual en $\mathbb{R}$.

Es evidente que $MP_n(\{0,1\}) \subseteq M_{nn}(\{0,1\})$, (matrices de n filas y n columnas con elementos en $\{0,1\}$).

Por otra parte,

la multiplicación de matrices es asociativa en $M_{nn}(\{0,1\})$. (5.52)

En efecto, sean $A, B, C \in \mathcal{M}_{nn}(\{0,1\}); A = (a_{ij}), B = (b_{ij}), C = (c_{ij})$, debemos probar que $A \cdot (B \cdot C) = (A \cdot B) \cdot C$. Consideremos $D = A \cdot (B \cdot C)$ y $E = (A \cdot B) \cdot C$. Para verificar la asociatividad demostraremos que $D = E$ o, de manera equivalente:

$$d_{ij} = e_{ij} \qquad \forall i, j \in \{1, ..., n\}.$$

Calculemos el término d_{ij}. Por definición, éste es el producto de la fila i de la matriz A por la columna j de la matriz $S = B \cdot C$. Esquemáticamente

$$d_{ij} = (a_{i1}a_{i2},...,a_{in}) \begin{pmatrix} s_{1j} \\ s_{2j} \\ \vdots \\ s_{nj} \end{pmatrix} = \sum_{\ell=1}^{n} a_{i\ell}s_{\ell j}, \qquad (5.53)$$

pero,

s_{1j} : es el producto de la fila 1 de B por la columna j de C
s_{2j} : es el producto de la fila 2 de B por la columna j de C
$\vdots$
s_{nj} : es el producto de la fila n de B por la columna j de C.

Es decir,

$$s_{1j} \text{ está dado por } (b_{11},...,b_{1n}) \begin{pmatrix} c_{1j} \\ c_{2j} \\ \vdots \\ c_{nj} \end{pmatrix}$$

$$s_{2j} \text{ está dado por } (b_{21},...,b_{2n}) \begin{pmatrix} c_{1j} \\ c_{2j} \\ \vdots \\ c_{nj} \end{pmatrix}$$

$$\vdots$$

$$s_{nj} \text{ está dado por } (b_{n1},...,b_{nn}) \begin{pmatrix} c_{1j} \\ c_{2j} \\ \vdots \\ c_{nj} \end{pmatrix}$$

De la definición de producto matricial:

$$s_{1j} = \sum_{k=1}^{n} b_{1k}c_{kj}, \quad s_{2j} = \sum_{k=1}^{n} b_{2k}c_{kj}, ..., s_{nj} = \sum_{k=1}^{n} b_{nk}c_{kj}.$$

Reemplazando en (5.53):

$$d_{ij} = \sum_{\ell=1}^{n} a_{i\ell}(\sum_{k=1}^{n} b_{\ell k}c_{kj}).$$

De manera análoga se tiene que e_{ij} es el producto de la i-ésima fila de $A \cdot B$ por la j-ésima fila de C :

$$e_{ij} = (\sum_{\ell=1}^{n} a_{i\ell}b_{\ell 1}, ..., \sum_{\ell=1}^{n} a_{i\ell}b_{\ell n}) \begin{pmatrix} c_{1j} \\ c_{2j} \\ \vdots \\ c_{nj} \end{pmatrix}$$

de donde:

$$e_{ij} = \sum_{k=1}^{n}(\sum_{\ell=1}^{n} a_{i\ell}b_{\ell k})c_{kj}.$$

Cambiando el orden de las sumatorias:

$$e_{ij} = \sum_{\ell=1}^{n} a_{i\ell}(\sum_{k=1}^{n} b_{\ell k}c_{kj}) = d_{ij},$$

luego, la multiplicación de matrices en $\{0,1\}$ es asociativa ■

Además, la multiplicación admite un elemento neutro, *la matriz identidad:*

$$I = \begin{pmatrix} 1 & & & \\ & 1 & & 0 \\ & & \ddots & \\ & 0 & & 1 \\ & & & & 1 \end{pmatrix}, \text{ o bien } I = (\delta_{ij}), \quad \delta_{ij} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases} \qquad (5.54)$$

En efecto, dada $A \in \mathcal{M}_{nn}(\{0,1\})$ se tiene:

$$A \cdot I = (\sum_{k=1}^{n} a_{ik}\delta_{kj})$$

pero $\sum_{k=1}^{n} a_{ik}\delta_{kj}$ es el producto de la fila i-ésima de A por la columna j de I :

$$(a_{i1}, a_{i2}, ..., a_{ij}, ..., a_{in}) \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \longleftarrow \text{ posición } j$$

luego,

$$\sum_{k=1}^{n} a_{ik}\delta_{kj} = a_{i1}0 + \cdots + a_{ij-1}0 + a_{ij}\cdot 1 + a_{ij+1}0 + \cdots + a_{in}0 = a_{ij},$$

concluyendo que $A \cdot I = (a_{ij}) = A$. La multiplicación por la izquierda se demuestra de manera análoga ■

Veamos si la multiplicación es cerrada en $MP_n(\{0,1\})$. Consideremos $A, B \in MP_n(\{0,1\})$ y tomemos su producto:

$$C = A \cdot B = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ & \vdots & \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ & \vdots & \\ b_{n1} & \cdots & b_{nn} \end{pmatrix},$$

obteniendo $C = (c_{ij})$, donde $c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}, \forall i, j \in \{1, ..., n\}$.

Recuerde que normalmente utilizamos la suma booleana $(1 + 1 = 1)$. Si cambiamos esta manera de sumar por la suma usual en $\mathbb{R}$, lo único que sucede es que acumulamos unos $(1 + 1 = 2)$. Para que la matriz $C \in MP_n(\{0,1\})$, de acuerdo a la caracterización de este conjunto, nos basta probar que la suma real por filas y columnas es 1.

Luego, si tomamos c_{ij} con la sumatoria real y calculamos el valor de la sumatoria real de la i-ésima fila de C :

$$\sum_{j=1}^{n} c_{ij} = \sum_{j=1}^{n}\sum_{k=1}^{n} a_{ik}b_{kj} = \sum_{k=1}^{n} a_{ik}\sum_{j=1}^{n} b_{kj},$$

como $B \in MP_n(\{0,1\}) \Longrightarrow \sum_{j=1}^{n} b_{kj} = 1, \Longrightarrow \sum_{j=1}^{n} c_{ij} = \sum_{k=1}^{n} a_{ik} = 1,$

pues $A \in MP_n(\{0,1\})$.

De manera análoga, tomando la suma real de la j-ésima columna de C :

$$\sum_{i=1}^{n} c_{ij} = \sum_{i=1}^{n}\sum_{k=1}^{n} a_{ik}b_{kj} = \sum_{k=1}^{n} b_{kj}\sum_{i=1}^{n} a_{ik} = 1,$$

luego, $C \in MP_n(\{0,1\})$, concluyendo que la multiplicación de matrices es cerrada en $MP_n(\{0,1\})$ ■

Veamos la existencia de inversos. Sea $A \in MP_n(\{0,1\})$ y supongamos que:

$$a_{1i_1} = 1, a_{2i_2} = 1, ..., a_{ni_n} = 1, \quad i_k \neq i_j, \quad \forall j \neq k,$$

es decir, los n 1's se encuentran en esas posiciones. Por ejemplo, si

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \text{ se tiene } : i_1 = 1, \quad i_2 = 3, \quad i_3 = 4, \quad i_4 = 2.$$

Volviendo al caso general, tomemos la matriz $B \in MP_n(\{0,1\})$ tal que:

$$b_{i_1 1} = 1, \quad b_{i_2 2} = 1, \cdots, b_{i_n n} = 1,$$

o, de manera equivalente, $B = {}^tA$ (la matriz traspuesta de A, definida en capítulo III). En el ejemplo $b_{11} = b_{32} = b_{43} = b_{24} = 1$

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \text{ luego } C = A \cdot B = A^tA = I.$$

En general, si $C = A \cdot B$:

$$c_{11} = \sum_{k=1}^{n} a_{1k}b_{k1} = \cdots + a_{1i_1}b_{i_1 1} + \cdots = 1$$

$$c_{22} = \sum_{k=1}^{n} a_{2k}b_{k2} = \cdots + a_{2i_2}b_{i_2 2} + \cdots = 1$$

$$\vdots$$

$$c_{nn} = \sum_{k=1}^{n} a_{nk}b_{kn} = \cdots + a_{ni_n}b_{i_n n} + \cdots = 1$$

y $c_{ij} = 0 \quad \forall i \neq j$, de donde $C = I$ ■

Hemos probado entonces que:

$$(MP_n(\{0,1\}), \cdot) \textit{ es un grupo.} \tag{5.55}$$

Verifiquemos ahora que

$$(MP_n(\{0,1\}), \cdot) \textit{ es isomorfo a } (S_n, \circ). \tag{5.56}$$

Para ello consideremos la aplicación:

$$\begin{aligned}\varphi : S_n &\longrightarrow MP_n(\{0,1\})\\ p &\longrightarrow \varphi(p) = M = (m_{ij})\end{aligned}$$

tal que:

$$\begin{aligned} m_{p(s),s} &= 1 \qquad \forall s \in \{1, \cdots, n\}\\ m_{ij} &= 0 \qquad \text{en otro caso.}\end{aligned}$$

Por ejemplo, dadas las permutaciones

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad q = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$$

sus imágenes son:

$$\varphi(p) = A = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}; \quad \varphi(q) = B = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Demostremos que, en el caso general, φ es un isomorfismo. Veamos primero que φ es una biyección:

<u>φ es inyectiva</u>: Si $\varphi(p) = \varphi(q) \Longleftrightarrow$ los 1's de ambas matrices están en las mismas posiciones, digamos $(i_1, 1), (i_2, 2), ..., (i_n, n)$. De la definición de φ se concluye que:

$$p = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} = q.$$

<u>φ es epiyectiva</u>. Sea $M \in MP_n(\{0,1\})$. Supongamos que los 1's de M están en las posiciones $(i_1, 1), ..., (i_n, n)$. Le asociamos como pre-imagen la permutación:

$$p = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}.$$

Directamente de la definición de φ se tiene $\varphi(p) = M$.
Hemos demostrado entonces que φ es una biyección ■

<u>φ es un homomorfismo.</u> Debemos probar que

$$\varphi(p \circ q) = \varphi(p) \cdot \varphi(q). \tag{5.57}$$

Sea $C = \varphi(p \circ q), A = \varphi(p), \; B = \varphi(q), \; D = A \cdot B$. Demostrar (5.57) es equivalente a probar $C = D$.
Calculemos los elementos de $C = (c_{ij})$. Se tiene que:

$$p \circ q = \begin{pmatrix} 1 & 2 & & n \\ p(1) & p(2) & \cdots & p(n) \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & \cdots & n \\ q(1) & q(2) & \cdots & q(n) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & \cdots & n \\ p(q(1)) & p(q(2)) & \cdots & p(q(n)) \end{pmatrix}.$$

Luego, C verifica:

$$\begin{aligned} c_{p(q(s)),s} &= 1 \qquad \forall s \in \{1, \cdots, n\}\\ c_{ij} &= 0 \qquad \text{en otro caso .}\end{aligned}$$

Estudiemos ahora $A \cdot B = D = (d_{ij})$: calculando la fila i-ésima

$$\underset{A}{\begin{pmatrix} & & & \ell & & & \\ & & & 0 & & & \\ & & & \vdots & & & \\ & & & 0 & & & \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ & & & 0 & & & \\ & & & \vdots & & & \\ & & & 0 & & & \end{pmatrix}}_{i} \underset{B}{\begin{pmatrix} & & & s & & & \\ & & & 0 & & & \\ & & & \vdots & & & \\ & & & 0 & & & \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ & & & 0 & & & \\ & & & \vdots & & & \\ & & & 0 & & & \end{pmatrix}}_{\ell} = D$$

$$\text{Luego: } \begin{cases} d_{i1} = d_{i2} = \cdots = d_{is-1} = 0 \\ d_{is} = 1 \\ d_{is+1} = d_{is+2} = \cdots = d_{in} = 0 \end{cases}$$

Pero, de la definición de φ:

$$a_{i\ell} = 1 \Longleftrightarrow p(\ell) = i$$

$$b_{\ell s} = 1 \Longleftrightarrow q(s) = \ell.$$

Luego $d_{is} = 1 \Longleftrightarrow d_{p(\ell)s} = 1 \Longleftrightarrow d_{p(q(s))s} = 1$. De donde se concluye:

$d_{p(q(s)),s} = 1 \quad \forall s \in \{1, ..., n\}$ y 0 en otro caso.

Por otra parte, sabemos que C es tal que $c_{p(q(s)),s} = 1 \quad \forall s \in \{1, \cdots, n\}$ y 0 en otro caso, de donde $D = C$ y en consecuencia φ es un isomorfismo, concluyendo $(S_n, \circ) \cong (MP_n(\{0,1\}, \cdot)$ ■

Verifiquemos el homomorfismo para las permutaciones p, q del ejemplo anterior:

$$\varphi(p) \cdot \varphi(q) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\varphi(p \circ q) = \varphi \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \varphi(p) \cdot \varphi(q).$$

Como moraleja, podemos decir que las matrices, como ya lo habíamos intuído en capítulos anteriores, son sumamente útiles. En este caso concreto, se deduce directamente del isomorfismo anterior y el teorema de Cayley, que:

Cualquier grupo finito es isomorfo a un subgrupo del grupo de matrices de permutación. (5.58)

5.8.5 Teorema de Lagrange.

Este teorema, de hermosa demostración y gran utilidad, dice lo siguiente:

Dado un grupo $(\mathcal{G}, *)$ *finito, el orden de un subgrupo arbitrario,* $(\mathcal{H}, *)$ *divide el orden de* $(\mathcal{G}, *)$. (5.59)

Para demostrarlo necesitamos algunas definiciones y resultados previos. Consideremos entonces un grupo finito $(\mathcal{G}, *)$ y un subgrupo $(\mathcal{H}, *)$. Dado $g \in \mathcal{G}$, definimos como el *factor izquierdo* de $\mathcal{H}$ al conjunto

$$g * \mathcal{H} = \{g * h / h \in \mathcal{H}\}. \tag{5.60}$$

Por ejemplo, si consideramos al subgrupo:

$$\mathcal{H} = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \right\}$$

de las matrices de permutación, $MP_3(\{0,1\})$, y el elemento

$$P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \in MP_3(\{0,1\}).$$

obtenemos el factor izquierdo

$$P * \mathcal{H} = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \right\}$$

Vemos, del ejemplo, que no necesariamente $g * \mathcal{H}$ es un subgrupo de $\mathcal{G}$.

Definamos la relación

$$(\forall g_1, g_2 \in \mathcal{G})\ (g_1 \sim g_2 \iff g_1^{-1} * g_2 \in \mathcal{H}). \tag{5.61}$$

Es directo que $\sim$ es relación de equivalencia

Refleja: $g \sim g$, pues $g^{-1} * g = e \in \mathcal{H}$.

Simétrica: $g_1 \sim g_2 \iff g_1^{-1} * g_2 \in \mathcal{H}$, como $\mathcal{H}$ es subgrupo, $\iff (g_1^{-1} * g_2)^{-1} \in \mathcal{H} \iff g_2^{-1} * g_1 \in \mathcal{H} \iff g_2 \sim g_1$.

Transitiva: $g_1 \sim g_2 \wedge g_2 \sim g_3 \iff g_1^{-1} * g_2 \in \mathcal{H} \wedge g_2^{-1} * g_3 \in \mathcal{H}$. Como $\mathcal{H}$ es subgrupo, $g_1^{-1} * g_2 * g_2^{-1} * g_3 \in \mathcal{H} \iff g_1^{-1} * g_3 \in \mathcal{H} \iff g_1 \sim g_3$ ■

Consideremos la clase de equivalencia asociada a g,

$$[g] = \{b \in \mathcal{G} / g \sim b\} = \{b \in \mathcal{G} / g^{-1} * b \in \mathcal{H}\},$$

se tiene entonces:

$$[g] = g * \mathcal{H}. \tag{5.62}$$

En efecto, $b \in g * \mathcal{H} \iff b = g * h, h \in \mathcal{H} \iff g^{-1} * b = h \in \mathcal{H} \iff b \in [g]$ ■

Consideremos el conjunto cociente $\mathcal{G}/\sim$. Como $\mathcal{G}$ es finito, existe un número finito de clases distintas,

$$G/\sim = \{g_1 * \mathcal{H}, ..., g_r * \mathcal{H}\}.$$

Este número, r, se denomina el *índice* del subgrupo $\mathcal{H}$ y se denota Ind$\mathcal{H}$.

Por otra parte, la aplicación $\varphi : \mathcal{H} \to g * \mathcal{H}$, $\varphi(h) = g * h$ es biyectiva.

En efecto, $\varphi(h_1) = \varphi(h_2) \iff g * h_1 = g * h_2 \iff h_1 = h_2$. Además, dado $u \in g * \mathcal{H}$, $u = g * h$, $h \in \mathcal{H}$, luego $\varphi(h) = u$ ■

Como $\mathcal{G}$ es finito, concluímos que:

$$|\mathcal{H}| = |g * \mathcal{H}|.$$

Pero $\mathcal{G} = \bigcup_{i=1}^{r} g_i * \mathcal{H} \Rightarrow |\mathcal{G}| = \sum_{i=1}^{r} |g_i * \mathcal{H}| = |\mathcal{H}| \cdot Ind\mathcal{H}$

$$|\mathcal{G}| = |\mathcal{H}| \cdot Ind\mathcal{H}. \tag{5.63}$$

Luego, el orden y el índice del subgrupo $\mathcal{H}$ dividen el orden de $\mathcal{G}$, lo cual prueba el teorema de Lagrange ■

Un corolario directo es el siguiente:

Cualquier grupo $(\mathcal{G}, *)$de orden primo, no posee subgrupos distintos de los triviales: $(\{e\}, *)$ y $(\mathcal{G}, *)$. (5.64)

Señalemos que el teorema de Lagrange nos da una condición necesaria que debe satisfacer un subgrupo de $(\mathcal{G}, *)$, pero no nos asegura que si q divide $|\mathcal{G}|$ entonces existe un subgrupo de orden q. Para ver en qué casos se tiene esto último deberíamos ir bastante más lejos en la teoría.

5.8.6 Grupos cíclicos.

Consideremos la matriz

$$M = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} \in MP_4(\{0,1\}) \qquad G(M): \begin{array}{ccc} 1 & \to & 2 \\ \uparrow & & \downarrow \\ 4 & \leftarrow & 3 \end{array}$$

y calculemos sus potencias sucesivas (de acuerdo al resultado del Tema 3 del Capítulo III se puede hacer directamente examinando el grafo $G(M)$)

$$M^2 = M \cdot M = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

$$M^3 = M^2 \cdot M = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}; \quad M^4 = M^3 \cdot M = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = I$$

$$M^5 = M \cdot I = M, M^6 = M^5 \cdot M = M^2, \ldots$$

obteniendo el conjunto

$$< M >= \{M^p / p \geq 0\} = \{M^0 = I, M, M^2, M^3\}.$$

Es directo que el resultado de la multiplicación de dos de estas matrices está en $< M >$, existe elemento neutro I, la multiplicación es asociativa y cada elemento posee inverso:

$$I^{-1} = I, \quad M^{-1} = M^3, \quad (M^2)^{-1} = M^2.$$

Luego, $(< M >, \cdot)$ es grupo y todos sus elementos están generados por las potencias de M.

Observamos que a partir del entero $m = 4$, los elementos de este grupo comienzan a repetirse indefinidamente, según el diagrama:

$$\begin{array}{ccc} I & \to & M \\ \uparrow & & \downarrow \\ M^3 & \leftarrow & M^2 \end{array}$$

donde "$\to$" $\iff$"multiplicar por M".

Tal como en el caso de potencias de matrices, dado un grupo $(\mathcal{G}, *)$, definimos, $\forall x \in \mathcal{G}$:

$$x^\circ = e, \text{ elemento neutro}$$

$$x^n = x \cdot x^{n-1} = x * \cdots * x, \quad n \text{ veces}, \quad n \geq 1. \tag{5.65}$$

Además:

$$(x^{-1})^n = x^{-1} * \cdots * x^{-1}$$
$$n \text{ veces.}$$

También es fácil verificar por inducción que

$$x^{-m} = (x^{-1})^m. \tag{5.66}$$

Diremos que $(\mathcal{G}, *)$ es un *grupo cíclico* si es grupo y verifica:

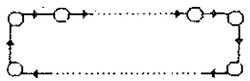
$$(\exists a \in \mathcal{G})\ (\forall x \in \mathcal{G})\ (\exists n \in \mathbb{Z})(x = a^n) \tag{5.67}$$

Este elemento $a \in \mathcal{G}$ se denomina *generador* del grupo.

Ejemplos:

1) El grupo anterior $(< M >, \cdot)$.

2) El grupo de permutaciones generado por la composición reiterada de una permutación *circular*, p, donde p es circular si y sólo si el grafo asociado a la permutación es un circuito único:



Por ejemplo,

$$PC(4)=\left\{\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}\right\}$$

Donde la permutación $p = \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$. verifica:

$$p^2 = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}, \quad p^3 = \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}, \quad p^4 = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$$

3) $(\mathbb{Z}, +)$; en este grupo es más adecuado usar la notación aditiva:

$$0a = 0 \qquad \text{elemento neutro de } \mathbb{Z} \tag{5.68}$$

$$na = a + (n-1)a = a + \cdots + a, \quad n \text{ veces.} \tag{5.69}$$

Si $n < 0$: $\quad na = |n|(-a)$ donde $-a$ es el inverso de a.

Con esta notación,

$$(\forall x \in \mathbb{Z})(\exists m \in \mathbb{Z})(x = m \cdot 1).$$

Por ejemplo, si $x = 4$:

$$4 = 4 \cdot 1 = 1 + 1 + 1 + 1.$$

Si $x = -5$

$$-5 = (-5)1 = 5(-1) = (-1) + (-1) + (-1) + (-1) + (-1).$$

Es decir, $(\mathbb{Z}, +)$ es grupo cíclico generado por $1 \in \mathbb{Z}$.

4) $(\mathbb{Z}_n, \oplus)$ es cíclico generado por $[1]$:

$$k[1] = [1] + \cdots + [1] = [k] \qquad 0 \leq k \leq n-1.$$

5) El grupo de las rotaciones del cuadrado es cíclico.

6) No son cíclicos el grupo de Klein, K_4, y el grupo de permutaciones $(S_n, \circ), n \geq 3$. En el caso de K_4, basta examinar su tabla de Pitágoras:

$*$	a_0	a_1	a_2	a_3
a_0	a_0	a_1	a_2	a_3
a_1	a_1	a_0	a_3	a_2
a_2	a_2	a_3	a_0	a_1
a_3	a_3	a_2	a_1	a_0

$$a_1, \quad a_1^2 = a_0, \quad a_1^3 = a_1^2 \cdot a_1 = a_0 * a_1 = a_1, \cdots$$
$$a_2, \quad a_2^2 = a_0, \quad a_2^3 = a_2$$
$$a_3, \quad a_3^2 = a_0, \quad a_3^3 = a_3.$$

Ningún elemento, mediante el cálculo de sus potencias, engendra todo K_4. Luego, éste no es cíclico.

En el caso de las permutaciones es claro que, mediante una inspección similar, $(S_3, \circ)$ no es cíclico (ver su tabla en capítulo IV).

Dado un grupo $(\mathcal{G}, *)$, $\quad \forall x \in \mathcal{G}$ definimos

$$< x >= \{x^p / p \in \mathbb{Z}\}. \tag{5.70}$$

Es fácil ver que $(< x >, *)$ es un subgrupo de $(\mathcal{G}, *)$.

En efecto, sean $a, b \in < x > \Longleftrightarrow \exists m, n \in$ tales que $a = x^n$, $b = x^m$, luego

$$\begin{aligned} a * b^{-1} &= x^n * (x^m)^{-1} \\ &= x^n * (x^{-1} * x^{-1} * \cdots * x^{-1}) \\ &\qquad\qquad m \text{ veces} \\ &= (x * x * \cdots * x) * (x^{-1} * \cdots * x^{-1}) \\ &\qquad \leftarrow n \rightarrow \qquad\quad \leftarrow m \rightarrow \\ &= x^{n-m} \in < x >, \text{ tomando } p = n - m \in \mathbb{Z} \quad \blacksquare \end{aligned}$$

Luego, $\forall x \in \mathcal{G}$, $(< x >, *)$ es siempre un subgrupo cíclico de $(\mathcal{G}, *)$ que denominaremos el *subgrupo cíclico generado por* x.

De lo anterior es directa la equivalencia:

$$(\mathcal{G}, *) \text{ es grupo cíclico } \Longleftrightarrow (\exists a \in \mathcal{G})(< a >= \mathcal{G}). \tag{5.71}$$

Una propiedad importante es que

$$\textit{todo grupo cíclico } (\mathcal{G}, *) \textit{es abeliano}. \tag{5.72}$$

En efecto, sean $x, y \in \mathcal{G}$;
Luego, $\exists a \in \mathcal{G}$, $n, m \in \mathbb{Z}$ tales que $x = a^n$, $y = b^m$:

$$x * y = a^n * b^m = \underbrace{a * \cdots * a}_{\leftarrow n \rightarrow} * \underbrace{(a * \cdots * a)}_{\leftarrow m \rightarrow}$$

$$= a^{n+m} = a^{m+n} = a^m * a^n = y * x \quad \blacksquare$$

De esta propiedad es trivial concluir que $(S_n, \circ)$ no es cíclico para $n \geq 3$, ya que para $n \geq 3$, S_n no es abeliano (justifique). Se concluye también que un grupo de orden ≥ 6 no es necesariamente abeliano y por lo tanto, tampoco cíclico.

Finalmente,

$$\textit{cualquier grupo finito } \mathcal{G} \textit{ de orden primo es cíclico.} \tag{5.73}$$

En efecto, sea $g \in \mathcal{G}$, $g \neq e$, y tomemos el subgrupo cíclico de $\mathcal{G}$ generado por g, $< g >$. Como $< g >$ es subgrupo de $\mathcal{G}$, por el teorema de Lagrange $| < g > |$ divide $|\mathcal{G}|$. Como $|\mathcal{G}|$ es primo y $| < g > | \geq 2$ se tiene necesariamente que $| < g > | = |\mathcal{G}|$, es decir, $< g >= \mathcal{G}$ $\blacksquare$

Se tiene entonces que los grupos de orden 5 son cíclicos, luego abelianos. De esto concluímos que cualquier grupo no-abeliano debe tener al menos seis elementos. También es directo de (5.73) que cualquier elemento de un grupo cíclico, $g \in \mathcal{G} \setminus \{e\}$, es generador.

5.9 Anillos.

Sin pérdida de generalidad, notaremos las dos operaciones involucradas en las estructuras algebraicas que siguen como "+" (notación aditiva) y como "·" (notación multiplicativa).

Diremos que $(\mathcal{A}, +, \cdot)$ es un *anillo* si y sólo si

$(\mathcal{A}, +)$ es un grupo abeliano,

$\cdot$ es asociativa (5.74)

$\cdot$ distribuye con respecto a $+$.

El anillo se dice *conmutativo* si la multiplicación es conmutativa. Este se dira con *unidad* si admite elemento neutro para $\cdot$

Algunos ejemplos de anillos son los siguientes:

1. $(\mathbb{R}, +, \cdot)$ es un anillo conmutativo con unidad.

2. Sea $X = \{a + b\sqrt{3}/a, b \in \mathbb{Z}\}$, con la suma y la multiplicación usual en $\mathbb{R}$. En estas condiciones $(X, +, \cdot)$ es un anillo. En efecto

   $(X, +)$ es grupo abeliano:

   i) $+$ es cerrada en X :

   $$(a + b\sqrt{4}) + (c + d\sqrt{3}) = (a + c) + (b + d)\sqrt{3} \in A.$$

   ii) $+$ es conmutativa y asociativa por herencia de la suma en $\mathbb{R}$.

   iii) El neutro es $0 = 0 + 0\sqrt{3} \in X$.

   iv) El inverso aditivo de $a + b\sqrt{3}$ es $-a + (-b)\sqrt{3}$.

   - La asociatividad de la multiplicación es heredada de $\mathbb{R}$.

   - la Distributividad de $\cdot$ con respecto a $+$ se obtiene directamente de la distributividad de estas operaciones en $\mathbb{R}$ $\blacksquare$

3. Sea X un conjunto no vacío arbitrario y $\mathcal{P}(X)$ el conjunto de las partes. $(\mathcal{P}(X), \cup, \cap)$ no es anillo, ya que $(\mathcal{P}(X), \cup)$ no es grupo (verifique).

4. $(\mathcal{P}(X), \Delta, \cap)$ es un anillo, donde Δ es la diferencia simétrica: $A \Delta B = (A \setminus B) \cup (B \setminus A)$. En efecto

- $(\mathcal{P}(X), \Delta)$ es grupo abeliano:

  El neutro es $\phi : A\Delta\phi = (A \setminus \phi) \cup (\phi \setminus A) = A \cup \phi = A$. El inverso de A es $A : A\Delta A = (A \setminus A) \cup (A \setminus A) = \phi \cup \phi = \phi$.

- Δ es conmutativa.

- $\cap$ distribuye con respecto a Δ

  Para demostrar esta última propiedad, basta aplicar la identidad: $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$. En efecto,

$$\begin{aligned} A \cap (B \Delta C) &= A \cap ((B \setminus C) \cup (C \setminus B)) \\ &= (A \cap (B \setminus C)) \cup (A \cap (C \setminus B)) \\ &= ((A \cap B) \setminus (A \cap C)) \cup ((A \cap C) \setminus (A \cap B)) \\ &= (A \cap B) \Delta (A \cap C). \end{aligned}$$

  Además, como $\cap$ es conmutativa y X es neutro para $\cap$, se tiene que es un anillo conmutativo con unidad ■

5. La estructura de congruencias $(\mathbb{Z}_p, \oplus, \cdot)$ es un anillo conmutativo con unidad. En efecto,
   - sabemos que $(\mathbb{Z}_p, \oplus)$ es un grupo abeliano.
   - $\cdot$ es asociativa:

$$\begin{aligned} [a] \cdot ([b] \cdot [c]) &= [a] \cdot ([bc]) = [a(bc)] \\ &= [(ab)c] = [ab] \cdot [c] = ([a] \cdot [b]) \cdot [c]. \end{aligned}$$

   - $\cdot$ distribuye con respecto a $\oplus$:

$$\begin{aligned} [a] \cdot ([b] \oplus [c]) &= [a] \cdot [b + c] \\ &= [a(b + c)] = [ab + ac] = [ab] \oplus [ac] \\ &= [a] \cdot [b] \oplus [a] \cdot [c]. \end{aligned}$$

   Como la multiplicación, es conmutativa y $[1]$ es neutro para $\cdot$, concluímos que es un anillo conmutativo con unidad ■

5.9.1 Propiedades elementales de un anillo.

Sea $(\mathcal{A}, +, \cdot)$ un anillo. Se verifica:

$$\forall a \in \mathcal{A}, \quad a0 = 0a = 0, 0 \text{ es el neutro aditivo.} \tag{5.75}$$

$$\forall a, b \in A, \quad -(ab) = a(-b) = (-a)b. \tag{5.76}$$

Además,

$$\forall a, b, c \in A, \quad \begin{aligned} &(-a)(-b) = ab \\ &a(b - c) = ab - ac \\ &(b - c)a = ba - ca. \end{aligned} \tag{5.77}$$

Demostración:

(5.75) $a0 + a0 = a(0 + 0)$ (distributividad). Pero 0 es el neutro aditivo $(0 + 0 = 0)$, luego, $a0 + a0 = a0$, lo cual es equivalente a:

$$a0 + a0 = a0 + 0.$$

Cancelando

$$a0 = 0.$$

De manera análoga se obtiene $0a = 0$.

(5.76) Sabemos que:

$$b + (-b) = 0,$$

luego,

$$\begin{aligned} a(b + (-b)) = a0 = 0 \\ ab + a(-b) = 0. \end{aligned}$$

Como el inverso aditivo en un grupo es único:

$$-(ab) = a(-b).$$

De manera análoga se demuestra

$$(-a)b = -(ab).$$

Además, de las dos propiedades anteriores se deduce

$$(-a)(-b) = -((-a)b) = -(-(ab));$$

como el inverso aditivo de $-ab$ es ab y es único se concluye:

$$-(-(ab)) = ab.$$

Luego,

$$(-a)(-b) = ab.$$

La propiedad (5.77) queda como ejercicio ■

Una propiedad importante en las estructuras algebraicas con dos operaciones es la noción de "divisor del cero".

Diremos que un anillo $(\mathcal{A}, +, \cdot)$ admite *divisores de cero* si y sólo si:

$$(\exists a, b \in \mathcal{A} \setminus \{0\})(ab = 0). \tag{5.78}$$

En los ejemplos anteriores

$(\mathcal{P}(X), \Delta, \cap)$ tiene divisores del cero :

$$A \cap C_X(A) = \phi \qquad \forall A \in \mathcal{P}(X).$$

Luego, todos los conjuntos propios y no vacíos de X:

$$(A \neq \phi) \wedge (C_X(A) \neq \phi)$$

son divisores de cero.

$(\mathbb{Z}_p, \oplus, \cdot)$ puede tener divisores de cero. Tomemos por ejemplo $p = 4$. La tabla de multiplicación es:

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

se tiene que $[2] \neq [0]$ y $[2] \cdot [2] = [0]$, ergo $[2]$ es divisor de cero.

Para $p = 3$ la tabla de la multiplicación es:

$\cdot$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$
$[2]$	$[0]$	$[2]$	$[1]$

la cual no admite divisores de cero. Aparentemente, $(\mathbb{Z}_p, \oplus, \cdot)$ tiene o no divisores de cero según el valor de p. Esto lo precisaremos más adelante.

El ejemplo más corriente de anillo sin divisores de cero es $(\mathbb{R}, +, \cdot)$, pues sabemos que

$$ab = 0 \Longrightarrow (a = 0) \vee (b = 0).$$

El hecho de que una estructura no posea divisores de cero es importante. Esta propiedad la poseen las estructuras algebraicas que estudiaremos a continuación.

5.10 Cuerpos.

Recordemos que $(\mathcal{K}, +, \cdot)$ es *cuerpo* si y sólo si:

$(\mathcal{K}, +, \cdot)$ es un anillo. (5.79)
$(\mathcal{K} \setminus \{0\}, \cdot)$ es grupo abeliano.

Ejemplos:

1. $(\mathbb{R}, +, \cdot)$ es un cuerpo.

2. Dado el conjunto $X = \{a + b\sqrt{3}/a, b \in \mathbb{Z}\}$,$(X, +, \cdot)$ no es cuerpo, ya que el inverso multiplicativo de $a + b\sqrt{3} \in A \setminus \{0 + 0\sqrt{3}\}$, es

$$\frac{1}{a + b\sqrt{3}} = \frac{a - b\sqrt{3}}{(a + b\sqrt{3})(a - b\sqrt{3})} = \frac{a - b\sqrt{3}}{a^2 - 3b^2}$$
$$= \frac{a}{a^2 - 3b^2} - \frac{b}{a^2 - 3b^2}\sqrt{3}$$

   y los elementos $\frac{a}{a^2-3b^2}; \frac{-b}{a^2-3b^2}$ no pertenecen necesariamente a $\mathbb{Z}$. Tomando Q en lugar de $\mathbb{Z}$ y el conjunto $B = \{a + b\sqrt{3}/a, b \in Q\}$, se tiene que $(B, +, \cdot)$ es cuerpo (verifique).

3. $(\mathbb{Z}_4, \oplus, \cdot)$ no es cuerpo pues $(\mathbb{Z}_4 \setminus \{[0]\}, \cdot)$ no es grupo (en la tabla de Pitágoras existen elementos repetidos por filas y columnas). Ni siquiera es estructura, pues $2 \cdot 2 = 0$, elemento que no pertenece el conjunto donde se define la operación. Sin embargo $(\mathbb{Z}_3, \oplus, \cdot)$ es cuerpo.

Una propiedad muy importante es que

un cuerpo no tiene divisores de cero. (5.80)

Demostración: Supongamos $ab = 0$, $a, b \in A$. Si $a = 0$ está demostrado, luego supongamos $a \neq 0$. Debemos demostrar que $b = 0$; como $a \neq 0$, a admite un inverso multiplicativo a^{-1}, de donde

$$\begin{aligned} ab = 0 &\Longleftrightarrow a^{-1}(ab) = a^{-1}0 = 0 \\ &\Longleftrightarrow (a^{-1}a)b = 0 \\ &\Longleftrightarrow 1b = 0 \Longleftrightarrow b = 0 \quad \blacksquare \end{aligned}$$

En las clases de congruencia módulo p, hemos visto que, dependiendo de p, $(\mathbb{Z}_p, \oplus, \cdot)$ es o no un cuerpo. Se tiene el resultado siguiente:

$$(\mathbb{Z}_p, \oplus, \cdot) \textit{ es cuerpo} \Longleftrightarrow p \textit{ es un número primo} . \qquad (5.81)$$

Demostración:

$\Longrightarrow$) Si p no es primo, existen $a, b \in \mathbb{Z}$ tales que $p = ab$,$0 < a < p$, $0 < b < p$, luego:

$$[a] \cdot [b] = [ab] = [p] = [0]$$

con $[a] \neq 0$ y $[b] \neq 0$, es decir $(\mathbb{Z}_p, \oplus, \cdot)$ posee $[a], [b]$ como divisores de cero, lo cual es una contradicción ya que un cuerpo no tiene divisores de cero, luego p es primo.

$\Longleftarrow$) si p es un número primo, basta probar que cualquier elemento $[a] \neq [0]$ tiene un inverso multiplicativo:
Como $[a] \neq [0] \Longrightarrow 0 < a < p$. Como p es primo $mcd(a, p) = 1$ y del Capítulo 3, $\exists r, s \in \mathbb{Z}$ tales que:

$$ar + ps = 1,$$

de donde

$$[a] \cdot [r] = [ar] + [0] = [ar] + [ps] \quad (\text{ pues } [0] = [ps]);$$

luego,

$$[a] \cdot [r] = [ar + ps] = [1],$$

concluyendo

$$[a]^{-1} = [r] \quad \blacksquare$$

A modo de ejemplo, resolvamos, en el cuerpo $(\mathbb{Z}_5, \oplus, \cdot)$, la ecuación en x:

$$[2]x^2 \oplus [3]x \oplus [1] = [0].$$

De las tablas de $(\mathbb{Z}_5, \oplus)$ y $(\mathbb{Z}_5, \cdot)$ se observa que la ecuación es equivalente a

$$(x \oplus [1]) \cdot ([2]x \oplus [1]) = [0].$$

Como $(\mathbb{Z}_5, \oplus, \cdot)$ es cuerpo, no posee divisores de cero; luego,
$x \oplus [1] = [0]$, $[2]x \oplus [1] = 0$, lo cual implica las soluciones [4] y [2].

Ejercicios.

1. Estudie las estructuras:
   (a) $(\mathbb{R}^2, *)$; $(a,b)*(c,d) = (a+c, b+d+2bd)$.
   (b) Sea $S = \{a+b\sqrt{2}/a,b \in \mathbb{R}\}$, se definen $\forall x,y \in S$
   $x*y = (a+b\sqrt{2})\cdot(c+d\sqrt{2})$
   $x\Delta y = (a+b\sqrt{2})+(c+d\sqrt{2})$.
   (c) $(\mathbb{N}, *)$, $a*b = \max(a,b)$.
   (d) $(\mathbb{N}, *)$, $a*b = \max(a,b) - \min(a,b)$.
   (e) Sea $S = \{1,2,3,4,6\}$, estudie $(S,*)$: $a*b = mcd(a,b)$.
   (f) Sea $S = \{1,2,5,10\}$ y consideremos
   $(S,+,\bullet) : a+b = mcd(a,b), a\bullet b = mcm(a,b)$, donde $mcm(a,b) =$ mínimo común múltiplo entre a y b, está definido como sigue: $mcm(a,b) = k$ si y sólo si $(a|k \wedge b|k) \wedge (a|k' \wedge b|k' \Longrightarrow k|k')$.
   (g) $(\mathcal{P}(X), \cup, \cap), X \neq \phi$.
   (h) $\mathcal{P}(X), \Delta, \cap), X \neq \phi$, donde Δ es la diferencia simétrica.
2. Dados $\mathbb{Z}_2, \mathbb{Z}_3$ se define la operación $*$ en $\mathbb{Z}_2 \times \mathbb{Z}_3$ dada por:
   (a) $(a,b)*(c,d) = (a\cdot_2 c, b\oplus_3 d)$. Estudie las propiedades de $*$
   (b) En $\mathbb{R}^3$ se define $\times$ por:

$$(x_1,x_2,x_3)\times(y_1,y_2,y_3) = (x_2y_3 - x_3y_2, x_3y_1 - x_1y_3, x_1y_2 - x_2y_1).$$

   Estudie las propiedades de $\times$.
3. Sea $E \neq \phi$. Sobre E se definen dos operaciones: $*$ y $\cdot$, con elementos neutros e y f respectivamente, y que cumplen $\forall x,y,u,v \in E$, $(x*y)\cdot(u*v) = (x\cdot u)*(y\cdot v)$. Demuestre que:
   (a) $e = f$
   (b) $\forall (x,v) \in E\times E \quad x*v = x\cdot v$
   (c) $*$ es asociativa y conmutativa.
4. Sea $\mathcal{F} = \{f/f$ es función de $\mathbb{N}$ en $\mathbb{R}\}$. Se define en $\mathcal{F}$ la *l.c.i.* $*$:

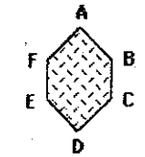
$$(f*g)(n) = \sum_{j=0}^{n} f(j)g(n-j) \quad \forall n \in \mathbb{N}.$$

   (a) Para las funciones f y g dadas por $f(n) = n, g(n) = 1 \quad \forall n \in \mathbb{N}$, demuestre que:
   (a.1) $(g*g)(n) = n+1$
   (a.2) $(f*g)(n) = n(n+1)$
   (a.3) $(f*f)(n) = \frac{n(n+1)(n-1)}{6}$
   (b) Demuestre que $*$
   (b.1) es conmutativa,
   (b.2) posee elemento neutro (encuéntrelo),

   (b.3) distribuye con respecto a $+$, en que $(f+g)(n) = f(n)+g(n)$.
5. Sea $\mathcal{G} = \{a \in \mathbb{R}/a \in]-1,+1[\ \}$ y sea $a*b = \frac{a+b}{1+ab}$, $a,b \in \mathcal{G}$. Demuestre que $(\mathcal{G},*)$ es grupo abeliano.
6. Pruebe que $(\mathcal{G},*)$ es un grupo abeliano si y sólo si $\varphi : \mathcal{G} \to \mathcal{G}, g \to g*g$, es un homorfismo.
7. Sea $X \neq \phi$ y el anillo $(\mathcal{P}(X), \Delta, \cap)$. Para un conjunto $S \in \mathcal{P}(X)$ sea la función: $f : \mathcal{P}(X) \to \mathcal{P}(X), A \to f(A) = A \cap S$. Demuestre que f es un homorfismo.
8. Sean $L_1 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\}$
   $L_2 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$, cada uno de ellos con la multiplicación de matrices (entendiendo la multiplicación real de cada elemento):

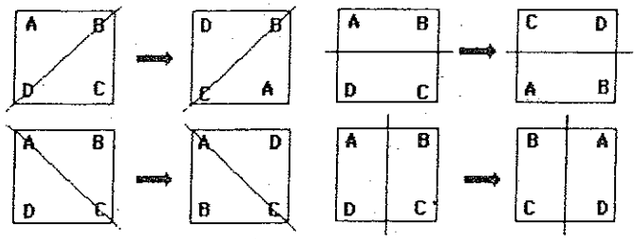
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix}$$

   donde $+$ es la suma usual en $\mathbb{R}$.
   (a) Demuestre que ambos son grupos conmutativos.
   (b) Establezca cuál es isomorfo al grupo de Klein y cuál al de las rotaciones de un cuadrado.
9. Sea $(\mathcal{G},*)$ un grupo. Estudie del punto de vista de morfismo, las aplicaciones:
   (a) $\varphi : \mathcal{G} \to \mathcal{G}, \quad x \to a*x$
   (b) $\varphi : \mathcal{G} \to \mathcal{G}, \quad x \to a^{-1}*x*a$ ¿Qué sucede si $\mathcal{G}$ es abeliano?
10. Sea $(\mathcal{G},\bullet)$ grupo tal que: $\forall a,b \in \mathcal{G}$ se verifica $(a\bullet b)^2 = a^2 \bullet b^2$
    (a) demuestre que $\mathcal{G}$ es abeliano.
    (b) Deduzca $\forall n \geq 2\ (a\bullet b)^n = a^n \bullet b^n$.
11. Pruebe que para cualquier grupo finito $(\mathcal{G},*)$ se tiene: $\forall g \in \mathcal{G}, \exists k \in \mathbb{N}$ tal que $g^k = e$ (e es el neutro).
12. Demuestre que si $\mathcal{G}$ es un grupo finito de orden impar, necesariamente algún elemento es su propio inverso.
13. Pruebe que si en $(\mathcal{G},*)$: $(\forall g \in \mathcal{G})\ (g^2 = e)$, entonces $(\mathcal{G},*)$ es grupo abeliano.
14. Dado un polígono regular convexo de 6 lados:



estudie el grupo de rotaciones asociado. Generalice para un polígono regular de n lados.

15. Sea $\mathcal{G} = \{\varphi_{a,b} : x \to ax + b / a, b \in \mathbb{R}, a \neq 0\}$.
    (a) Demuestre que $(\mathcal{G}, \circ)$ es un grupo.
    (b) Demuestre que $\mathcal{G}^1 = \{x \to x + b / b \in \mathbb{R}\}$ es un subgrupo de $\mathcal{G}$.
16. Estudie la estructura formada por las rotaciones de un cuadrado, más las reflexiones en torno a las dos diagonales y los ejes cartesianos y determine sus subgrupos

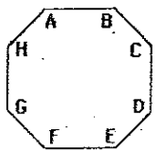


17. Sea $(\mathcal{G}, *)$ un grupo y $(\mathcal{H}, *)$ un subgrupo. Sea, además, $\mathcal{G}/\mathcal{H} = \{g * \mathcal{H} / g \in \mathcal{G}\}$ el conjunto de todos los factores izquierdos de H. En $\mathcal{G}/\mathcal{H}$ definimos la $\ell.c.i$ $\bullet$ como: $(g * \mathcal{H}) \bullet (h * \mathcal{H}) = (a * b) \bullet \mathcal{H}$. Pruebe que $(\mathcal{G}/\mathcal{H}, \bullet)$ es un grupo.
18. Sea $(\mathcal{G}, *)$ un grupo y $(\mathcal{H}, *)$ un subgrupo de $(\mathcal{G}, *)$. Pruebe que
    (a) $g \in \mathcal{H} \Rightarrow g * \mathcal{H} = \mathcal{H}$
    (b) $g * \mathcal{H} \cap h * \mathcal{H} \neq \phi \Rightarrow g * \mathcal{H} = h * \mathcal{H}$.
19. Demuestre que un subgrupo de un grupo cíclico es cíclico.
20. Pruebe que si $\mathcal{G} \cong \mathcal{E}$, ($\mathcal{G}$ isomorfo a $\mathcal{E}$), grupos, entonces $\mathcal{G}$ cíclico $\iff \mathcal{E}$ cíclico.
21. Sea la permutación

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix}$$

    Sea $\mathcal{G} = \{p^n / n \in \mathbb{N}\}$. Demuestre que $(\mathcal{G}, \circ)$ es un grupo cíclico de orden 6. Estudie los subgrupos.

* 22. Determine todos los divisores del cero de $(\mathbb{Z}_8, \oplus, \cdot)$. Demuestre que $(\mathbb{Z}_8, \oplus)$ es isomorfo al grupo de rotaciones de un octógono:



¿Es $(\mathbb{Z}_8, \oplus, \cdot) \cong (\mathbb{Z}_2 \times \mathbb{Z}_4, +, \cdot)$? donde

$$(x, y) + (x', y') = (x \oplus x', y \oplus y')$$
$$(x, y) \cdot (x', y') = (x \cdot x', y \cdot y').$$

Considere que las operaciones en la primera componente son en $\mathbb{Z}_2$ y en la segunda en $\mathbb{Z}_4$.

23. Sea $M(\mathbb{Z}_3) = \{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} / a, b \in \mathbb{Z}_3\}$. Demuestre que $M(\mathbb{Z}_3, +, \cdot)$ (con la suma y multiplicación de matrices inducidas por $\mathbb{Z}_3$) es un cuerpo con 9 elementos y $(M \setminus \{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\}, \cdot)$ es un grupo cíclico de orden 8.
24. Las siguientes tablas incompletas corresponden a las operaciones en el anillo $(\mathcal{A}, +, \cdot)$ para $\mathcal{A} = \{a, b, c, d\}$:

$+$	a	b	c	d
a	a	b	$\cdot$	d
b	$\cdot$	a	$\cdot$	$\cdot$
c	$\cdot$	$\cdot$	a	$\cdot$
d	$\cdot$	$\cdot$	$\cdot$	$\cdot$

$\cdot$	a	b	c	d
a	a	a	a	a
b	a	$\cdot$	$\cdot$	a
c	a	$\cdot$	c	$\cdot$
d	a	b	c	$\cdot$

    (a) Considerando las propiedades de anillo estudiadas, complete las tablas anteriores (justifique).
    (b) ¿Es $(\mathcal{A}, +, \cdot)$ conmutativo? ¿Posee $(\mathcal{A}, +, \cdot)$ unidad?
25. Considere en $\mathbb{Z}^2$ las $\ell.c.i$.

$$(a, b) \oplus (c, d) = (a + c, b + d)$$
$$(a, b) \odot (c, d) = (ac - bd, ad + cb).$$

Demuestre que $(\mathbb{Z}^2, \oplus, \odot)$ es un anillo conmutativo con unidad.

* 26. $(\mathcal{A}, +, \cdot)$ es un anillo booleano, si $(a \cdot a = a)(\forall a \in \mathcal{A})$. Demuestre que si $(\mathcal{A}, +, \cdot)$ es booleano:
    (a) $x = -x \ \forall x \in \mathcal{A}$ ($-x$ inverso aditivo de x)

(b) $(\mathcal{A},+,\cdot)$ es conmutativo
(c) $(x\cdot y)\cdot(x+y)=0\ \forall x,y\in\mathcal{A}$.

27. Sea $(\mathcal{A},+,\cdot)$ un anillo, definimos: $CE(A)=\{c\in\mathcal{A}/c\cdot x=x\cdot c\quad\forall x\in\mathcal{A}\}$. Demuestre que $CE(\mathcal{A})$ es un subanillo de $\mathcal{A}$. $((CE(\mathcal{A}),+)$, y $(CE(\mathcal{A})\setminus\{0\},\cdot)$ son subgrupos de $(\mathcal{A},+)$ y $(\mathcal{A}\setminus\{0\},\cdot)$ respectivamente).

28. Sea $M_{22}(\mathbb{Z})=\{\begin{pmatrix}a&b\\c&d\end{pmatrix}/a,b,c,d\in\mathbb{Z}\}$ con la multiplicación (definida en ejercicio 8) y suma de matrices:

$$\begin{pmatrix}a&b\\c&d\end{pmatrix}+\begin{pmatrix}a'&b'\\c'&d'\end{pmatrix}=\begin{pmatrix}a+a'&b+b'\\c+c'&d+d'\end{pmatrix}$$

(a) Demuestre que es un anillo con unidad (elemento neutro para $\cdot$), pero con divisores del cero y no conmutativo.

(b) Demuestre que $T=\{\begin{pmatrix}a&b\\0&c\end{pmatrix}/a,b,c\in\mathbb{Z}\}$ es un subanillo de $M_{22}(\mathbb{Z})$.

29. Sea $(\mathcal{A},+,\cdot)$ un anillo y $a\in\mathcal{A}$, definimos $f_a:\mathcal{A}\to\mathcal{A},\ x\to ax$. Sea $F_{\mathcal{A}}=\{f_a/a\in\mathcal{A}\}$. Pruebe que:
(a) $(F_{\mathcal{A}},+,\circ)$ es un anillo con la suma y composición funciones.
(b) $(F_{\mathcal{A}},+,\circ)\cong(\mathcal{A},+,\circ)$ (considere $\varphi:\mathcal{A}\to F_{\mathcal{A}}$ tal que $a\mapsto f_a$).

* 30. Sea $(\mathcal{A},+,\cdot)$ un anillo con unidad, $x\in\mathcal{A}$ se dice *nilpotente* si $\exists n\in\mathbb{N}$ tal que $x^n=0$. Demuestre:
(a) $1-x$ es nilpotente $\Rightarrow x$ es invertible $(\exists x^{-1}\in\mathcal{A})$.
(b) En el anillo $(\mathbb{Z}_n,\oplus,\cdot)$, demostrar que: $\mathbb{Z}_n$ posee elementos nilpotentes $\iff n$ es divisible por el cuadrado de un natural $k>1$, es decir, $n=k^2\alpha;\quad k>1,k\in\mathbb{N}$.

* 31. Un anillo conmutativo con unidad y sin divisores de cero se le denomina *dominio de integridad*. Sea $(\mathcal{A},+,\cdot)$ un dominio de integridad tal que $|\mathcal{A}|<\infty$. Pruebe que tiene también estructura de cuerpo.

32. Sea $(\mathcal{K},+,\cdot)$ un cuerpo cualquiera (0 neutro de $(\mathcal{K},+)$ y 1 neutro de $(\mathcal{K},\cdot)$). Pruebe que
(a) $x\neq 0\Rightarrow(-x)^{-1}=-(x^{-1})$
(b) $x^2=1\Rightarrow(x=1)\wedge(x=-1)$
(c) $x+x=0\Rightarrow x=0$.

33. Muestre que en un cuerpo $(\mathcal{K},+,\cdot)$, no es necesario exigir la conmutatividad de $+$. (Indicación: Considere el desarrollo de $(1+1)(x+y)$ de dos maneras diferentes).

34. En el cuerpo $(\mathbb{Z}_5,\oplus,\cdot)$ resuelva las ecuaciones
(a) $[3]x\oplus[1]=[4]$.
(b) $([2]x\oplus[3]y=[2])\wedge(x\oplus(-[4])y=[1])$.

TEMAS CAPITULO V

1. **Torres.**

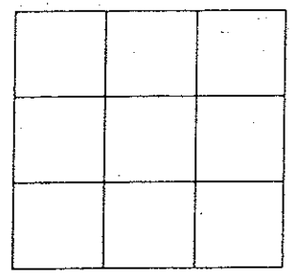
2. **Variaciones sobre el triángulo de las Bermudas.**

3. **La Pascalina reproductora.**

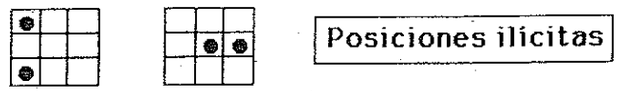
4. **Funciones indicatrices.**

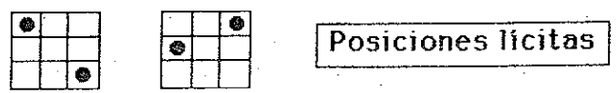
1. Torres.

Tomemos un tablero de 3×3 y dos fichas:



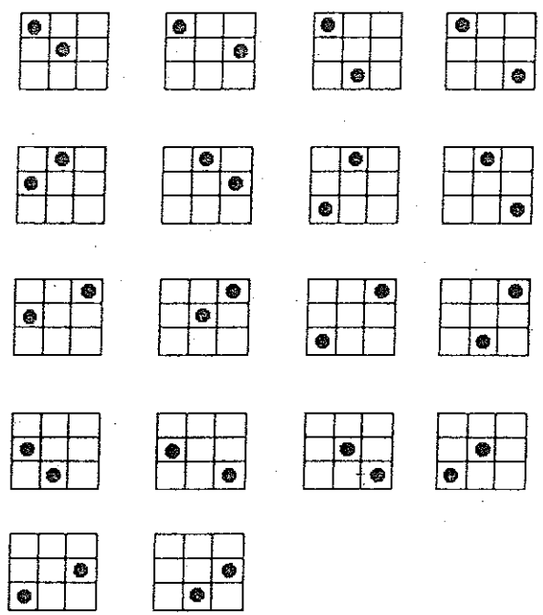
Las posiciones lícitas de las fichas son tales que no deben encontrarse en la misma línea ni en la misma columna. Por ejemplo:





de lo anterior podemos considerar que las fichas son torres de ajedrez.

No es difícil determinar todas las posiciones lícitas posibles:



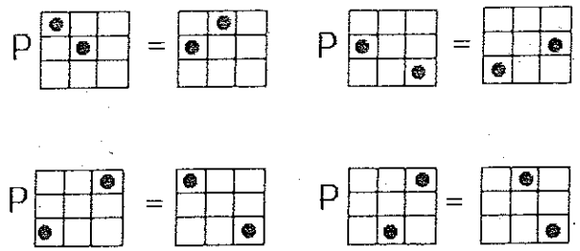
(Justifique de manera más formal).

Definamos sobre el conjunto C, de configuraciones lícitas, los operadores siguientes:

$$P : C \to C$$
$$c \to P(c)$$

donde $P(c)$ consiste en cambiar las fichas a los extremos del rectángulo que definen.

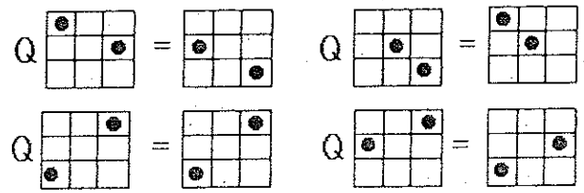
Por ejemplo:



Definamos ahora

$$Q : C \to C$$
$$c \to Q(c)$$

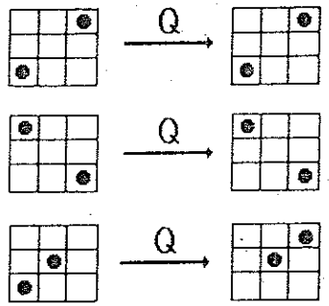
tal que Q coloca las fichas en la posición simétrica con respecto al cuadrado central:



Las siguientes propiedades de P y Q son evidentes:

1. $P^2 = P \circ P = id$ (función identidad).

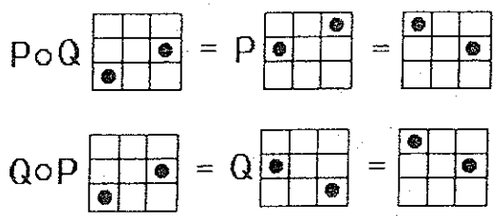
2. Q deja invariantes las configuraciones que son simétricas con respecto al cuadrado central. Además deja invariante la ficha colocada en el cuadrado central:



3. $Q^2 = Q \circ Q = id$.

4. P y Q son aplicaciones bivectivas (verifique).

Apliquemos ahora $P \circ Q$ y $Q \circ P$, sobre algunas configuraciones:



En general se tiene que $P \circ Q = Q \circ P$. (Verifique).

¿Qué podemos decir de $P \circ Q \circ P$, $Q \circ P \circ Q$? Como P y Q permutan se tiene:

$$P \circ Q \circ P = P \circ P \circ Q = P^2 \circ Q = id \circ Q = Q$$
$$Q \circ P \circ Q = Q^2 \circ P = id \circ P = P.$$

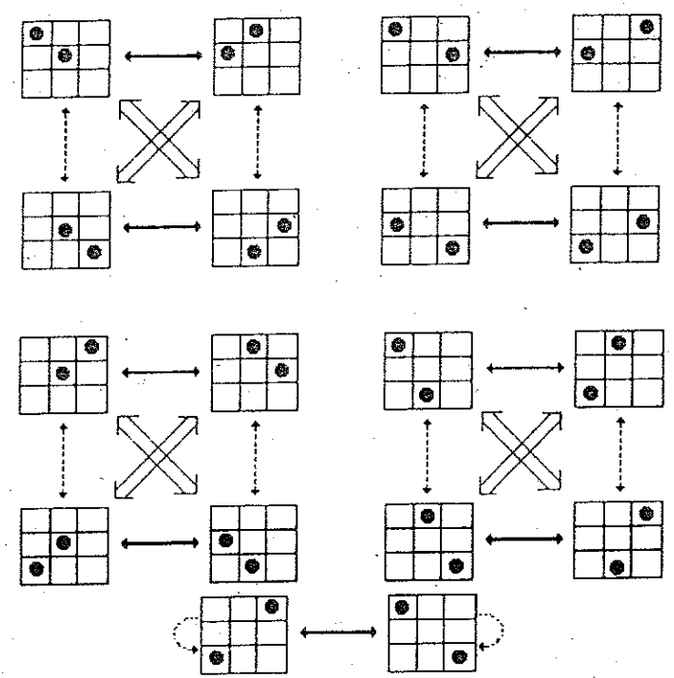
Luego, al componer, siempre obtenemos una de las cuatro funciones: $id, P, Q,$
$P \circ Q$. Formemos la tabla de Pitágoras de la estructura $(U, \circ)$ donde $U = \{id, P, Q,$
$P \circ Q\}$:

$\circ$	id	P	Q	$P \circ Q$
id	id	P	Q	$P \circ Q$
P	P	id	$P \circ Q$	P
Q	Q	$P \circ Q$	id	P
$P \circ Q$	$P \circ Q$	P	Q	id

Por ejemplo: $(P \circ Q) \circ (P \circ Q) = P \circ (Q \circ Q) \circ P = P \circ P = id$.

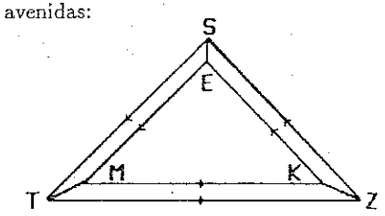
De la tabla es directo que $(U, \circ)$ es isomorfo al grupo de Klein (verifique estableciendo el isomorfismo).

Veamos finalmente el diagrama de trayectorias marcando: $\rightarrow$ por P, $--\!>$ por Q y $\Rightarrow$ por $P \circ Q$



2. Variaciones sobre el triángulo de Las Bermudas.

Supongamos una ciudad hipotética cuyo centro cívico está formado por el conjunto de avenidas:



Flecha: sentido de circulación. Ausencia de flecha: doble sentido.

Un vehículo puede ir de T a S de muchas maneras (hay varias trayectorias o caminos):
de T ir a Z y de Z a S: TZS o bien $TMKES, TMKZS$, etc....

El primer problema que nos proponemos es el siguiente:
Dado el punto inicial, ¿cómo codificar las trayectorias sin ambigüedad y sin escribir los puntos de intersección de las avenidas?
Notemos: $\rightarrow$ acción de seguir una avenida de sentido único.
$\leftrightarrow$: la acción de seguir una avenida de doble sentido.

De esta manera, partiendo del punto T:

$\rightarrow\rightarrow$ codifica TZS
$\leftrightarrow\rightarrow\leftrightarrow\rightarrow$ codifica $TMKZS$
$\leftrightarrow\leftrightarrow$ codifica TMT
$\rightarrow\rightarrow\rightarrow$ codifica $TZST$.

Los dos últimos caminos codifican un regreso al punto inicial, lo que de algún modo, es equivalente a que el vehículo no se hubiese desplazado.

Obviamente, si sólo nos interesa ir de un cierto punto X a otro Y, sin importar el largo del recorrido, todos los caminos posibles entre estos puntos son equivalentes. En tal sentido definimos la siguiente relación entre caminos:
Sea C el conjunto de todos los caminos dados por los diagramas de flechas:
$\forall c, c' \in C : c \sim c' \Leftrightarrow$ *Dado un punto inicial arbitrario común a ambos caminos* c *y* c', *el punto final es el mismo.*

Por ejemplo $\rightarrow\rightarrow$ y $\leftrightarrow\rightarrow\rightarrow\leftrightarrow$ están relacionados entre sí:
Aplicados al punto S:
$\rightarrow\rightarrow$ codifica STZ y $\leftrightarrow\rightarrow\rightarrow\leftrightarrow$ codifica $SEMKZ$
(verifique para otros puntos iniciales).

$\rightarrow\rightarrow\rightarrow$ y $\rightarrow\leftrightarrow$ no están relacionados entre sí:
Partiendo de T:
$\rightarrow\rightarrow\rightarrow$ codifica $TZST$ y $\rightarrow\leftrightarrow$ codifica TZK, los cuales tienen el mismo punto final.

No es difícil verificar que $\sim$ es una relación de equivalencia sobre C.

Por comodidad notemos $a = \leftrightarrow \quad b = \rightarrow$. Luego el conjunto C de caminos está formado de todas las palabras con letras en el "abecedario" $\{a, b\}$. Agreguemos, al conjunto C una palabra, denominada *vacía*, v que significa no hacer movimiento alguno. Por ejemplo:

$$(aa = v) \ \wedge \ (bbb = v)$$

En tal sentido notemos $C = \{a, b\}^*$ como el conjunto de todas las palabras en C, incluyendo la palabra vacía v.

De esta manera hemos definido un lenguaje en $\{a, b\}$ con su gramática y sintaxis. Obviamente este "lenguaje" dista muchísimo de la complejidad del lenguaje natural (en nuestro caso, el castellano). Modelos algebraicos de lenguajes naturales han sido desarrollados con relativo éxito por N. Chomsky y otros matemáticos y lingüistas, pero no nos alejemos de nuestro problema.

Como $\sim$ es una relación de equivalencia sobre $\{a, b\}^*$, definamos el conjunto cociente $\{a, b\}^* / \sim$. Para esto analicemos cuáles son los caminos más cortos, partiendo del punto E (dada la simetría de los triángulos, da lo mismo partir de otro punto de intersección) a las otras intersecciones de avenidas:
camino más corto de E *a* :

$E : v$ (no moverse, palabra vacía)
$M : b$
$K : bb$
$S : a$
$T : ab, ba$
$Z : bba, bab, abb.$

Pero $ab \sim ba$, en efecto:

Si partimos de un punto arbitrario, digamos T, ab codifica TMK y ba codifica TZK. Análogamente:

$$bba \sim abb \sim bab.$$

Esto es directo del hecho que $ab \sim ba$:

$$bba \sim bab \qquad (\text{ aplicando } ab \sim ba)$$

$$bab \sim abb \qquad (\text{ aplicando } ab \sim ba).$$

El hecho que $ab \sim ba$ puede interpretarse como la conmutatividad de la concatenación de dos letras del abecedario.

Tomemos ahora una palabra arbitraria $w \in \{a,b\}^*$. Por ejemplo:

$$w = abbbaaaabab$$

como $bbb \sim aa \sim v \Rightarrow$
$w \sim abab$ y por conmutatividad
$w \sim baab \sim bb$.

Es decir, el camino w está en la misma clase de equivalencia que bb.

En forma general podemos enunciar el resultado siguiente:

Cualquier palabra $w \in \{a,b\}^*$ es equivalente a alguna palabra del conjunto $\{v, b, bb, a, ab, abb\}$.

Demostración. Por inducción sobre n, número de letras (a o b) de la palabra.

Obviamente se verifica para $n = 0, 1, 2, 3$. Veamos el caso $n = 4$:

$$w = x_1x_2x_3x_4.$$

Claramente, si el número de $a's$ es 0
$w \sim b$.
Si el número de $a's$ es 1:
$w \sim a$ (verifique).
Si el número de $a's$ es 2:
$w \sim bb$ (verifique).
Si el número de $a's$ es 3:
$w \sim ab$ (verifique).

Si el número de $a's$ es 4:
$w \sim v$.

Luego la propiedad se verifica para las palabras de largo $n \leq 4$, supongamos que es cierto para las palabras de largo $k \leq n$ y demostremos para $n+1$.

Sea $w = x_1x_2x_3x_4....x_{n+1}$. Sabemos que $x_1x_2x_3x_4 \sim u$ donde u tiene a lo más dos letras, luego

$$w \sim ux_5x_6...x_{n+1} = w'$$

y w' tiene $\leq n-1$ letras. Luego, por hipótesis de inducción, existe $h \in \{v, a, b, bb, ab, abb\}$ tal que $w' \sim h$. Por transitividad concluímos que $w \sim h$ ■

Del teorema se deduce como corolario que el conjunto $C = \{a,b\}^*$ se particiona en 6 clases de equivalencia:

$$C = [v] \cup [a] \cup [b] \cup [ab] \cup [bb] \cup [abb].$$

Definamos ahora una operación entre las clases de equivalencia.
Dadas dos clases x, y:

$$[x] \cdot [y] = [xy].$$

Es decir, se escribe la palabra x seguida de la palabra y. Esta operación se denomina concatenación. Claramente, es una *l.c.i.* en $C/\sim$. Formemos la tabla de Pitágoras (en la cual omitimos, por comodidad, los paréntesis de las clases):

$\cdot$	v	a	b	ab	bb	abb
v	v	a	b	ab	bb	abb
a	a	v	ab	b	abb	bb
b	b	ab	bb	abb	v	a
ab	ab	b	abb	bb	a	v
bb	bb	abb	v	a	b	ab
abb	abb	bb	a	v	ab	b

Claramente, la concatenación es asociativa y conmutativa, admite v como neutro y cada elemento tiene inverso:

$$v^{-1} = v, a^{-1} = a, b^{-1} = bb, (ab)^{-1} = abb, (bb)^{-1} = b, (abb)^{-1} = ab.$$

Luego, $(C/\sim, \cdot)$ es un grupo abeliano de orden seis.

Ejercicios.

1. a) Interprete la conmutatividad de la concatenación en términos de caminos a partir de un punto de intersección de avenidas.
   b) Interprete el inverso de una clase en el mismo sentido.
2. Dado el alfabeto $\{a, b\}$ y el conjunto de palabras (ahora sin incluir la palabra vacía) $\{a, b\}^*$, construya la estructura asociada cuando se tiene: (1) $a^2 = aa = a, b^2 = bb = b, ab = ba$.
   Dadas $w, v \in \{a, b\}^*$ se define la relación:
   $w \sim v \Leftrightarrow$ aplicando la propiedad (1) w y v se reducen a una misma palabra $u \in \{a, b\}^*$.
   Por ejemplo: $abbaa \sim baaabb$.
   En efecto:

$$abbaa \rightarrow aba \rightarrow ab$$

$$baaabb \rightarrow bab \rightarrow ab.$$

Por otra parte,

$$aabaaaa \text{ pués } aaba \rightarrow ab \wedge aaa \rightarrow a.$$

Demuestre que $\sim$ es una relación de equivalencia en $\{a, b\}^*$ y que las clases de equivalencia son $[a], [b], [ab]$ (recuerde que no incluye la palabra nula v).

Definiendo la concatenación $\cdot$ entre palabras, estudie las propiedades de la estructura $(\{a, b\}^*/\sim, \cdot)$.

3. Consideremos el conjunto $\{a, b\}^*$ de "palabras" de cualquier largo formadas con a, b y v como la "palabra" vacía perteneciente a $\{a, b\}^*$.
   Sean los subconjuntos de $\{a, b\}^*$ siguientes:
   $V = \{$ palabra vacía $= v\}$
   $AA = \{$ palabra de largo impar que comienza con a alternando con $b\}$
   $AB = \{$ palabra de largo par que comienza con a alternando con $b\}$
   $BA = \{$ palabra de largo par que comienza con b alternando con $a\}$
   $BB = \{$ palabra de largo impar que comienza con b alternando con $a\}$.

   Ejemplo: $bababa \in BA$; $aba \in AA$

   Sea $U = \{V, AA, AB, BA, BB\}$.
   Se define la operación reducción r en $\{a, b\}^*$ que trabaja con la regla $a^2 = b^2 = v$ (palabra vacía).
Ejemplo: $u = abbaaab \xrightarrow{r} r(u) = avvab = abb \xrightarrow{r} vb = b$.

Sean $u, w \in r(\{a, b\}^*)$ se define $\sim$ como sigue: $u \sim w \Longleftrightarrow u$ y v pertenecen al mismo conjunto de U.

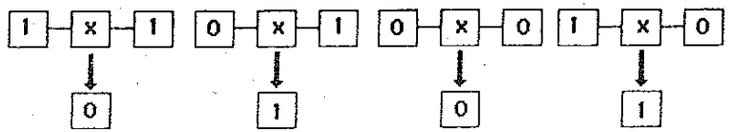
(a) Demuestre que $\sim$ es relación de equivalencia y que $r(\{a, b\}^*)/_\sim = U$.
(b) Entregue los representantes más cortos (en número de letras) de cada clase.
(c) Dadas dos clases $X, Y \in U$ definimos la concatenación (pegar dos palabras) como la clase $XY \in U$. Estudie las propiedades estructurales de U con la concatenación.

3. La Pascalina reproductora.

Definamos el siguiente juego en el grupo $(\mathbb{Z}_p, \oplus)$: tomemos una línea infinita compuesta de celdas

i: indica la posición i-ésima en la línea.

En cada celda coloquemos un "cero" o un "uno". Si la celda central está en el valor $x \in \{0,1\}$, ésta cambia de valor, en la línea siguiente, de acuerdo a la regla:



No es agotador darse cuenta que: $\forall x, y, z \in \{0,1\}$ el nuevo valor de la componente central de la configuración (y, x, z) es $x' = y \oplus z \in \mathbb{Z}_2$, donde $(\mathbb{Z}_2, \oplus)$ es el grupo abeliano de las clases de equivalencia módulo dos

$\oplus$	0	1
0	0	1
1	1	0

Además, en $(\mathbb{Z}_2, \oplus)$, se verifica:

$$\forall x \in \mathbb{Z}_2, \quad x \oplus x = 0.$$

Propiedad que usaremos posteriormente.

La evolución en paralelo (todos el mismo tiempo) de la regla anterior se denomina un *autómata celular*. Consideremos la evolución siguiente:

$t=0$	$\cdots$	0	0	0	0	**1**	0	**0**	**1**	0	0	0	0 $\cdots$
$t=1$	$\cdots$	0	0	0	1	0	1	1	0	1	0	0	0 $\cdots$
$t=2$	$\cdots$	0	0	1	0	0	1	1	0	0	1	0	0 $\cdots$
$t=3$	$\cdots$	0	1	0	1	1	1	1	1	1	0	1	0 $\cdots$
$t=4$	$\cdots$	**1**	**0**	**0**	**1**	0	0	0	0	**1**	**0**	**0**	**1** $\cdots$

¡Magia!, en la línea $t = 4$ hemos obtenido dos copias de la isla inicial (entre los dos unos).

Usted alegará casualidad o que la isla inicial es muy simétrica. Razonable duda; veamos otro ejemplo:

$t=0$	$\cdots$	0	0	0	0	0	**1**	**1**	**0**	**1**	0	0	0	0	0 $\cdots$
$t=1$	$\cdots$	0	0	0	0	1	1	1	0	0	1	0	0	0	0 $\cdots$
$t=2$	$\cdots$	0	0	0	1	1	0	1	1	1	0	1	0	0	0 $\cdots$
$t=3$	$\cdots$	0	0	1	1	1	0	1	0	1	0	0	1	0	0 $\cdots$
$t=4$	$\cdots$	0	1	1	0	1	0	0	0	0	1	1	0	1	0 $\cdots$

¡Nuevamente hemos obtenido dos copias!

Conjeturamos entonces que cualquier isla se "reproduce" en un número finito de aplicaciones de la regla. Es decir, en un número finito de pasos, aparecen en el mar sólo copias de la isla inicial (¡el ADN en su sopa primitiva diría un entusiasta!).

Verifiquemos la propiedad para una isla arbitraria de largo 4:

$$\ldots 0\ a\ b\ c\ d\ 0 \ldots$$

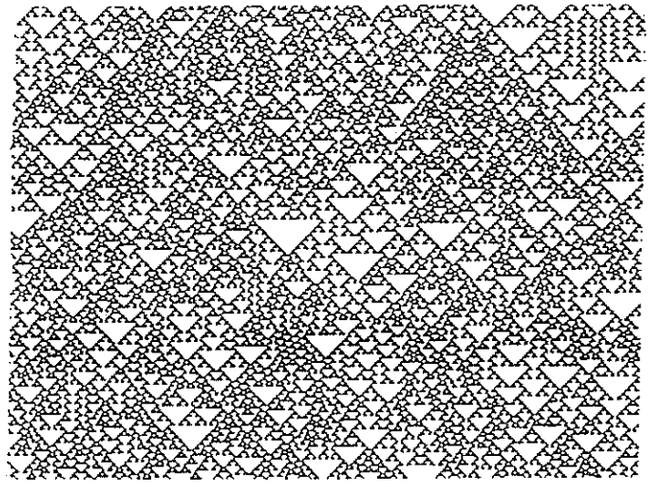
Es claro que $a = d = 1$. Si no, la isla sería de tamaño menor.

Vamos ahora la dinámica:

0	0	0	0	1	b	c	1	0	0	0	0
0	0	0	1	b	$1 \oplus c$	$1 \oplus b$	c	1	0	0	0
0	0	1	b	c	1	1	b	c	1	0	0
0	1	b	$1 \oplus c$	$1 \oplus b$	$1 \oplus c$	$1 \oplus b$	$1 \oplus c$	$1 \oplus b$	c	1	0
1	b	c	1	0	0	0	0	1	b	c	1

Hemos verificado que cualquier isla de largo cuatro se reproduce (en dos copias) en cuatro pasos. Obviamente, esta manera de atacar el problema no

constituye una demostración para el caso general. El mismo análisis puede hacerse para islas de largo 5,6,7,8,9,10,... pero, para n arbitrario se requiere una aproximación diferente. En cualquier caso, el fenómeno esencial está implícito en el viejo triángulo de Pascal (codificando 0 si el número es par y 1 si es impar). Una evolución típica para un archipiélago (conjunto de islas) es la siguiente:



En la figura anterior un punto negro codifica 1 y un blanco, el 0.

Este tipo de regla puede aún generalizarse al grupo de congruencias $(\mathbb{Z}_p, \oplus) = (\{0, 1, ..., p-1\}, \oplus)$. Por ejemplo en $(\mathbb{Z}_5, \oplus)$ la regla sería

$$\begin{array}{c} y\ x\ z \\ \downarrow \\ y \oplus z \end{array}$$

y también se reproducen las islas:

```
                0 2 3 4 1 0
              0 2 3 1 4 4 1 0
            0 2 3 3 2 0 0 4 1 0
          0 2 3 0 0 3 2 4 1 4 1 0
        0 2 3 2 3 3 2 2 3 3 2 4 1 0
      0 2 3 4 1 0 0 0 0 0 0 2 3 4 1 0
```

obteniéndose dos copias de la isla original.

4. Funciones indicatrices.

Sea el cuerpo de congruencias módulo dos: $(\mathbb{Z}_2, \oplus, \cdot)$. Recordemos

$\oplus$	0	1
0	0	1
1	1	0

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

Sea U un conjunto arbitrario y sea $\mathcal{Y}(U, \mathbb{Z}_2)$ el conjunto de funciones de U en $\mathbb{Z}_2$.

Dado un conjunto $X \in \mathcal{P}(U)$ asociamos la aplicación:

$$f_X : U \to \mathbb{Z}_2$$

tal que

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

f_X se denomina la indicatriz del conjunto X.

Por ejemplo si $U = \{1, 2, 3, 4\}$ y $X = \{1, 3\}$:

$$f_X(1) = f_X(3) = 1, \quad f_X(2) = f_X(4) = 0.$$

Estructuremos el conjunto de indicatrices $\mathcal{Y}(U, \mathbb{Z}_2)$ asociándole las operaciones siguientes:

$$\begin{array}{l} (f_A \oplus f_B)(x) = f_A(x) \oplus f_B(x) \\ (f_A \cdot f_B)(x) = f_A(x) \cdot f_B(x) \end{array} \qquad A, B \in \mathcal{P}(U), x \in U$$

donde las operaciones $\oplus, \cdot$ de la derecha corresponden a la suma y la multiplicación en $\mathbb{Z}_2$.

- No es difícil verificar que, con estas operaciones, $(\mathcal{Y}(U, \mathbb{Z}), \oplus, \cdot)$ es un anillo conmutativo con unidad.
- Señalemos que el neutro aditivo es f_ϕ y el neutro multiplicativo es f_U.

También es fácil ver que si U tiene más de un elemento (no es un singleton), entonces $(\mathcal{Y}(U, \mathbb{Z}_2) \setminus \{f_\phi\}, \cdot)$ no es grupo. Es decir, si U no es singleton $(Y(U, \mathbb{Z}_2), \oplus, \cdot)$ no es un cuerpo.

Ejercicio: Demuestre que si $|U| \geq 2$ entonces la estructura admite divisores del cero.

Las identidades siguientes nos serán de gran utilidad (demuestre):

Dado $X \in \mathcal{P}(U)$ y $\bar{X} = C_U(X)$ se verifica:

1. $f_X \oplus f_X = f_\phi$ 2. $f_X = f_U \oplus f_{\bar{X}}$

3. $f_X \cdot f_X = f_X$ 4. $f_X \cdot f_{\bar{X}} = f_\phi$.

Además:

5. $f_{A\cap B} = f_A \cdot f_B$

6. $f_{A\cup B} \oplus f_{A\cap B} = f_A \oplus f_B$.

Demostremos 6 mediante una tabla de pertenencia (¿por qué?):

	$f_{A\cup B}(x)$	$f_{A\cap B}(x)$	$f_{A\cup B}(x) \oplus f_{A\cap B}(x)$	$f_A(x) \oplus f_B(x)$
$x \in A \wedge x \in B$	1	1	0	0
$x \in A \wedge x \notin B$	1	0	1	1
$x \notin A \wedge x \in B$	1	0	1	1
$x \notin A \wedge x \notin B$	0	0	0	0

De la igualdad de las dos últimas columnas obtenemos la identidad ■

De la identidad 6, sumando a ambos lados $f_{A\cap B}$:

$$f_{A\cup B} \oplus (f_{A\cap B} \oplus f_{A\cap B}) = (f_A \oplus f_B) \oplus f_{A\cap B}$$

obtenemos:

7. $f_{A\cup B} = f_A \oplus f_B \oplus (f_A \cdot f_B)$.

Analicemos ahora cuál es la función indicatriz de la diferencia simétrica de dos conjuntos:

$$A\triangle B = (A \setminus B) \cup (B \setminus A) = (A \cap \bar{B}) \cup (\bar{A} \cap B)$$

$$f_{A\triangle B} = f_{(A\cap\bar{B})\cup(\bar{A}\cap B)}$$

De la identidad 7:

$$= f_{A\cap\bar{B}} \oplus f_{\bar{A}\cap B} \oplus (f_{A\cap\bar{B}} \cdot f_{\bar{A}\cap B}).$$

De la identidad 5:

$$= (f_A \cdot f_{\bar{B}}) \oplus (f_{\bar{A}} \cdot f_B) \oplus (f_A \cdot f_{\bar{B}} \cdot f_{\bar{A}} \cdot f_B).$$

De la identidad 4 se tiene que el tercer término es el neutro aditivo f_ϕ, de donde:

$$f_{A\triangle B} = (f_A \cdot f_{\bar{B}}) \oplus (f_{\bar{A}} \cdot f_B).$$

Utilizando la identidad 2 para $\bar{B}$ y $\bar{A}$:

$$= [f_A \cdot (f_U \oplus f_B)] \oplus [(f_U \cdot f_A) \cdot f_B],$$

distribuyendo:

$$= [(f_A \cdot f_U) \oplus (f_A \cdot f_B)] \oplus [(f_U \cdot f_B) \oplus (f_A \cdot f_B)]$$
$$= [f_A \oplus (f_A \cdot f_B)] \oplus [(f_B \oplus (f_A \cdot f_B)],$$

por asociatividad y conmutatividad de $\oplus$:

$$= f_A \oplus f_B \oplus ((f_A \cdot f_B) \oplus (f_A \cdot f_B)).$$

De la identidad 1 concluímos:

8. $f_{A\triangle B} = f_A \oplus f_B$.

Ahora estamos en condiciones de probar que:

$$(\mathcal{P}(U), \triangle, \cap) \cong (\mathcal{Y}(U, \mathbb{Z}_2), \oplus, \cdot).$$

En efecto, sea la aplicación

$$\varphi : \mathcal{P}(U) \to \mathcal{Y}(U, \mathbb{Z}_2)$$
$$X \to \varphi(X) = f_X$$

φ es una biyección:

- Inyectividad:

$$\varphi(X) = \varphi(Y) \Leftrightarrow f_X = f_Y$$
$$\Leftrightarrow \forall x \in U, f_X(x) = f_Y(x)$$
$$\Leftrightarrow f_X(x) = 1 \Leftrightarrow f_Y(x) = 1$$
$$\Leftrightarrow x \in X \Leftrightarrow x \in Y \Leftrightarrow X = Y \quad ■$$

- Epiyectividad: Sea una aplicación $g \in \mathcal{Y}(U, \mathbb{Z}_2)$ y sea $A_g = \{x \in U / g(x) = 1\}$, luego $\varphi(A_g) = g$ ■

- φ es un homomorfismo:

$$\varphi(X\triangle Y) = f_{X\triangle Y} = f_X \oplus f_Y = \varphi(X) \oplus \varphi(Y)$$
$$\varphi(X \cap Y) = f_{X\cap Y} = f_X \cdot f_Y = \varphi(X) \cdot \varphi(Y) \quad ■$$

Aplicación:

Las funciones indicatrices son útiles para probar propiedades de conjuntos. Por ejemplo, demostremos la propiedad:

$$[(A \cup B) = B \ \wedge \ (A \cap B = \phi)] \Rightarrow (A = \phi).$$

Las hipótesis se escriben en términos de generatrices, como sigue:

$$f_{A\cup B} = f_B \wedge f_{A\cap B} = f_\phi.$$

Aplicando las identidades anteriores:

$$f_A \oplus f_B \oplus (f_A \cdot f_B) = f_B \ \wedge \ f_A \cdot f_B = f_\phi,$$

luego, $f_A \oplus f_B = f_B$, de donde:

$$f_A = f_\phi \Leftrightarrow A = \phi \quad \blacksquare$$

Demostremos, de manera análoga, una ley de De Morgan:

$$\overline{A \cup B} = \bar{A} \cap \bar{B}.$$

En términos de generatrices, desarrollemos

$$\begin{aligned} f_{\overline{A\cup B}} &= f_U \oplus f_{A\cup B} \qquad \text{(identidad 2)} \\ &= f_U \oplus (f_A \oplus f_B \oplus (f_A \cdot f_B)) \qquad \text{(identidad 7)} \\ &= (f_U \oplus f_A) \oplus (f_B \oplus (f_A \cdot f_B)), \end{aligned}$$

pero $f_B \oplus (f_A \cdot f_B) = f_{\bar{A}} \cdot f_B$ (verifique utilizando una tabla), de donde,

$$f_{\overline{A\cup B}} = (f_U \oplus f_A) \oplus (f_{\bar{A}} \cdot f_B),$$

aplicando 2 y la identidad $f_X = f_X \cdot f_U \ \ \forall x \in \mathcal{P}(U)$:

$$\begin{aligned} &= (f_U \oplus f_A) \oplus ((f_U \oplus f_A) \cdot f_B) \\ &= ((f_U \oplus f_A) \cdot f_U) \oplus ((f_U \oplus f_A) \cdot f_B), \end{aligned}$$

por distributividad:

$$= (f_U \oplus f_A) \cdot (f_U \oplus f_B)$$

y finalmente, de la identidad 2:

$$f_{\overline{A\cup B}} = f_{\bar{A}} \cdot f_{\bar{B}} = f_{\bar{A}\cap\bar{B}}.$$

Es decir: $\overline{A \cup B} = \bar{A} \cap \bar{B}$ ■

Ejercicios.

1. Utilizando indicatrices, demuestre:
   (a) $A \cup B = U \wedge A \cap B = \phi \Rightarrow A = \bar{B}$.
   (b) $(A \cup B) \cap \bar{B} = A \Rightarrow A \cap B = \phi$.
   (c) Asociatividad de $\triangle$: $A\triangle(B\triangle C) = (A\triangle B)\triangle C$.
   (d) $\overline{A\triangle B} = \bar{A}\triangle B = A\triangle\bar{B}$.
   (e) $A\triangle B = \bar{A}\triangle\bar{B}$.
2. Calcule $f_{A\setminus B}$ en términos de las identidades conocidas de indicatrices.
3. Demuestre, utilizando indicatrices:
   (a) $B \setminus A = (A\triangle B) \cap B$.
   (b) $A \setminus B = A \Rightarrow A \cap B = \phi$.
4. Demuestre $A \subseteq B \Leftrightarrow f_A = f_A \cdot f_B$.

CAPITULO VI

Imaginario: guardia que no efectúa rondas, pero se encuentra en un lugar fijo dispuesto a intervenir si fuera necesario. (boinazo para el autor, imaginario según el diccionario práctico de la lengua española)

COMPLEJOS Y POLINOMIOS

6.1. El Cuerpo de los complejos.

Los números complejos se originan en la ecuación $x^2 + 1 = 0$. Esta ecuación no tiene solución real. Acostumbramos a resolver esto, escribiendo sus soluciones como $\pm\sqrt{-1}$ y definiendo $\sqrt{-1} = i$, como *unidad imaginaria*. Esto es, aparentemente, un procedimiento harto simplista y oscuro. Cuando un problema no tiene solución en un conjunto, lo agrandamos, agregando las soluciones y listo.... Pero esto es sólo aparente, ya que esta idea se ha revelado muy fructífera, como veremos a continuación.

Trataremos de dar en este párrafo la construcción detallada de un cuerpo denominado de los *números complejos*, y que notamos $\mathbb{C}$, tal que "contenga" $\mathbb{R}$ y la ecuación $x^2 + 1 = 0$ admita solución. Más aún, cuando estudiemos el anillo de polinomios veremos que $\mathbb{C}$ es, en realidad, la estructura natural donde "viven" las soluciones de una ecuación polinomial.

Pero la utilidad de $\mathbb{C}$ no radica solamente en lo anterior: los números complejos aparecen también en diversas áreas de la física, matemática y ciencias de la ingeniería, de manera crucial e insoslayable.

Construyamos entonces $\mathbb{C}$, de modo que la ecuación $x^2 + 1 = 0$ tenga solución. Para ello, agregamos a $\mathbb{R}$ el "número" $i = \sqrt{-1}$ y definimos operaciones de reales con este número, de manera que se obtenga una estructura de cuerpo.

Sea $\mathbb{C} = \{a + bi / a, b \in \mathbb{R}\}$ el conjunto denominado de *números complejos*. Claramente, $\mathbb{R} \subseteq \mathbb{C}$ (basta tomar $b = 0$). Definiremos las operaciones en $\mathbb{C}$ tales que al aplicarlas a números reales recuperemos la suma y la multiplicación usuales.

Dados $z = z + bi, \quad z' = c + di$:

$$z + z' = (a + bi) + (c + di) = (a + c) + (b + d)i \in \mathbb{C} \qquad (6.1)$$

$$zz' = (a+bi)\cdot(c+di) = ac + adi + bci + bdi^2$$
$$\text{como } i^2 = -1:$$
$$= (ac - bd) + (ad + bc)i \in \mathbb{C}, \tag{6.2}$$

donde las operaciones $+, \cdot$, que aparecen en el lado derecho de cada ecuación, corresponden a las operaciones reales. Como el resultado de operar con esta suma y multiplicación es un elemento de $\mathbb{C}$, ambas operaciones son leyes de composición interna en $\mathbb{C}$.

Además, $(\mathbb{C}, +, \cdot)$ es un cuerpo, denominado *cuerpo de los Números Complejos*.

En efecto, $(\mathbb{C}, +)$ es un grupo abeliano:

$+$ es asociativa y conmutativa, ya que la suma en $\mathbb{R}$ lo es. El elemento $0 = 0 + 0i$ es el neutro aditivo de $\mathbb{C}$. Dado $z = a + bi$, su inverso aditivo es
$-z = (-a) + (-b)i$ ■

$(\mathbb{C} \setminus \{0+0i\}, \cdot)$ es grupo abeliano.

La multiplicación es asociativa y conmutativa, ya que la multiplicación en $\mathbb{R}$ lo es. Además, $1 = 1 + 0i$ es el neutro multiplicativo:

$$(a+bi)(1+0i) = (a+bi)1 = a + bi.$$

Dado $a + bi \neq 0$ ($a \neq 0$ o $b \neq 0$) su inverso multiplicativo es:

$$(a+bi)^{-1} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$$

En efecto:

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

Finalmente, $\cdot$ distribuye con respecto a $+$:

$$(a+bi)((c+di)+(e+fi)) = (a+bi)((c+e)+(d+f)i)$$
$$= (a(c+e) - b(d+f)) + (b(c+e) + a(d+f))i$$
$$= (ac - bd) + (bc + ad)i + (ae - bf) + (be + af)i$$
$$= (a+bi)(c+di)) + (a+bi)(e+fi)$$ ■

Claramente, la ecuación $x^2 + 1 = 0$ tiene solución en $\mathbb{C}$ y, en forma más general, cualquier ecuación cuadrática $ax^2 + bx + c = 0$. Más adelante

veremos un resultado mucho más fuerte: cualquier ecuación polinomial de grado n tiene solución en $\mathbb{C}$ y, a lo más, n soluciones.

Como notación, dado $z = a + bi$, diremos que a es la *parte real* y b la *parte imaginaria* del número complejo z. Se nota $a = \mathcal{R}e(z), b = Im(z)$.

A modo de ejercicio, veamos cómo se escribe el número complejo $\sqrt{2 + i\sqrt{12}}$ en la forma $x + iy$.

Se tiene: $\sqrt{2 + i\sqrt{12}} = x + iy \Rightarrow 2 + i\sqrt{12} = (x+iy)^2 = x^2 - y^2 + 2xyi$.
Luego, $(x^2 - y^2 = 2) \wedge (2xy = \sqrt{12})$. Elevando ambas ecuaciones al cuadrado y sumando se obtiene: $x^4 + 2x^2y^2 + y^4 = 16 \Leftrightarrow (x^2+y^2)^2 = 16$,
de donde $x^2 + y^2 = 4$.
Obtenemos entonces el sistema cuadrático:

$$x^2 - y^2 = 2$$
$$x^2 + y^2 = 4,$$

cuyas soluciones son: $x = \pm\sqrt{3}$, $y = \pm 1$.

Por otra parte, como $2xy = \sqrt{12} > 0$, las soluciones que nos interesan deben tener el mismo signo; concluyéndose $x + yi = \sqrt{3} + i, x + yi = -\sqrt{3} - i$ (¿qué significa que no haya unicidad?) ■

6.1.1. Conjugados.

Definimos la operación de *conjugación* de $z \in \mathbb{C}$ como la aplicación de $\mathbb{C}$ en sí mismo, tal que $z \to \bar{z} = a - bi$, donde $\bar{z} = a - bi$ se denomina el *conjugado* de z.

Algunas propiedades de la conjugación son las siguientes:

$\forall z_1, z_2 \in \mathbb{C}$:

$$\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2 \tag{6.3}$$
$$\overline{z_1 z_2} = \bar{z}_1 \bar{z}_2 \tag{6.4}$$
$$z \in \mathbb{R} \Leftrightarrow \bar{z} = z \tag{6.5}$$
$$\bar{\bar{z}} = z \tag{6.6}$$
$$\text{Si } z_2 \neq 0,\ \left(\overline{\frac{z_1}{z_2}}\right) = \frac{\bar{z}_1}{\bar{z}_2},\ \text{donde } \frac{1}{z_2} = z_2^{-1} \tag{6.7}$$
$$\mathcal{R}e(z) = \frac{1}{2}(z + \bar{z}), Imz = \frac{1}{2i}(z - \bar{z}) \tag{6.8}$$
$$z\bar{z} = \mathcal{R}e(z)^2 + Im(z)^2 \in \mathbb{R} \tag{6.9}$$

Demostremos algunas de ellas:

(6.3) Sea $z_1 = a + bi, z_2 = c + di$:

$$\begin{aligned}\overline{z_1 + z_2} &= \overline{(a+c)+(b+d)i} = (a+c) - (b+d)i \\ &= (a - bi) + (c - di) = \bar{z}_1 + \bar{z}_2.\end{aligned}$$

(6.5) Sea $z = a + bi$,
Si $\bar{z} = z \Leftrightarrow a + bi = a - bi \Leftrightarrow$
$\Leftrightarrow 2bi = 0 \Leftrightarrow b = 0$ (pues $\mathbb{C}$ es cuerpo, luego no tiene divisores del cero)
$\Leftrightarrow z \in \mathbb{R}$.

(6.8) Sea $z = a + bi$:
$z + \bar{z} = a + bi + a - bi = 2a \Rightarrow \mathcal{R}e(z) = \frac{1}{2}(z + \bar{z})$.

(6.9) $z\bar{z} = (a + bi)(a - bi) = (a^2 + b^2) + (ab - ab)i = a^2 + b^2$
$= \mathcal{R}e^2(z) + Im^2(z) \in \mathbb{R}$ ■

La aplicación $\varphi = \mathbb{C} \to \mathbb{C}, z \to \bar{z}$ es un isomorfismo. En efecto, directamente de (6.3) vemos que es un homomorfismo. Veamos que es biyectiva:
Es inyectiva:

$$\begin{aligned}\varphi(z_1) = \varphi(z_2) &\Leftrightarrow a - bi = c - di \Leftrightarrow \\ (a - c) = (b - d)i &\Leftrightarrow a = c \ \wedge \ b = d \\ &\Rightarrow z_1 = z_2.\end{aligned}$$

Es epiyectiva: dado el complejo $z = a + bi$, entonces $\bar{z} = a - bi$ es su pre-imagen por φ ■

6.1.2. Interpretación geométrica de $\mathbb{C}$.

Asimilaremos $(\mathbb{C}, +, \cdot)$ a los puntos del plano $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ con las operaciones siguientes: $\forall (a, b),\ (c, d) \in \mathbb{R}^2$

$$(a, b) + (c, d) = (a + c, b + d) \in \mathbb{R}^2 \qquad (6.10)$$

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc) \in \mathbb{R}^2. \qquad (6.11)$$

Claramente $+, \cdot$ son $\ell.c.i.$ en $\mathbb{R}^2$. Más aun:

$$\begin{aligned}\Psi : \mathbb{C} &\to \mathbb{R}^2 \\ z = a + bi &\to (a, b)\end{aligned}$$

es un isomorfismo.

En efecto:
Ψ es inyectiva, $\Psi(z_1) = \Psi(z_2) \Leftrightarrow \Psi(a + bi) = \Psi(c + di) \Leftrightarrow (a, b) = (c, d)$
$\Leftrightarrow (a = c) \wedge (b = d) \Leftrightarrow z_1 = z_2$.
Ψ es epiyectiva, dado $(a, b) \in \mathbb{R}^2$ su pre-imagen es el complejo $z = a + bi$.

Demostremos que Ψ es un homorfismo:

$$\begin{aligned}\Psi(z_1 + z_2) &= \Psi((a + bi) + (c + di)) = \Psi((a + c) + (b + d)i) \\ &= (a + c, b + d) = (a, b) + (c, d) = \Psi(z_1) + \Psi(z_2) \\ \Psi(z_1 z_2) &= \Psi((a + bi)(c + di)) = \Psi((ac - bd) + (ad + bc)i) \\ &= (ac - bd, ad + bc) = (a, b) \cdot (c, d) = \Psi(z_1) \cdot \Psi(z_2).\end{aligned}$$

Luego $(\mathbb{R}^2, +, \cdot) \cong (\mathbb{C}, +, \cdot)$ ■

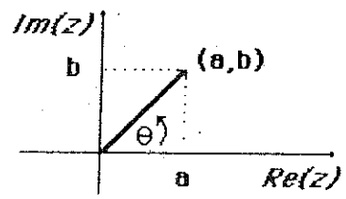
Veamos cuáles son las imágenes de algunos elementos importantes de $\mathbb{C}$, vía este isomorfismo:

$0 = 0 + 0i \leftrightarrow (0, 0)$ neutro aditivo de $(\mathbb{R}^2, +)$
$1 = 1 + 0i \leftrightarrow (1, 0)$ neutro multiplicativo de $(\mathbb{R}^2, +)$
$i = 0 + 1i \leftrightarrow (0, 1)$ unidad imaginaria en $(\mathbb{R}^2, +)$.

Además,

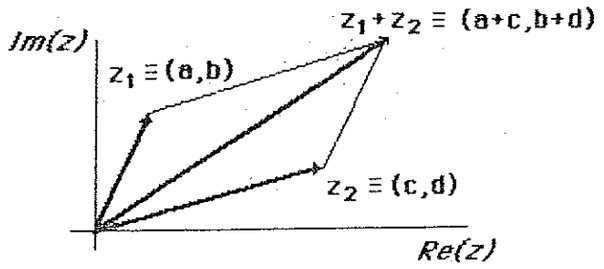
$$i \cdot i = -1 \leftrightarrow (0, 1)(0, 1) = (0 - 1, 0 \cdot 1 + 1 \cdot 0) = (-1, 0) = -(1, 0).$$

Mediante este isomofismo tenemos una interpretación geométrica de $\mathbb{C}$ en $\mathbb{R}^2$. A cada elemento $a + bi$ le asociamos un punto en el eje cartesiano o bien una flecha o vector:



donde θ es el ángulo entre el vector y el eje x, medido en sentido contrario a los punteros del reloj.

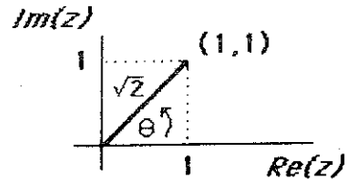
La operación suma en $\mathbb{C}$ puede interpretarse como la suma de vectores en el plano, según la regla del paralelógramo: $z_1 + z_2 = (a + bi) + (c + di) \Leftrightarrow (a, b) + (c, d) = (a + c, b + d)$.



Definamos el *módulo* de un número complejo $z = a + bi$ como sigue:

$$|z| = \sqrt{a^2 + b^2} \in \mathbb{R}. \tag{6.12}$$

Obviamente, $|z|$ es la magnitud del par ordenado (a, b) en el plano $\mathbb{R}^2$. Por ejemplo, $z = 1 + 1i$:



$|z| = \sqrt{2}$, $\cos\theta = \frac{1}{\sqrt{2}} \Rightarrow cos\theta = \frac{\sqrt{2}}{2} \Rightarrow \theta = 45^o$.

Si z tiene parte imaginaria nula, es decir $z = a + 0i$, entonces $|z| = \sqrt{a^2} = |a|$, que corresponde al módulo de un número real.

Algunas propiedades del módulo son las siguientes: $\forall z, z_1, z_2 \in \mathbb{C}$

$$|z| = |-z| = |\bar{z}| = |-\bar{z}| \tag{6.13}$$

$$\mathcal{R}e(z) \leq |z|, Im(z) \leq |z| \tag{6.14}$$

$$z = 0 \Leftrightarrow |z| = 0 \tag{6.15}$$

$$|z_1 \cdot z_2| = |z_1||z_2| \tag{6.16}$$

$$\text{Si } z_2 \neq 0,\ |\frac{z_1}{z_2}| = \frac{|z_1|}{|z_2|} \tag{6.17}$$

$$|z|^2 = z \cdot \bar{z} \tag{6.18}$$

$$|z_1 + z_2| \leq |z_1| + |z_2| \text{ (desigualdad triangular).} \tag{6.19}$$

Demostremos la propiedad (6.19):

Sabemos que si $z_1 = a + bi, z_2 = c + di$, entonces

$$\begin{aligned} |z_1 + z_2|^2 &= \mathcal{R}e(z_1 + z_2)^2 + Im(z_1 + z_2)^2 \\ &= (a + c)^2 + (b + d)^2 = a^2 + b^2 + c^2 + d^2 + 2ac + 2bd. \end{aligned}$$

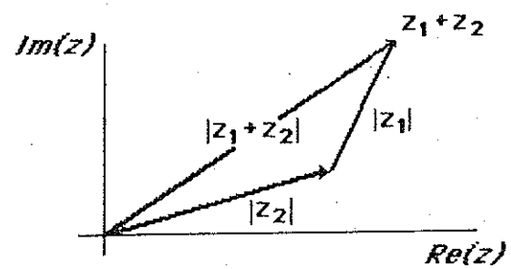
Acotemos el término $ac + bd$. Sabemos que: $(ac + bd)^2 = a^2c^2 + 2abcd + b^2d^2$. Además, $(ad - cb)^2 \geq 0$, lo cual implica $a^2d^2 + c^2b^2 \geq 2adbc$, de donde:

$$\begin{aligned} (ac + bd)^2 &\leq a^2c^2 + a^2d^2 + c^2b^2 + b^2d^2 \\ &\leq a^2(c^2 + d^2) + b^2(c^2 + d^2) \\ &\leq (a^2 + b^2)(c^2 + d^2) = |z_1|^2|z_2|^2; \end{aligned}$$

luego, $(ac + bd) \leq |z_1| \cdot |z_2|$. Reemplazando:

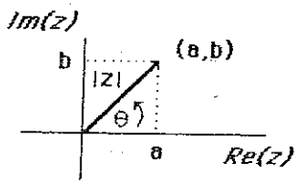
$$\begin{aligned} |z_1 + z_2|^2 &\leq a^2 + b^2 + c^2 + d^2 + 2|z_1||z_2| \\ &\leq |z_1|^2 + 2|z_1||z_2| + |z_2|^2 = (|z_1| + |z_2|)^2 \end{aligned}$$ ■

Geométricamente, la desigualdad triangular puede verse como la distancia más corta entre el origen $(0, 0)$ y el complejo $z_1 + z_2$:



6.1.3. Forma polar de un número complejo.

Dado $z = a + bi \neq 0 + 0i$



se tiene

$$cos\theta = \frac{a}{|z|}; \quad sen\theta = \frac{b}{|z|}.$$

obteniendo:

$$z = |z|(cos\theta + isen\theta), \tag{6.20}$$

que se denomina la *forma polar* de un número complejo, donde el ángulo θ corresponde al *argumento* de z y se nota, $arg(z)$. Por la periodicidad de las funciones trigonométricas, el argumento de z no es único, en realidad $arg(z) \in \{\theta + 2k\pi / k \in \mathbb{Z}\}$.

En este contexto, no es difícil probar que, dados $z_1, z_2 \in \mathbb{C}$:

$$arg(z_1 z_2) = arg(z_1) + arg(z_2) + 2k\pi, k \in \mathbb{Z} \tag{6.21}$$
$$arg(z_1/z_2) = arg(z_1) - arg(z_2) + 2k\pi, k \in \mathbb{Z};\ z_2 \neq 0. \tag{6.22}$$

Verifiquemos (6.21). Sean $z_1 = r_1(cos\varphi + isen\varphi), z_2 = r_2(cos\theta + isen\theta)$, las representaciones polares de z_1 y z_2; luego,

$$z_1 z_2 = r_1 r_2 \{(cos\varphi cos\theta - sen\varphi sen\theta) + (cos\varphi sen\theta + sen\varphi cos\theta)i\}.$$

Aplicando las fórmulas trigonométricas para $cos(\theta + \varphi)$ y $sen(\theta + \varphi)$ se obtiene:

$$z_1 z_2 = r_1 r_2 (cos(\theta + \varphi) + i(sen(\theta + \varphi))$$

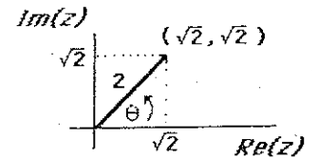
de donde

$$arg(z_1 z_2) = arg(z_1) + arg(z_2) + 2k\pi \quad \blacksquare$$

En particular, dado $z = |z|(cos\theta + isen\theta) \neq 0$, su inverso es $z^{-1} = |z|^{-1}(cos(-\theta) + isen(-\theta))$ (verifique).

Para evitar la multiplicidad de valores del argumento, se define el *argumento principal* como el ángulo comprendido entre $-\pi$ y π y se nota $Arg(z)$.

Escribamos, por ejemplo $z = \sqrt{2} + \sqrt{2}i$ en su forma polar, utilizando $Arg(z)$. A partir del gráfico de z:



Obtenemos $|z| = 2$ y $tg\theta = 1$, luego $Arg(z) = \frac{\pi}{2}$ y la forma polar es

$$z = 2(cos\frac{\pi}{2} + isen\frac{\pi}{2}) \quad \blacksquare$$

Consideremos la aplicación $\varphi : \mathbb{R} \to \mathbb{C},\ x \to cosx + isenx$. Notaremos $\varphi(x) = e^{ix} = cosx + isenx$. Esta función tiene las propiedades siguientes: $\forall x, y \in \mathbb{R}$

$$\overline{e^{ix}} = e^{-ix} = (e^{ix})^{-1} \tag{6.23}$$
$$|e^{ix}| = 1 \tag{6.24}$$
$$e^{ix} \cdot e^{iy} = e^{i(x+y)} \tag{6.25}$$
$$e^{i\theta} = e^{i(\theta + 2k\pi)},\ k \in \mathbb{Z} \tag{6.26}$$
$$\forall z \in \mathbb{C},\ z = |z|e^{iArg(z)}. \tag{6.27}$$

Demostremos la propiedad (6.25):

$$\begin{aligned} e^{ix} \cdot e^{iy} &= (cosx + isenx)(cosy + iseny) \\ &= (cosxcosy - senxseny) + (cosysenx + cosxseny)i \\ &= cos(x + y) + isen(x + y) = e^{i(x+y)}. \end{aligned}$$

La propiedad (6.26) es directa de la propiedad anterior. En efecto:

$$e^{i(\theta+2k\pi)} = e^{i\theta}e^{i2k\pi}$$
$$= e^{i\theta}(cos2k\pi + isen2k\pi)$$
$$= e^{i\theta}(1+i0) = e^{i\theta}.$$

Demostremos (6.27), sabemos que podemos escribir z en su forma polar, $z = |z|(cos\theta + isen\theta)$. Se obtiene el resultado considerando el ángulo $\theta = Arg(z)$ y la definición de la función φ ■

6.1.4. Potencias complejas.

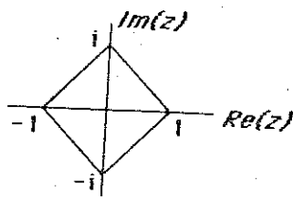
Definamos por recurrencia las potencias de un número complejo: $z^0 = 1, z^n = zz^{n-1}$. A modo de ejercicio, tomemos el conjunto de las potencias de la unidad imaginaria, i:

$$< i >= \{i^k / k \in \mathbb{Z}\}.$$

Se tiene que $i^0 = 1, i^1 = i, i^2 = -1, i^3 = -i, i^4 = 1$ y para las potencias negativas:

$$i^{-1} = \frac{1}{i} = \frac{i}{i^2} = -i$$
$$i^{-2} = \frac{1}{i^2} = -1$$
$$i^{-3} = \frac{-1}{i} = i$$
$$i^{-4} = 1.$$

Luego, $< i >= \{1, -1, i, -i\}$. Concluímos, entonces, que $(< i >, \cdot)$ es un grupo cíclico, luego abeliano, generado por i.



Utilizando la definición de potencia y las propiedades de e^{iz}, se obtiene la *identidad de De Moivre*:

$$\forall n \in \mathbb{N}, \quad (cosx + isenx)^n = cosnx + isennx. \tag{6.28}$$

En efecto, la identidad (6.28) es equivalente a

$$(e^{ix})^n = e^{inx}. \tag{6.29}$$

Demostremos (6.29) por inducción sobre n: trivialmente, se verifica para $n = 0$ (obtenemos $1 = 1$). Supongamos cierto para n y demostremos para $n+1$:

$$(e^{ix})^{n+1} = e^{ix}(e^{ix})^n = e^{ix}e^{inx} = e^{i(n+1)x}$$ ■

6.1.5. Raíces n-ésimas de un complejo.

Diremos que $w \in \mathbb{C}$ es una *raíz n-ésima* de $z \in \mathbb{C}$, $n \geq 1$ si y sólo si:

$$w^n = z \qquad (\text{formalmente } w = \sqrt[n]{z}). \tag{6.30}$$

Se tiene el teorema siguiente:

Todo complejo $z \neq 0$ tiene exactamente n raíces n-ésimas

$$w_k = \sqrt[n]{|z|}e^{i(\frac{\theta+2k\pi}{n})}, \quad 0 \leq k \leq n-1, \theta = Argz. \tag{6.31}$$

Demostración: Sea $w = |w|e^{i\phi}$ candidato a raíz n-ésima de $z = |z|e^{i\theta}$:

$$w^n = z \Leftrightarrow |w|^n e^{in\phi} = |z|e^{i\theta},$$

de donde:

$$|w|^n = |z| \text{ y } n\phi = \theta + 2k\pi.$$

Como $z \neq 0, |z| > 0$ y $|w| > 0$:

$$|w| = \sqrt[n]{|z|} \text{ y } \phi = \frac{\theta + 2k\pi}{n}.$$

Luego, los complejos candidatos a raíces son de la forma:

$$w_k = \sqrt[n]{|z|}e^{i(\frac{\theta+2k\pi}{n})}, \quad \forall k \in \mathbb{N}.$$

En efecto, es directo que:

$$w_k^n = |z|e^{(\theta+2k\pi)i} = |z|e^{\theta i}e^{2k\pi i} = |z|e^{\theta i} = z.$$

Además, $\forall k \in \mathbb{N}$:

$$w_{k+n} = \sqrt[n]{|z|}\ e^{i(\frac{\theta+2(k+n)\pi}{n})}$$
$$= \sqrt[n]{|z|}\ e^{i(\frac{\theta+2k\pi}{n})} = w_k.$$

Luego, las únicas raíces eventualmente distintas son $w_o, w_1, ..., w_{n-1}$, asociadas a los argumentos $\frac{\theta}{n}, \frac{\theta+2\pi}{n}, ..., \frac{\theta+2(n-1)\pi}{n}$.
Verifiquemos que estas raíces son distintas. Supongamos: $w_k = w_{k'}$, $0 \leq k, k' \leq n-1$ entonces:

$$e^{\frac{\theta+2k\pi}{n}i} = e^{\frac{\theta+2k'\pi}{n}i}$$

$$\Leftrightarrow \quad \frac{\theta+2k\pi}{n} = \frac{\theta+2k'\pi}{n} + 2\ell\pi, \quad \ell \in \mathbb{N}$$

$$2k\pi = 2k'\pi + 2\ell n\pi, \qquad \ell \in \mathbb{N}$$

$$k = k' + \ell n, \qquad \ell \in \mathbb{N},$$

pero $k \leq n-1$, de donde:

$$k' + \ell n \leq n-1 < n \Rightarrow \ell = 0, \text{ luego } k = k' \quad \blacksquare$$

Si $z = 0$, la ecuación $w^n = 0$ tiene $w = 0$ como la única raíz, ya que $\mathbb{C}$ es un cuerpo y, por ende, no posee divisores del cero.

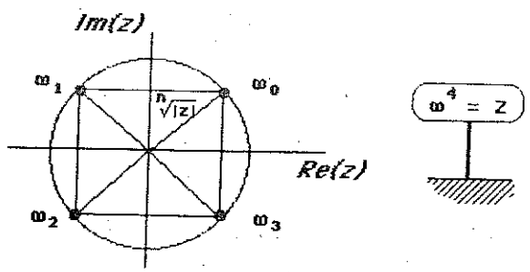
Otra particularidad de las raíces de z es:

$$|w_k| = |\sqrt[n]{|z|}\, e^{i(\frac{\theta+2k\pi}{n})}| = \sqrt[n]{|z|}\, |e^{i(\frac{\theta+2k\pi}{n})}|$$

$$= \sqrt[n]{|z|}\{cos^2(\frac{\theta+2k\pi}{n}) + sen^2(\frac{\theta+2k\pi}{n})\} = \sqrt[n]{|z|},$$

en otras palabras, el módulo de las raíces es constante, igual a la raíz n-ésima del módulo de z.

Podemos afirmar que todas las raíces se encuentran en los vértices de un polígono regular, inscrito en el círculo centrado en el origen $(0,0)$ y de radio $\sqrt[n]{|z|}$:



Como caso particular se tienen las *raíces de la unidad*:

$$w^n = 1 \Rightarrow w_k = e^{\frac{i2\pi k}{n}}, \quad k = 0, ..., n-1, \tag{6.32}$$

luego $|w_k| = 1$, es decir las raíces se encuentran sobre el círculo unitario. Además, si denominamos $U_n = \{w_k\}_{k=0}^{n-1}$. La estructura $(U_n, \cdot)$ es un grupo abeliano, isomorfo al grupo de congruencias módulo n:

$$(U_n, \cdot) \cong (\mathbb{Z}_n, \oplus).$$

En efecto, consideremos la función:

$$\phi : U_n \to \mathbb{Z}_n$$
$$w_k \mapsto [k].$$

ϕ es claramente biyectiva, además:

$$\phi(w_k \cdot w_{k'}) = \phi(e^{i\frac{2\pi}{n}(k+k')}) = [k+k']$$
$$= [k] \oplus [k'] = \phi(w_k) \oplus \phi(w_{k'}) \quad \blacksquare$$

De esta isomorfía concluímos también que $(U_n, \cdot)$ es un grupo cíclico generado por w_1, ya que $(\mathbb{Z}_n, \oplus)$ es cíclico, generado por la clase [1].

Veamos, mediante un ejemplo, cómo aprovechar las raíces de un número complejo para determinar soluciones de ecuaciones polinomiales. Sea la ecuación:

$$x^{12} - 65x^6 + 64 = 0.$$

Mediante el cambio de variables $z = x^6$, obtenemos

$$z^2 - 65z + 64 = 0,$$

cuyas raíces son $z_1 = 64, z_2 = 1$. Debemos resolver $(x^6 = 64) \wedge (x^6 = 1)$. Las soluciones son, para la primera y segunda ecuación respectivamente,

$$z_k = \sqrt[6]{64}e^{i(\frac{\theta+2k\pi}{6})}, \qquad w_k = e^{\frac{i2k\pi}{6}}, \qquad 0 \leq k \leq 5,$$

donde θ es el ángulo asociado a la expresión de $64 = 64(cos\theta + isen\theta)$, luego $\theta = 0$, obteniéndose las 12 raíces:

$$z_k = 2e^{\frac{i2k\pi}{6}}, w_k = e^{\frac{i2k\pi}{6}}, \quad 0 \leq k \leq 5 \quad \blacksquare$$

6.2 El anillo de los polinomios.

Sea $(\mathcal{K}, +, \cdot)$ un cuerpo. Denominamos *polinomio* con coeficientes en $\mathcal{K}$, en la *indeterminada o letra* x, la expresión formal:

$$p(x)=a_0 + a_1 x + a_2 x^2 + ... + a_n x^n = \sum_{i=0}^{n} a_i x^i, \quad n \in I\!N, \quad a_i \in \mathcal{K}, \quad i = 1, ..., n.$$

Notaremos $\mathcal{K}[x]$, al conjunto de todos los polinomios sobre el cuerpo $\mathcal{K}$ en la indeterminada x.

Los polinomios así definidos son objetos formales. La letra x no debe interpretarse a priori como una incógnita o una variable que toma valores en el cuerpo $\mathcal{K}$.

Diremos que dos polinomios:

$$p(x) = \sum_{j=0}^{n} a_j x^j, \quad q(x) = \sum_{j=0}^{m} b_j x^j$$

son *iguales* si y sólo si:

$$(n = m) \wedge (a_j = b_j, \ \forall j = 1, ..., n). \tag{6.33}$$

Ahora bien, si tenemos dos polinomios p, q iguales (idénticos coeficientes), es claro que $\forall c \in \mathcal{K}$, $p(c) = q(c)$, es decir coinciden como funciones. La propiedad inversa no es necesariamente cierta. Sea, por ejemplo, $\mathcal{K} = \mathbb{Z}_2$ el cuerpo de las clases de equivalencia módulo dos, y consideremos los polinomios, $p = x^4 \oplus x, q = x^3 \oplus x$. Es claro que $p \neq q$ como objeto formal, pues los coeficientes son distintos:

$$p(x) = 1 \cdot x^4 \oplus 0 \cdot x^3 \oplus 0 \cdot x^2 \oplus 1 \cdot x \oplus 0$$

$$q(x) = 0 \cdot x^4 \oplus 1 \cdot x^3 \oplus 0 \cdot x^2 \oplus 1 \cdot x \oplus 0;$$

sin embargo, son iguales al considerarlos como funciones de $\mathbb{Z}_2$ en sí mismo:

$$p(0) = 0^4 \oplus 0 = 0 = 0^3 \oplus 0 = q(0)$$

$$p(1) = 1^4 \oplus 1 = 0 = 1^3 \oplus 1 = q(1).$$

Más adelante veremos que si $\mathcal{K}$ es de cardinalidad infinita, se tiene que si dos polinomios son funcionalmente iguales (idéntica evaluación), también lo son a nivel formal (coeficientes iguales).

Algunos ejemplos de polinomios son los siguientes:

- El polinomio "nulo", $0 + 0x + 0x^2 + ...$, donde 0 es el neutro aditivo en $\mathcal{K}$.
  El polinomio "unidad", $1 + 0x + 0x^2 + ...$, donde 1 es el neutro multiplicativo en $\mathcal{K}$.
- El polinomio "constante" $\lambda \in \mathcal{K}$, $(a_o = \lambda, a_i = 0, \quad \forall i \geq 1)$.
- El polinomio "lineal", $a + bx; a, b \in \mathcal{K}, b \neq 0$.
- En $(I\!R, +, \cdot)$, $1 - x + 2.5x^3 - x^4$ es un polinomio con coeficientes reales $a_o = 1, a_1 = -1, a_2 = 0, a_3 = 2.5, a_4 = -1$.

Para dotar $\mathcal{K}[x]$ de una estructura algebraica definimos la suma y multiplicación de polinomios como sigue:

Consideremos $p, q \in \mathcal{K}[x], p(x) = \sum_{j=0}^{n} a_j x^j, q(x) = \sum_{j=0}^{m} b_j x^j$. Sin pérdida de generalidad, supongamos $m \leq n$ y que $b_i = 0, \forall i > m$. Se define la suma de ambos polinomios $p + q$, como la expresión:

$$(p + q)(x) = \sum_{i=0}^{n} (a_i + b_i) x^i \in \mathcal{K}[x]. \tag{6.34}$$

Es directo de la definición que la suma de polinomios es una ℓ.c.i. en $\mathcal{K}[x]$.

La multiplicación $p \cdot q$, se define como sigue:

$(p \cdot q)(x) = a_0 b_0 + ... + (a_0 b_k + a_1 b_{k-1} + ... + a_k b_0) x^k + ... + a_n b_m x^{n+m}$
o de manera equivalente:

$$(p \cdot q)(x) = \sum_{k=0}^{n+m} c_k x^k; \quad c_k = \sum_{i=0}^{k} a_i b_{k-i}, \quad 0 \leq k \leq n + m. \tag{6.35}$$

Observemos que el coeficiente $c_{n+m} = a_0 b_{n+m} + a_1 b_{n+m-1} + ... + a_n b_m$ $+ a_{n+1} b_{m-1} + ... + a_{n+m} b_0$ se reduce a $a_m b_m$ pues $a_i = b_j = 0$, $\forall i > n$ y $\forall j > m$.

Señalemos que, si pensamos en la multiplicación de dos polinomios, interpretando la indeterminada x como un elemento del cuerpo $\mathcal{K}$, se tiene

$$(p \cdot q)(x) = (\sum_{i=1}^{n} a_i x^i)(\sum_{j=1}^{m} b_j x^j) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i b_j x^{i+j};$$

vemos, entonces, que las operaciones "formales" definidas en $\mathcal{K}[x]$ coinciden con la multiplicación y suma de expresiones algebraicas usuales.

De estas dos operaciones concluímos que:

$$(\mathcal{K}[x], +, \cdot) \text{ es un } \textit{anillo conmutativo con unidad.} \tag{6.36}$$

En efecto:

$(\mathcal{K}[x], +)$ es un grupo abeliano:

- La asociatividad y conmutatividad de la suma es directa de las propiedades de $(\mathcal{K}, +)$.
- $O(x) = 0 + 0x + 0x^2 + ...$, es el elemento neutro.
- Dado $p(x) = \sum_{i=0}^{n} a_i x^i$, su inverso es $-p$, donde $(-p)(x) = \sum_{i=0}^{n} (-a_i)x^i$.

La multiplicación es asociativa y conmutativa:

$$\begin{aligned} p(x)\ (q(x)r(x)) &= (\sum_{i=0}^{n} a_i x^i)\left((\sum_{j=0}^{m} b_j x^j)(\sum_{k=0}^{s} c_k x^k)\right) \\ &= \sum_{i=0}^{n}\sum_{j=0}^{m}\sum_{k=0}^{s} a_i b_j c_k x^{i+j+k} \\ &= (\sum_{i=0}^{n}\sum_{j=0}^{m} a_i b_j x^{i+j})(\sum_{k=0}^{s} c_k x^k) \\ &= \left((\sum_{i=0}^{n} a_i x^i)(\sum_{j=0}^{m} b_j x^j)\right)(\sum_{k=0}^{s} c_k x^k) \\ &= (p(x)q(x))\ r(x). \end{aligned}$$

La conmutatividad de $\cdot$ se verifica de manera análoga.

La multiplicación admite el polinomio neutro (unidad):

$$\mathbb{1}(x) = 1 + 0x + 0x^2 + ...$$

La multiplicación distribuye con respecto a la suma:

$$p(x)(q(x) + r(x)) = (\sum_{i=0}^{n} a_i x^i)(\sum_{j=0}^{m} b_j x^j + \sum_{k=0}^{s} c_k x^k),$$

suponiendo $m \geq s$ y $c_k = 0 \quad \forall k > s$ y aplicando la definición de multiplicación:

$$= (\sum_{i=0}^{n} a_i x^i)(\sum_{j=0}^{m} (b_j + c_j)x^j) = \sum_{k=0}^{m+n} d_k x^k,$$

donde $d_k = \sum_{i=0}^{k} a_i(b_{k-i} + c_{k-i})$, luego

$$\begin{aligned} p(x)(q(x) + r(x)) &= \sum_{k=0}^{m+n}(\sum_{i=0}^{k} a_i(b_{k-i} + c_{k-i}))x^k \\ &= \sum_{k=0}^{m+n}(\sum_{i=0}^{k} a_i b_{k-i})x^k + \sum_{k=0}^{m+n}(\sum_{i=0}^{k} a_i c_{k-i})x^k \\ &= p(x)q(x) + p(x)r(x). \end{aligned}$$

Hemos así verificado que $(\mathcal{K}[x], +, \cdot)$ es un anillo conmutativo con unidad ■

Dado $p \in \mathcal{K}[x]$ definimos su *grado*, que notamos $gr(p)$, como el exponente de la mayor potencia con coeficiente no nulo (distinto del neutro aditivo de $\mathcal{K}$) que aparece en la expresión formal de p. Por ejemplo, en $\mathbb{R}[x]$:

$$p(x) = -2 + x^3 - 3x^5 - 3x^7, \quad gr(p) = 7.$$

Si $gr(p) = 0$ entonces $p(x) = a_0 x^0 = a_0$, es un polinomio constante. Como convención, diremos que el grado del polinomio nulo O, es $-\infty$, $gr(O) = -\infty$, entendiendo que $-\infty + (-\infty) = -\infty$ y $-\infty + n = -\infty \quad \forall n \in \mathbb{N}$.

Dado un polinomio de grado n, $p(x) = \sum_{i=0}^{n} a_i x^i$, $a_n \neq 0$, diremos que es *mónico* si $a_n = 1$.

Dos propiedades del grado de un polinomio son los siguientes (verifique):

$$gr(p + q) \leq max(gr(p), gr(q)) \tag{6.37}$$
$$gr(p \cdot q) = gr(p) + gr(q). \tag{6.38}$$

Por ejemplo, en $\mathbb{R}[x]$:

$$p(x) = -1 + x^2 - 3x^3$$
$$q(x) = -2x^2 + 3x^3$$

$$p(x)+q(x) = -1-x^2$$
$$p(x)q(x) = 2x^2-3x^3-2x^4+9x^5-9x^6,$$

de donde: $gr(p+q) = 2 < 3 = max(gr(p), gr(q))$ $\quad gr(p\cdot q) = 6 = gr(p) + gr(q)$.

De la propiedad (6.38) se deduce que

$$(\mathcal{K}[x], +, \cdot) \textit{ no tiene divisores del cero.} \tag{6.39}$$

En efecto, dados $p, q \in \mathcal{K}[x]$. Supongamos $p(x)q(x) = O$ luego $gr(p) + gr(q) = gr(O) = -\infty$, de donde necesariamente $gr(p) = -\infty$ o $gr(q) = -\infty$. Es decir, $p = O$ o $q = O$ ∎

6.2.1. División de polinomios.

De manera análoga a la divisibilidad entre enteros, dados dos polinomios no nulos $f, g \in \mathcal{K}[x]$, diremos que g *divide* f, notando $g|f$ si y sólo si existe un polinomio $h \in \mathcal{K}[x]$ tal que:

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

También se dice que $g(x)$ es un factor de $f(x)$.

Se tienen las dos propiedades elementales:

$$g|f \Rightarrow \forall \lambda \in \mathcal{K}[x] \setminus \{0\}, \text{ polinomio constante, } \lambda g|f \tag{6.40}$$
$$g|f \Rightarrow \forall \lambda \in \mathcal{K}[x],\ g|(\lambda f). \tag{6.41}$$

En efecto: sabemos que $f(x)=h(x)g(x)$, de donde $f(x)=(\frac{1}{\lambda}h(x)))(\lambda g(x))$ y $(\lambda f)(x) = (\lambda q(x))g(x)$ ∎

Ejemplos: En $\mathbb{R}[x]$, $(x-1)|(x^2-1)$, en $\mathbb{C}[x], (x+i)|(x^2+2ix-1)$.

De manera análoga al algoritmo de división de enteros, podemos dividir polinomios, mediante la propiedad:

Dados $f, g \in \mathcal{K}[x], g \neq O$, existen $q, r \in \mathcal{K}[x]$ únicos, tales que:

$$f(x) = q(x)g(x) + r(x), \qquad gr(r) < gr(g). \tag{6.42}$$

El polinomio q se denomina el *cociente* y r el *resto* de f.

Demostremos esta propiedad:

Claramente, si $gr(f) < gr(g)$ se tiene $f(x) = 0 \cdot g(x) + f(x)$. Es decir $q(x) = 0, r(x) = f(x)$.

Supongamos entonces $gr(f) \geq gr(g)$ y demostremos la propiedad por inducción sobre el grado de f.

1. Si $gr(f) = 0 \Rightarrow f(x) = \lambda \in K$ y $gr(g) = 0$ (pues $g \neq O$). Obteniendo la factorización
$$\lambda = f(x) = \frac{\lambda}{g(x)}g(x) + O(x).$$

Supongamos que la propiedad se verifica para $gr(f) < n$ y demostremos para $gr(f) = n$. Tenemos

$$f(x) = \sum_{i=0}^{n} a_i x^i, \quad a_n \neq 0$$
$$g(x) = \sum_{i=0}^{m} b_i x^i \quad b_m \neq 0; \quad m \leq n.$$

Sea

$$h(x) = f(x) - (a_n b_m^{-1})x^{n-m}g(x) \tag{6.43}$$
$$= \sum_{i=0}^{n} a_i x^i - (a_n b_m^{-1})x^{n-m}\sum_{i=0}^{m} b_i x^i$$
$$= \sum_{i=0}^{n} a_i x^i - (a_n b_m^{-1})x^{n-m}(b_0 + b_1 x + \ldots + b_m x^m)$$
$$= \sum_{i=0}^{n} a_i x^i - (a_n b_m^{-1})b_0 x^{n-m} - \ldots - a_n b_m^{-1} b_{m-1} x^{n-1} - a_n x^n$$
$$h(x) = \sum_{i=0}^{n-1} a_i x^i - a_n b_m^{-1}(\sum_{i=0}^{m-1} b_i x^{n-m+i}),$$

luego, $h \in \mathcal{K}[x]$ y $gr(h) \leq n-1$.

Podemos, entonces, aplicar la hipótesis de inducción al polinomio h, de grado $n-1$: Es decir, existen polinomios $q_1, r_1 \in \mathcal{K}[x]$, tales que:

$$h(x) = q_1(x)g(x) + r_1(x), \qquad gr(r_1) < gr(g).$$

Sustituyendo en (6.43):

$$f(x) = q_1(x)g(x) + r_1(x) + (a_n b_m^{-1})x^{n-m}g(x),$$

de donde

$$f(x) = (q_1(x) + a_n b_m^{-1} x^{n-m})g(x) + r_1(x) \qquad gr(r_1) < gr(g).$$

Notando $q(x) = q_1(x) + a_n b_m^{-1} x^{n-m}$, $r(x) = r_1(x)$, obtenemos la factorización de f ∎

Demostremos ahora la unicidad:

Supongamos $f(x) = q(x)g(x) + r(x) = q'(x)g(x) + r'(x)$, $gr(r) < gr(g)$ y $gr(r') < gr(g)$. Se tiene entonces:

$$r(x) - r'(x) = (q'(x) - q(x))g(x).$$

Si $r(x) - r'(x) \neq 0 \Rightarrow gr(r - r') = gr((q' - q)g) \geq gr(g)$. Por otra parte, sabemos que

$$gr(r - r') \leq max(gr(r), gr(r')) < gr(g),$$

lo cual es una contradicción con la desigualdad anterior, de donde concluímos $r = r'$, obteniendo:

$$(q'(x) - q(x))g(x) = O(x).$$

Como $g \neq O$ y $\mathcal{K}[x]$ no tiene divisores del cero, concluímos $q = q'$ ∎

Es directo del algoritmo de división que

$$g|f \text{ } \textit{si y sólo si la división por } g \textit{ tiene resto nulo.} \qquad (6.44)$$

Ejemplo 1: Tomemos $f, g \in \mathbb{R}[x]$:

$$f(x) = x^5 - x^4 - 6x^3 - 2x^2 + 5x + 3$$
$$g(x) = x^3 - 3x - 2$$

$$\begin{array}{l} x^5 - x^4 - 6x^3 - 2x^2 + 5x + 3 : x^3 - 3x - 2 = x^2 - x - 3 \\ \underline{x^5 \quad - 3x^3 - 2x^2} \\ 0 - x^4 - 3x^3 + 0 + 5x + 3 \\ \underline{\quad -x^4 \quad + 3x^2 + 2x} \\ 0 - 3x^3 - 3x^2 + 3x + 3 \\ \underline{\quad -3x^3 \quad + 9x + 6} \\ 0 \quad -3x^2 - 6x - 3 \end{array}$$

Luego: $q(x) = x^2 - x - 3$, $r(x) = -3x^2 - 6x - 3$.

$$f(x) = q(x)g(x) + r(x), \quad gr(r) = 2 < gr(g) = 3. \text{ ∎}$$

Ejemplo 2: Consideremos los polinomios $f(x) = x^n - a^n, g(x) = x - a$ en $\mathcal{K}[x]$. Se tiene:

$$x^n - a^n : x - a = x^{n-1} + ax^{n-2} + ... + a^i x^{n-(i+1)} + ... + a^{n-2}x + a^{n-1}$$

$$\begin{array}{l} \underline{x^n - ax^{n-1}} \\ ax^{n-1} - a^n \\ \underline{ax^{n-1} - a^2 x^{n-2}} \\ a^2 x^{n-2} - a^n \\ \vdots \\ \underline{a^i x^{n-i} - a^n} \\ a^i x^{n-i} - a^{i+1} x^{n-(i+1)} \\ \underline{a^{i+1} x^{n-(i+1)} - a^n} \\ \vdots \\ \underline{a^{n-2} x^2 - a^n} \\ a^{n-2} x^2 - a^{n-1} x \\ \underline{a^{n-1} x - a^n} \\ a^{n-1} x - a^n \\ \underline{a^{n-1} x - a^n} \\ 0 + 0 \end{array}$$

Luego, $(x - a)|(x^n - a^n)$ o, en $\mathbb{R}[x]$:

$$\frac{x^n - a^n}{x - a} = \sum_{j=0}^{n-1} a^j x^{n-1-j}.$$

También es posible verificar la propiedad anterior sin aplicar el algoritmo de división. En efecto:

$$(x - a)(x^{n-1} + ax^{n-2} + a^2 x^{n-3} + ... + a^{n-2}x + a^{n-1})$$

$$= \sum_{j=0}^{n-1} (x - a)a^j x^{n-1-j} = \sum_{j=0}^{n-1} (a^j x^{n-j} - a^{j+1} x^{n-1-j})$$

$$= \sum_{j=0}^{n-1} (a^j x^{n-j} - a^{j+1} x^{n-(j+1)}).$$

Utilizando la propiedad telescópica:

$$(x-a)\sum_{j=0}^{n-1} a^j x^{n-(j+1)} = x^n - a^n \quad \blacksquare$$

6.2.2. Máximo común divisor de dos polinomios.

Dados los polinomios $f, g \in \mathcal{K}[x]$, se dirá que el polinomio $mcd(f,g)$ es el *máximo común divisor* de f y g si y sólo si:

$$(mcd(f,g)|f) \wedge (mcd(f,g)|g) \tag{6.45}$$
$$\text{Si } \exists h \in \mathcal{K}[x], h|f \wedge h|g \Rightarrow h|mcd(f,g) \tag{6.46}$$
$$mcd(f,g) \text{ es mónico.} \tag{6.47}$$

De manera análoga, el estudio realizado para calcular el máximo común divisor entre dos enteros, podemos utilizar, en el contexto de polinomios, el algoritmo de Euclides:

Si $gr(g) \leq gr(f)$

$$\begin{aligned}
f &= g\cdot q_1 + r_1 && gr(r_1) < gr(g)\\
g &= r_1 q_2 + r_2 && gr(r_2) < gr(r_1)\\
r_1 &= r_2 q_3 + r_3 && gr(r_3) < gr(r_2)\\
&\vdots && \vdots\\
r_{n-2} &= r_{n-1} q_n + r_n && gr(r_n) < gr(r_{n-1})\\
r_{n-1} &= r_n q_{n+1}.
\end{aligned}$$

donde $r_n = mcd(f,g)$.

La demostración es análoga a la de números enteros. Para verificar la condición (6.47), basta dividir por un polinomio constante (elemento del cuerpo $\mathcal{K}$) al final del proceso.

Calculemos, por ejemplo, el polinomio el $mcd(6x^3+2x+8, 2x^3-x^2+3)$:

$$6x^3 + 2x + 8 : 2x^3 - x^2 + 3 = 3$$
$$\underline{6x^3 - 3x^2 + 9}$$
$$3x^2 + 2x - 1,$$

obteniendo, $6x^3 + 2x + 8 = 3\cdot(2x^3 - x^2 + 3) + (3x^2 + 2x - 1)$. De manera análoga:

$$x^3 - x^2 + 3 : 3x^2 + 2x - 1 = \tfrac{2}{3}x - \tfrac{7}{9}$$
$$\underline{2x^3 + \tfrac{4}{3}x^2 - \tfrac{2}{3}x}$$
$$\underline{-\tfrac{7}{3}x^2 + \tfrac{2}{3}x + 3}$$
$$\underline{-\tfrac{7}{3}x^2 - \tfrac{14}{9}x + \tfrac{7}{9}}$$
$$\tfrac{20}{9}x + \tfrac{20}{9}$$

luego, $2x^3 - x^2 + 3 = (\tfrac{2}{3}x - \tfrac{7}{9})(3x^2 + 2x - 1) + (\tfrac{20}{9}x + \tfrac{20}{9})$

$$3x^2 + 2x - 1 : \tfrac{20}{9}x + \tfrac{20}{9} = \tfrac{27}{20}x - \tfrac{9}{20}$$
$$\underline{3x^2 + 3x}$$
$$\underline{-x - 1}$$
$$\underline{-x - 1}$$
$$0$$

de donde, $3x^2 + 2x - 1 = (\tfrac{27}{20}x - \tfrac{9}{20})(\tfrac{20}{9}x + \tfrac{20}{9})$.

El último resto no nulo es: $\tfrac{20}{9}x + \tfrac{20}{9}$, el cual verifica las condiciones (6.45) y (6.46) necesarias para el *mcd*, pero no es mónico. Recordando que si $r|p \Rightarrow \lambda r|p$, basta considerar $\tfrac{9}{20}(\tfrac{20}{9}x + \tfrac{20}{9}) = x + 1$, que por ser mónico, y satisfacer (6.45) y (6.46), es el máximo común divisor.

6.2.3. Raíces de polinomios.

Uno de los problemas más importantes relacionado con un polinomio es determinar los elementos $c \in \mathcal{K}$ que lo anulan: dado $\sum_{i=1}^{n} a_i x^i \in \mathcal{K}[x]$, determinar $c \in \mathcal{K}$ tal que $\sum_{i=0}^{n} a_i c^i = 0 \in \mathcal{K}$. Hasta ahora hemos trabajado con un polinomio en términos formales (en función de la letra x). Sin embargo, en la noción anterior reemplazamos x por un elemento específico, c, del cuerpo $\mathcal{K}$. Hemos considerado entonces los valores de $\mathcal{K}$ que anulan el polinomio, visto éste como una función de $\mathcal{K}$ en sí mismo. En este contexto, diremos que:

$$c \in \mathcal{K} \textit{ es raíz del polinomio } p \in \mathcal{K}[x] \textit{ si y sólo si } p(c) = 0. \tag{6.48}$$

Un resultado importante de factorización de polinomios, que relaciona la divisibilidad con el concepto de raíz, es el siguiente:

Dado el cuerpo $(\mathcal{K},+,\cdot)$, $f \in \mathcal{K}[x]$, $a \in \mathcal{K}$, *entonces existe un único polinomio* $q \in \mathcal{K}[x]$ *tal que:*

$$f(x) = (x-a)q(x) + f(a). \tag{6.49}$$

La demostración es simple y consiste en aplicar el algoritmo de la división a f dividido por el polinomio lineal, $x-a$:

$$f(x) = (x-a)q(x) + r(x), \quad gr(r) < gr(x-a) = 1.$$

Luego, $gr(r) \leq 0$. Supongamos $r(x) = \lambda \in \mathcal{K}$. Se tiene entonces $f(x) = (x-a)q(x) + \lambda$. Evaluando en $x = a$:

$$f(a) = (a-a)q(a) + \lambda \Rightarrow \lambda = f(a) \quad \blacksquare$$

De este resultado se obtiene el corolario

$$x - a | f \Leftrightarrow a \text{ es raíz de } f \tag{6.50}$$

En efecto, $x-a|f \Rightarrow f(x) = (x-a)q(x) \Rightarrow f(a) = 0$. En el otro sentido, si $f(a) = 0$, se obtiene la factorización directamente del resultado anterior $\blacksquare$

Un resultado más fuerte en cuanto a las raíces de un polinomio es el siguiente:

Sea $f \in \mathcal{K}[x]$ *un polinomio de grado* $n \geq 0$. *Entonces* f *tiene, a lo más* n *raíces en el cuerpo* $\mathcal{K}$. (6.51)

La demostración la realizaremos por inducción sobre el grado de f.

Si $gr(f) = 0 \Rightarrow f(x) = \lambda \in \mathcal{K}, \lambda \neq 0$ (si no $gr(f) = -\infty$), luego f no tiene raíces en $\mathcal{K}$, es decir, un polinomio de grado 0 tiene 0 raíces.

Si $gr(f) = 1 \Rightarrow f(x) = a + bx$, $b \neq 0$, luego:

$$f(x) = 0 \Leftrightarrow a + bx = 0$$

de donde $x = (-a)b^{-1} \in \mathcal{K}$, es la única raíz en $\mathcal{K}$. (¿Por qué es única? Recuerde las propiedades de inversos en un grupo).

Supongamos que el resultado es verdadero para polinomios de grado $n-1 \geq 1$ y sea $gr(f) = n$.

Si f admite una raíz $a \in \mathcal{K}$, sabemos que (ver (6.50)):

$$f(x) = (x-a)q(x), \quad gr(q) = n-1.$$

Luego, cualquier raíz $r \neq a$ del polinomio f, debe ser necesariamente raíz de q:

$$0 = f(r) = (r-a)q(r),$$

de donde $q(r) = 0$, ya que $\mathcal{K}$ no tiene divisores del cero.

Por hipótesis de inducción q tiene, a lo más, $n-1$ raíces en $\mathcal{K}$, concluyendo que f tiene, a lo más, n $\blacksquare$

Del resultado anterior se desprenden las propiedades siguientes:

Si dos polinomios de grado n *en* $\mathcal{K}[x]$ *coinciden en* $n+1$ *valores, entonces son iguales:*

$$f(a_i) = g(a_i), \quad i = 1,...,n+1 \;\Rightarrow\; f = g. \tag{6.52}$$

Si $\mathcal{K}$ *es un cuerpo de cardinalidad infinita, dados* $f(x) = \sum_{i=0}^{n} a_i x^i, g(x) = \sum_{i=0}^{n} b_i x^i$:

$$(f(c) = g(c))(\forall c \in \mathcal{K}) \Rightarrow (a_i = b_i)\ (\forall i = 0,...,n). \tag{6.53}$$

Demostremos estas propiedades:

(6.52) El polinomio $h(x) = f(x) - g(x)$, que es a lo más de grado n, tiene al menos $n+1$ raíces, $(h(a_i) = 0,\ i = 1,...,n+1)$ luego, necesariamente $h = O$, es decir $f = g$.

(6.53) Se tiene $f(c) - g(c) = \sum_{i=0}^{n}(a_i - b_i)c^i = 0$, $\forall c \in \mathcal{K}$. Luego el polinomio $\sum_{i=0}^{n}(a_i - b_i)x^i$ tiene infinitas raíces (ya que $\mathcal{K}$ es infinito). Ergo es el polinomio nulo, es decir: $a_i - b_i = 0, \quad \forall i = 1,...,n$ $\blacksquare$

Recordemos que dos polinomios p, q, pueden coincidir como funciones; $(p(c) = q(c))(\forall c \in \mathcal{K})$, pero no como expresiones formales (p y q pueden tener asociados coeficientes distintos). Por ejemplo, en el cuerpo $(\mathbb{Z}_3, \oplus, \cdot)$, los polinomios $p(x) = x^4 \oplus x \oplus 1, q(x) = x^3 \oplus x^2 \oplus 1$ son distintos como

expresiones en la indeterminada x (coeficientes diferentes), pero son iguales como funciones:

$$p(0) = 0^4 \oplus 0 \oplus 1 = 1 = 0^3 \oplus 0^2 \oplus 1 = q(0)$$
$$p(1) = 1^4 \oplus 1 \oplus 1 = 0 = 1^3 \oplus 1^2 \oplus 1 = q(1)$$
$$p(2) = 2^4 \oplus 2 \oplus 1 = 1 \oplus 2 \oplus 1 = 1 = 2^3 \oplus 2^2 \oplus 1 = 2 \oplus 1 \oplus 1 = q(2).$$

El problema de determinar si un polinomio tiene o no raíces sobre un cuerpo (existencia de soluciones) ha sido crucial en el desarrollo del álgebra y nada de fácil. A continuación enunciamos, sin demostración, el *teorema de d'Alembert o teorema fundamental del álgebra*, el cual da una respuesta a este problema en el cuerpo $\mathbb{C}$, de los números complejos:

Teorema fundamental del álgebra:

$$\forall p \in \mathbb{C}[x],\ gr(p) \geq 1,\ \exists z \in \mathbb{C},\ p(z) = 0 \qquad (6.54)$$

de manera equivalente:

cualquier polinomio de grado ≥ 1 con coeficientes complejos admite, al menos, una raíz en $\mathbb{C}$.

La demostración de este teorema está fuera del alcance de los conocimientos desarrollados en este libro. Los fanáticos pueden "aproximarse" a las demostraciones de existencia de raíces leyendo el caso particular desarrollado en el tema "Raíces", al final del capítulo.

De este teorema se deduce el corolario:

cualquier polinomio, $f \in \mathbb{C}[x]$, $gr(f) \geq 1$, puede factorizarse como el producto de n factores lineales (no necesariamente distintos):

$$f(x) = \lambda \prod_{i=1}^{n} (x - z_i); \quad \lambda, z_i \in \mathbb{C}; i = 1, ..., n. \qquad (6.55)$$

En efecto, por el *teorema fundamental*, existe $z_1 \in \mathbb{C}$ tal que $f(z_1) = 0$. Sabemos que esto es equivalente a que existe $q_1 \in P(\mathbb{C})$, tal que $f(x) = (x - z_1)q_1(x)$. Luego, por recurrencia sobre el grado del polinomio f, y aplicando reiteradamente el teorema y la propiedad de factorización, concluímos que $f(x) = \lambda(x - z_1)(x - z_2)...(x - z_n)$ ■

Desarrollemos un ejemplo de esta factorización. Sea $f(x) = 2x^3 - 8x^2 + 10x - 4 = 0$. Este polinomio admite como raíz $x_1 = 1$. Dividiendo por $x - 1$:

$$2x^3 - 8x^2 + 10x - 4 : x - 1 = 2x^2 - 6x + 4$$
$$\underline{2x^3 - 2x^2}$$
$$-6x^2 + 10x - 4$$
$$\underline{-6x^2 + 6x}$$
$$4x - 4$$
$$\underline{4x - 4}$$
$$0$$

luego, $2x^3 - 8x^2 + 10x - 4 = (x - 1)(2x^2 - 6x + 4)$

$$f(x) = 0 \Leftrightarrow (x - 1)(2x^2 - 6x + 4) = 0$$

$\Rightarrow 2x^2 - 6x + 4 = 0$, que admite 1 como raíz. Dividiendo por $x - 1$

$$2x^2 - 6x + 4 : x - 1 = 2x - 4$$
$$\underline{2x^2 - 2x}$$
$$-4x + 4$$
$$\underline{-4x + 4}$$
$$0$$

se obtiene la factorización $2x^2 - 6x + 4 = (x - 1)(2x - 4)$, de donde $f(x) = 2(x - 2)(x - 1)(x - 1)$ ■

Es directo de la demostración de la propiedad (6.55) que si un polinomio $p \in \mathcal{K}[x], gr(p) = n$, es tal que sus n raíces $\{x_1, ..., x_n\}$, están en $\mathcal{K}$, entonces

$$p(x) = \lambda(x - x_1)...(x - x_n).$$

para demostrarlo basta aplicar la recurrencia utilizada para determinar la expresión (6.55) ■

También, podemos aplicar el resultado en $\mathbb{R}[x]$, entendiendo que los coeficientes reales pueden interpretarse como números complejos con parte imaginaria nula:

$$\forall p \in \mathbb{R}[x],\ p(x) = \lambda(x - z_1)...(x - z_n),\ \lambda \in \mathbb{R},\ z_i \in \mathbb{C}. \qquad (6.56)$$

Tomemos, por ejemplo, $p(x) = x^2 + 1$. Este polinomio no tiene raíces reales, pero sí tiene dos raíces en $\mathbb{C}, x = \pm i \in \mathbb{C}$. Además puede factorizarse en $\mathbb{C}$ (no en $\mathbb{R}$) como el producto de dos polinomios lineales: $p(x) = (x - i)(x + i)$.

Lo anterior nos lleva a la noción de polinomio "no factorizable", análoga a la de número primo.

6.2.4. Polinomios irreductibles.

Dado $f \in \mathcal{K}[x], gr(f) \geq 1$, diremos que f es *irreductible* si y sólo si no es factorizable como producto de dos polinomios de grado positivo. O, de manera equivalente, un polinomio $f, gr(f) \geq 1$ es irreductible si y sólo si:

$$(\forall g, h \in \mathcal{K}[x])(f(x) = g(x)h(x)) \Rightarrow (g(x) = \lambda) \vee (h(x) = \lambda), \lambda \in \mathcal{K} \quad (6.57)$$

En caso contrario, diremos que f es *reductible*.

Ejemplos:

1. Claramente, $x^2 + 1$ es irreductible en $\mathbb{R}[x]$, pero es reductible en $\mathbb{C}[x]$: $x^2 + 1 = (x + i)(x - i)$.

2. Un polinomio lineal $p(x) = a + bx \in \mathcal{K}[x], b \neq 0$ es irreductible. En efecto:

$$a + bx = g(x)h(x) \Rightarrow gr(g(x)h(x)) = 1,$$

luego:

$$gr(g) + gr(h) = 1 \Rightarrow gr(g) = 0 \text{ o } gr(h) = 0,$$

en otras palabras, uno de los dos polinomios es constante.

De esto concluímos que un polinomio reductible en un cuerpo $\mathcal{K}$ arbitrario debe tener al menos grado 2.

3. En el cuerpo $(\mathbb{Z}_3, \oplus, \cdot)$ el polinomio $x^2 \oplus 2$ es reductible. En efecto, omitiendo por comodidad los paréntesis de las clases de equivalencia ($\dot{x} = [x]$), se tiene: $x^2 \oplus 2 = 0 \Leftrightarrow x^2 \oplus 2 \oplus 1 = 1 \Leftrightarrow x^2 \oplus 3 = 1$. Recordando que en $\mathbb{Z}_3$ $3 = [3] = [0] = 0$ obtenemos $x^2 \oplus 3 = 1 \Leftrightarrow x^2 = 1 \Leftrightarrow x \cdot x = 1$ $\Rightarrow (x = 1) \wedge (x = 2)$. Del teorema de factorización mediante raíces:

$$x^2 \oplus 2 = (x \oplus 2)(x \oplus 1).$$

4. El polinomio $p(x) = x^2 \oplus x \oplus 2$ es irreductible en $\mathbb{Z}_3$. En efecto:

(i) p no tiene raíces en $\mathbb{Z}_3$:
Si $x = 0$: $0 \oplus 0 \oplus 2 = 2 \neq 0$.
Si $x = 1$: $1 \cdot 1 \oplus 1 \oplus 2 = 1 \oplus 0 = 1 \neq 0$.
Si $x = 2$: $2 \cdot 2 \oplus 2 \oplus 2 = 1 \oplus 2 \oplus 2 = 3 \oplus 2 = 0 \oplus 2 = 2 \neq 0$.

(ii) Supongamos que $p(x) = q(x)h(x)$, con $0 \leq gr(q) < 2$, $0 \leq gr(h) < 2$ luego, si p es reductible, necesariamente q y h tienen grado 1. Tomemos por ejemplo $q(x) = a \oplus bx, b \neq 0$. Luego $b^{-1}p(x) = (ab^{-1} \oplus x)h(x)$, de donde $-ab^{-1} \in \mathbb{Z}_3$ es raíz del polinomio $b^{-1}p(x)$; pero si $b \neq 0$ las raíces de $b^{-1}p(x)$ son las mismas de p y éste no tiene raíces en $\mathbb{Z}_3$, concluyéndose la irreductibilidad de p ∎

Recordando que un número entero es factorizable, de manera única (salvo el orden), como producto de primos, en el anillo de polinomios tenemos el resultado análogo:

cualquier polinomio $f \in \mathcal{K}[x], gr(f) \geq 1$ puede escribirse de manera única (salvo el orden) como el producto de una constante y polinomios mónicos irreductibles:

$$p(x) = \lambda \prod_{i=1}^{s} q_i(x); \quad (6.58)$$

$\lambda \in \mathcal{K}$, $s \in \mathbb{N}$, $q_i \in \mathcal{K}[x]$ *son mónicos irreductibles*

Demostremos este resultado por inducción sobre el grado de f:

Para $gr(f) = 1$, $f(x) = ax + b, a \neq 0$ de donde:

$$f(x) = a(x + ba^{-1})$$

y $x + ba^{-1}$ es un polinomio mónico irreductible (pues es de grado 1).

Supongamos $gr(f) = n > 1$ y que la propiedad es cierta para polinomios de grado inferior o igual a $n - 1$. Si f es irreductible en $K[x]$,

$$f(x) = a_0 + a_1 x + ...a_n x^n, \quad a_n \neq 0$$

$$\Rightarrow \quad f(x) = a_n(\sum_{i=0}^{n} a_i a_n^{-1} x^i)$$

que es la factorización pedida. (Observación: hemos utilizado el hecho que si w es irreductible $\Rightarrow \forall \lambda \in K \setminus \{0\}, \lambda w$ también lo es; demuéstrelo).

Supongamos entonces que f es reductible, luego:

$$f(x) = g(x)h(x), \ 0 < gr(g) < n, \ 0 < gr(h) < n.$$

Por hipótesis de inducción:

$$g(x) = \lambda_1 \prod_{i=1}^{r} g_i(x); \quad g_i \text{ mónicos irreductibles}$$

$$h(x) = \lambda_2 \prod_{i=1}^{s} h_i(x); \quad h_i \text{ mónicos irreductibles,}$$

luego, $f(x) = \lambda_1\lambda_2 g_1(x)...g_r(x)h_1(x)...h_s(x)$.

La unicidad queda como ejercicio (inducción sobre el grado de f) ■

Consideremos un polinomio con coeficientes reales, $f \in \mathbb{R}[x]$. Se tiene la propiedad siguiente:

si $z \in \mathbb{C}$ con $Im(z) \neq 0$, es raíz de f, entonces $\bar{z}$ también es raíz de f.

En efecto, sea $z = z + ib$, $b \neq 0$. Como $f(z) = 0$:

$$f(z) = \sum_{i=0}^{n} a_i z^i = 0 \Leftrightarrow \overline{\sum_{i=0}^{n} a_i z^i} = \bar{0} = 0$$

$$\Leftrightarrow \sum_{i=0}^{n} a_i \bar{z}^i = 0 \Leftrightarrow f(\bar{z}) = 0.$$

Luego $\bar{z} = a - bi \in \mathbb{C}$ es raíz del polinomio f ■

Podemos resumir lo anterior diciendo que:

Las raíces complejas de un polinomio con coeficientes reales ocurren en pares conjugados. (6.59)

Interpretando los coeficientes del polinomio real f como números complejos, con parte imaginaria nula, se tiene (ver (6.56)):

$$f(x) = \lambda \prod_{j=1}^{n} (x - z_j), z_j \in \mathbb{C}. \tag{6.60}$$

Si z_j tiene parte imaginaria nula, entonces el polinomio lineal $x - z_j \in \mathbb{R}[x]$.

Si $z_j = a + bi$, $b \neq 0$, se tiene de (6.59) que $\bar{z}_j$ es también raíz, en $\mathbb{C}$, del polinomio f. Luego, en la descomposición (6.60) aparecen ambos polinomios $x - z_j$, $x - \bar{z}_j \in \mathbb{C}[x]$. Multiplicándolos:

$$\begin{aligned}(x - z_j)(x - \bar{z}_j) &= x^2 - \bar{z}_j x - z_j x + z_j \bar{z}_j \\ &= x^2 - (a - bi)x - (a + bi)x + (a + bi)(a - bi) \\ &= x^2 - 2ax + (a^2 + b^2) \in \mathbb{R}[x],\end{aligned}$$

que es un factor cuadrático de f, irreductible en $\mathbb{R}$ ■

De donde concluimos que:

Un polinomio con coeficientes reales, $f \in \mathbb{R}[x]$ se factoriza, en $\mathbb{R}[x]$, en polinomios lineales y cuadráticos irreductibles. (6.61)

Ejemplo: Sea $f(x) \in \mathbb{R}[x], f(x) = x^3 - 2x^2 + x - 2$. Claramente:

$$f(x) = x^2(x - 2) + (x - 2) = (x - 2)(x^2 + 1),$$

cuyos factores son irreductibles en $\mathbb{R}[x]$. Tomando f como polinomio en $\mathbb{C}$:

$$f(x) = (x - 2)(x + i)(x - i),$$

que son elementos irreductibles de $\mathbb{C}[x]$.

6.2.5 Relación entre raíces y coeficientes polinomiales.

Para terminar este capítulo, estableceremos, en el caso de un cuerpo $\mathcal{K}$ infinito, una relación entre los coeficientes y las raíces de una función polinomio. Consideremos, por ejemplo, la ecuación polinomial cúbica en un cuerpo $\mathcal{K}$, infinito:

$$f(x) = x^3 + a_2x^2 + a_1x + a_0 = 0 \qquad x \in \mathcal{K}$$

y supongamos que sus tres raíces r_1, r_2, r_3 están en $\mathcal{K}$. Factorizando, y teniendo en cuenta que f es mónico:

$$\begin{aligned}f(x) &= (x - r_1)(x - r_2)(x - r_3) \\ &= x^3 + (-r_1 - r_2 - r_3)x^2 + (r_1r_2 + r_1r_3 + r_2r_3)x + (-r_1r_2r_3).\end{aligned}$$

Como esta igualdad es válida $\forall x \in \mathcal{K}$, y $|\mathcal{K}| = +\infty$, obtenemos, de la propiedad (6.53), la igualdad de coeficientes:

$$a_3 = 1, a_2 = -r_1 - r_2 - r_3, a_1 = r_1r_2 + r_1r_3 + r_2r_3, \ a_0 = -r_1r_2r_3.$$

En el caso general, si $\{r_1, ..., r_n\} \subseteq \mathcal{K}$, son las raíces del polinomio mónico:

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

obtenemos, igualando coeficientes, cuando el cuerpo $\mathcal{K}$ es infinito:

$$\begin{aligned}
a_n &= 1 \\
a_{n-1} &= (-1)^1 \sum_{i=1}^{n} r_i \\
a_{n-2} &= (-1)^2 \sum_{i<j} r_i r_j \\
&\vdots \\
a_{n-k} &= (-1)^k \sum_{i_1<i_2<\ldots<i_k} r_{i_1} r_{i_j} \ldots r_{i_k} \\
&\vdots \\
a_0 &= (-1)^n r_1 r_2 \ldots r_n.
\end{aligned} \tag{6.62}$$

Demostremos (6.62), por inducción sobre el grado de f. Si $r_1, \cdots, r_n$ son las raíces del polinomio mónico $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, entonces $f(x) = (x - r_n)g(x)$, donde g es mónico, $gr(g) = n-1$ y $r_1, \cdots, r_{n-1}$ son las raíces de g. Ahora bien, podemos escribir

$$g(x) = x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_1 x + b_0$$

y por hipótesis de inducción, se tendrá:

$$\begin{aligned}
b_{n-1} &= 1 \\
b_{n-2} &= (-1)^1 \sum_{i=1}^{n-1} r_i \\
b_{n-3} &= (-1)^2 \sum_{\substack{i<j \\ (i,j \in \{1,\ldots,n-1\})}} r_i r_j \\
&\vdots \\
b_0 &= (-1)^{n-1} r_1 \ldots r_{n-1}.
\end{aligned}$$

Luego,

$$\begin{aligned}
f(x) &= xg(x) - r_n g(x) \\
&= (x^n + b_{n-2}x^{n-1} + \cdots + b_1 x^2 + b_0 x) \\
&\quad - (r_n \cdot x^{n-1} + r_n b_{n-2} x^{n-2} + \cdots + r_n b_1 x + r_n b_0).
\end{aligned}$$

Reuniendo los términos semejantes del polinomio:

$f(x) = x^n + (b_{n-2} - r_n)x^{n-1} + (b_{n-3} - r_n b_{n-2})x^{n-2} + \cdots$
$\ldots + (b_0 - r_n b_1)x - r_n b_0$, obtenemos

$$\begin{aligned}
a_n &= 1 \\
a_{n-1} &= (b_{n-2} - r_n) = (-1)^1 \sum_{i=1}^{n} r_i \\
a_{n-2} &= (b_{n-3} - r_n b_{n-2}) = (-1)^2 \sum_{\substack{i<j \\ i,j \in \{1,\ldots,n-1\}}} r_i r_j + (-1)^2 \sum_{i=1}^{n-1} r_i r_n \\
&= (-1)^2 \sum_{\substack{i<j \\ i,j \in \{1,\ldots,n\}}} r_i r_j
\end{aligned}$$

y sucesivamente hasta $a_0 = r_n b_0 = (-1)^n r_1 \ldots r_n$ ■

Las identidades de (6.62) son útiles para calcular las raíces de una ecuación polinomial cuando conocemos alguna relación entre ellas. Por ejemplo, consideremos el polinomio real $p(x) = 2x^3 - 8x^2 + 10x - 4$, con la información adicional que dos de sus raíces son iguales. Sin pérdida de generalidad consideremos las tres raíces r_1, r_2, r_3 tales que $r_1 = r_2$. Recordemos que las identidades de (6.62) son válidas para un polinomio mónico. Luego, dividiendo $p(x)$ por $a_3 = 2$ no alteramos sus raíces y obtenemos $q(x) = x^3 - 4x^2 + 5x - 2$. Aplicando (6.62):

$$\begin{aligned}
-r_1 - r_2 - r_3 &= -2r_1 - r_3 = \frac{a_2}{2} = -4 \\
r_1 r_2 + r_1 r_3 + r_2 r_3 &= r_1^2 + 2r_1 r_3 = \frac{a_1}{2} = 5 \\
-r_1 r_2 r_3 &= -r_1^2 r_3 = -2,
\end{aligned}$$

de donde obtenemos el sistema:

$$\begin{aligned}
2r_1 + r_3 &= 4 \\
r_1^2 + 2r_1 r_3 &= 5 \\
r_1^2 r_3 &= 2.
\end{aligned}$$

Reemplazando $r_3 = 4 - 2r_1$ en la segunda ecuación, obtenemos las soluciones de una ecuación de segundo grado $(r_1 = 1, r_3 = 2) \wedge (r_1 = \frac{5}{3}, r_3 = \frac{2}{3})$. De la tercera ecuación se concluye que las raíces son $r_1 = 1$ y $r_3 = 2$ ■

Ejercicios.

Números complejos.

1. Determine todos los números complejos, tales que:

$$|\frac{z-12}{z-8i}| = \frac{5}{3}; \quad |\frac{z-4}{z-8}| = 1.$$

2. Demuestre que $\forall z \in \mathbb{C}$, $|z| = 1$, puede escribirse:

$$z = \frac{1+\alpha i}{1-\alpha i}; \quad \alpha \in \mathbb{R},$$

determine el valor de α en función de $Arg(z)$.

3. Calcular: $\sqrt[3]{-1}$, $\sqrt[4]{1+i}$, $\sqrt{4i-3}$, $(\frac{1+\sqrt{3}i}{1-i})^{40}$.
4. (a) Muestre que la ecuación:

$$\bar{z}_0 z + z_0 \bar{z} + k = 0 \quad \text{con} \quad k \in \mathbb{R}, z_0 \in \mathbb{C} \text{ (fijo)}$$

representa a una recta perpendicular a $0P_0$ donde P_0 es el punto del plano asociado a z_0.

(b) Sea $x_n + iy_n = (1+\sqrt{3}i)^n$. Probar la relación recurrente $x_{n-1}y_n - x_n y_{n-1} = 2^{2n-2}\sqrt{3}$.

5. Resolver en $\mathbb{C}$: $x^3 + 3x + 2i = 0$.
6. Resolver $x^6 = i$.
7. Sea $n \in \mathbb{N}, n \geq 2$. Considere $w_k = e^{i\frac{2\pi k}{n}}, k = 0, 1, ..., n-1$. Pruebe que:

(a) $(w_k)^j = (w_j)^k, \quad k, j \in \{0, 1, ..., n-1\}$.

(b) $w_k^{-j} = \overline{(w_k^j)}$.

(c) Pruebe que $\sum_{k=0}^{n-1} w_k^j w_k^{-k} = \begin{cases} n & \text{si } j = k \\ 0 & \text{si } j \neq k \end{cases}$ con $j, k \in \{0, 1, ..., n-1\}$.

(d) Pruebe, además, que $\sum_{k=0}^{n-1} w_k = 0$.

8. Sea $a \in \mathbb{C}, |a| < 1$. Pruebe que:

$$\left|\frac{z-a}{1-\bar{a}\cdot z}\right| \quad \begin{cases} < 1 & \text{si } |z| < 1 \\ = 1 & \text{si } |z| = 1 \\ > 1 & \text{si } |z| > 1. \end{cases}$$

9. Pruebe que si w es raíz cúbica de la unidad, entonces $-3i\sqrt{3}(b-c)(c-a)(a-b) = (cw^2 + bw + a)^3 - (bw^2 + cw + a)^3$.

10. (a) Pruebe que $e^{\frac{i2k\pi}{n}}$ $k = 1, .., n = -1$, es raíz de $p(z) = 1 + z + ... + z^{n-1}$.

(b) Deduzca que $1 + z + ... + z^{-n1} = \prod_{k=1}^{n-1}(z - e^{\frac{i2k\pi}{n}})$ y concluya que

$$\frac{n^2}{z^{n-1}} = \prod_{k=1}^{n-1}(1 - cos(\frac{2k\pi}{n})).$$

11. Si $z^n = 1$ y $(z+1)^n = 1$, pruebe que n es divisible por 6 y que $z^3 = 1$.

Polinomios.

12. Dividir en $\mathbb{R}[x]$
(a) $f(x) = x^3 + 2x^2 - 1$ por $g(x) = x^2 + 2$.
(b) $f(x) = x^6 - 3x^5 + 2x^2 - x + 3$ por $g(x) = x^4 - 2x^2 + 1$.
13. Calcule: $mcd(x^3, x^2), mcd(1, x), mcd(x^3 - 3x + 2, x^2 + 2x - 1)$.
14. ¿En qué condiciones un polinomio de segundo grado es irreductible en $\mathbb{R}$?, ¿Qué sucede en $\mathbb{C}$?
15. Dado que el polinomio $p(z) = z^4 - 4z^3 + 10z^2 - 12z + 8$ posee sólo raíces complejas, y una de ellas tiene módulo 2, encuentre todas las raíces del polinomio.
16. Determine un polinomio cuadrático con coeficientes reales que admita como raíz :

$$z_0 = \frac{i}{1 + i + \frac{i}{1-i+\frac{i}{1+i}}}.$$

17. Considere el polinomio con coeficientes reales no nulos:

$$p(x) = x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0.$$

(a) Pruebe que si p posee una raíz imaginaria pura, entonces $a_1^2 + a_0 a_3^2 = a_1 a_2 a_3$.

(b) Si $a_3 = -8, a_2 = 24$ y $a_1 = -32$, encuentre a_0 de modo que $x_0 = 2$ sea una raíz cuádruple de p.

18. Descomponga el polinomio $p(x) = x^6 - 3x^5 - 4x^4 + 16x^2 - 48x - 64$ en polinomios reales irreductibles. (Indicación: -1 y 4 son raíces de p).
19. Determine si son o no reductibles los polinomios siguientes (en caso de ser reductibles de la factorización):
(a) $x^3 - 2x^2 + 1$ y $x^2 + 2$ en $\mathbb{R}$.
(b) $x^2 + 3x - 1$ en $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.
(c) $x^2 \oplus x \oplus 1$ en $\mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7$.
(d) $x^4 \oplus x^3 \oplus 1$ en $\mathbb{Z}_2$.
20. Demuestre, utilizando el algoritmo de la división, que para $a \in \mathbb{R}$:

(a) $\frac{x^n+a^n}{x-a} = \sum_{i=1}^{n} a^{i-1}x^{n-i} + \frac{2a^n}{x-a}$. Deduzca que $x^n + a^n$ no es divisible por $x - a$ para $a \neq 0$.

(b) Dé expresiones cerradas para $(x^n - a^n)/(x + a)$ y estudie la divisibilidad según la paridad de n.

21. Vía un ejemplo (en $(\mathbb{Z}_n, \oplus, \cdot)$ para algún valor de n), muestre que si $\mathbb{Z}_n$ tiene divisores de cero: $\exists f, g \in P(\mathbb{Z}_n)$ tales que: $gr(fg) < gr(f)+gr(g)$.

22. Demuestre que todo polinomio real p, de grado impar, es epiyectivo.

23. En el plano complejo, los vértices de un triángulo ABD están dados por las raíces del polinomio $p(z) = z^3 - 3pz^2 + 3qz - r$. Muestre que:
    (a) El centro de gravedad del triángulo está dado por $z = p$.
    (b) Si el triángulo es equilátero, entonces $p^2 = q$.

* 24. Considere el algoritmo de Horner para la evaluación del polinomio $p(z) = a_n z^n + a_{n-1}z^{n-1} + ... + a_1 z + a_0$, en z_0:
$h_{n+1}(z_0) = 0$ $h_k(z_0) = z_0 \cdot h_{k+1}(z_0) + a_k$, $k = n, n-1, ..., 1, 0$.
    (a) Pruebe que $h_0(z_0) = p(z_0)$ (use inducción).
    (b) Indique el número de sumas y productos que efectúa el algoritmo, en función de n.

25. Considere $p(z) = z^n + a_1 z^{n-1} + ... + a_{n-1}z + a_n$ y su descomposición

$$p(z) = \prod_{k=1}^{n}(z - z_k) \quad (\text{ en } \mathbb{C}).$$

Muestre que

$$\prod_{k=1}^{n}(1 + z_k^2) = (a_n - a_{n-2} + a_{n-4} + ...)^2 - (a_{n-1} - a_{n-3} + ...)^2.$$

* 26. En $\mathbb{R}^2$, considere los puntos $(x_i, y_i), i = 0, 1, ..., n$. Anotemos $p_{i_0 i_1, ..., i_k}$ al polinomio obtenido por las fórmulas recursivas:

1) $p_i(x) \equiv y_i$

2) $p_{i_0 i_1 ... i_k}(x) = \frac{(x-x_{i_0})p_{i_1 i_2 ... i_k}(x) - (x-x_{i_k})p_{i_0 i_1 ... i_{k-1}}(x)}{x_{i_k} - x_{i_0}}$

Pruebe que $p_{i_0 i_1 ... i_k}(x_{i_j}) = y_{i_j} \quad j = 0, ..., k$. ¿Cuál es el grado de $p_{i_0 i_1 ... i_k}$?

* 27. Consideremos el anillo de polinomios $Q[x]$. Definimos por recurrencia, dados $x_0, x_1, ..., x_n, ...$ reales diferentes, la diferencia dividida:

$$\delta_{x_0}(p) = p(x_0)$$

$$\delta_{x_0 ... x_n}(p) = \frac{\delta_{x_1, ..., x_n}(p) - \delta_{x_0, ..., x_{n-1}}(p)}{x_n - x_0}; \; p \in Q[x].$$

(a) Pruebe que si p tiene grado n, entonces $\delta_{x_0, ..., x_j}(p) = 0 \quad \forall j > n$.
(b) Pruebe que, si $p, q \in Q[x]$,

$$\delta_{x_0, ..., x_n}(p \cdot q) = \sum_{k=0}^{n} \delta_{x_0, ..., x_k}(p) \cdot \delta_{x_k, ..., x_n}(q)$$

(use inducción sobre n).

TEMAS CAPITULO VI

1. Raíces.

2. Descomposición de fracciones racionales.

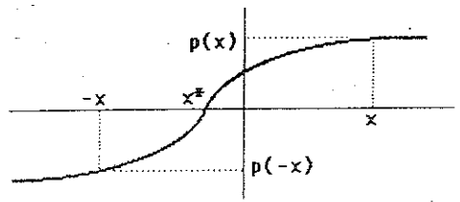
1. Raíces.

Como lo comentamos en el capítulo, la demostración de existencia de raíces en $\mathbb{C}$ (teorema fundamental de álgebra) escapa al nivel de este libro. Sin embargo, algo podemos hacer en el caso de polinomios con coeficientes reales y de grado impar. Demostraremos que

un polinomio de grado impar y coeficientes reales admite, al menos, una raíz real.

La idea de la demostración es simple: dado el polinomio $p(x) = \sum_{j=0}^{n} a_j x^j$, $gr(p) \geq 1$, veremos que para un valor "grande" de la variable x, el signo del polinomio (positivo o negativo) sólo depende del término $a_n x^n$. Como, además, n es impar, este valor cambia de signo para los valores x y $-x$: $p(x) = -p(-x)$.

Dado que una función polinomial es continua (al dibujar la curva no se levanta el lápiz) determinamos un valor, x^*, donde el polinomio "corta" el eje x.



Para demostrar seriamente la existencia de la raíz, probemos primero la propiedad:

$$|\sum_{j=0}^{n-1} a_j x^j| < |a_n x^n| \quad (\forall x \in \mathbb{R})\ (|x| > \frac{M}{|a_n|} + 1), \tag{6.63}$$

donde $M = \max\{|a_j| : j = 0, \cdots, n-1\}$ y $|\cdot|$ es la función módulo en $\mathbb{R}$.

En efecto, de las propiedades del módulo:

$$|\sum_{j=0}^{n-1} a_j x^j| \leq \sum_{j=0}^{n-1} |a_j| \cdot |x|^j \leq M \sum_{j=0}^{n-1} |x|^j.$$

Como esta sumatoria contiene los términos de una progresión geométrica:

$$|\sum_{j=0}^{n-1} a_j x^j| \leq M\frac{|x|^n - 1}{|x| - 1} \leq (\frac{M}{|x| - 1})|x|^n,$$

pero, por hipótesis, $|x| > \frac{M}{|a_n|} + 1 \Longleftrightarrow |a_n| > \frac{M}{|x|-1}$. De donde

$$|\sum_{j=0}^{n-1} a_j x^j| < |a_n| \cdot |x|^n = |a_n x^n| \quad \blacksquare$$

De este resultado se desprende directamente la propiedad

$$sgn(p(x)) = sgn(a_n x^n) \quad (\forall x \in \mathbb{R})(|x| > \frac{M}{|a_n|} + 1), \tag{6.64}$$

donde

$$sgn(u) = \begin{cases} 1 & \text{si } u > 0 \\ 0 & \text{si } u = 0 \\ -1 & \text{si } u < 0. \end{cases}$$

En efecto, supongamos que, para $|x| > \frac{M}{|a_n|} + 1$, $\text{sgn}(p(x)) \neq \text{sgn}(a_n x^n)$. Se tiene dos casos:

1. $(p(x) > 0) \wedge (a_n x^n < 0)$.
2. $(p(x) < 0) \wedge (a_n x^n > 0)$.

Observemos, que, si $p(x) = 0$, entonces x es raíz, demostrándose la existencia.

Analicemos el primer caso:

$$\sum_{j=0}^{n} a_j x^j > 0 \Longleftrightarrow -a_n x^n < \sum_{j=0}^{n-1} a_j x^j \leq |\sum_{j=0}^{n-1} a_j x^j|.$$

Como $a_n x^n < 0$, concluímos:

$$|a_n x^n| < |\sum_{j=0}^{n-1} a_j x^j|,$$

lo cual contradice (6.63).

En el segundo caso:

$$\sum_{j=0}^{n} a_j x^j < 0 \Longleftrightarrow |a_n x^n| < -\sum_{j=0}^{n-1} a_j x^j \leq |\sum_{j=0}^{n-1} a_j x^j|,$$

en contradicción con (6.63) ■

Supongamos ahora que $gr(p) = n$ es un número impar. Afirmamos entonces que:

$p(x)$ admite una raíz $x^* \in \mathbb{R}$ en el intervalo $]-\frac{M}{|a_n|} - 1, \frac{M}{|a_n|} + 1[$.

En efecto, sea $|x| > \frac{M}{|a_n|} + 1$. Como n es impar:

$$sgn(a_n(-x)^n) = sgn(-a_n x^n) = -sgn(a_n x^n).$$

De la propiedad (6.64) se tiene entonces:

$$sgn(p(-x)) = sgn(a_n(-x))^n = -sgn(a_n x^n) = -sgn(p(x)).$$

Es decir, $sgn(p(-x)) \neq sgn(p(x))$, o, de manera equivalente, el polinomio cambia de signo en los valores $-x$ y x.

Como un polinomio es una función continua (se traza su gráfico sin levantar el lápiz del papel), existe un real $x^* \in]\frac{-M}{|a_n|} - 1, \frac{M}{|a_n|} + 1[$ tal que $p(x^*) = 0$ ■

En base a argumentos similares, analicemos ahora el caso siguiente: supongamos que $gr(p(x)) = n$ es par y $sgn(a_n) \neq sgn(a_0)$, (el término constante y el asociado al grado tienen diferente signo). Tenemos entonces:

El polinomio $p(x)$ admite raíces reales, x_1, x_2, donde $x_1 \in]-\frac{M}{|a_n|} - 1, 0[$ *y* $x_2 \in]0, \frac{M}{|a_n|} + 1[$.

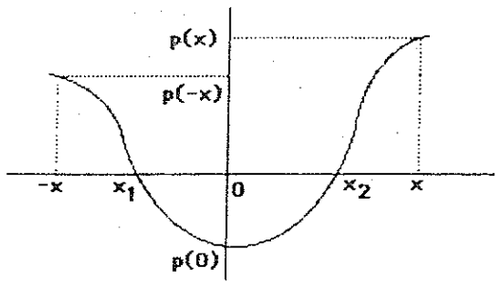
En efecto, si tomamos el valor de $-x < 0$, con $|x| > \frac{M}{|a_n|} + 1$, sabemos que

$$sgn(p(-x)) = sgn(a_n(-x)^n).$$

Como n es par, $(-x)^n = x^n > 0$:

$$sgn(p(-x)) = sgn(a_n x^n) = sgn(a_n) = sgn(p(x)).$$

Por otra parte $sgn(p(0)) = sgn(a_0)$.
Luego, $sgn(p(-x)) = sgn(p(x)) = sgn(a_n) \neq sgn(a_0) = sgn(p(0))$.



Por continuidad de $p(x)$, concluímos que:

$$(\exists x_1 \in]-x, 0[,\ p(x_1) = 0) \wedge (\exists x_2 \in]0, x[, p(x_2) = 0) \quad \blacksquare$$

Aplicación: Consideremos el polinomio $p(x) = x^4 + 3x^3 + x^2 - 3x - 2$. Del resultado anterior: $a_n = 1, a_0 = -2, M = 3$. Aseguramos así la existencia de dos raíces reales en los intervalos $]-4, 0[$ y $]0, 4[$. Se tiene

$$p(-4) = 90 \text{ y } p(0) = -2.$$

Evaluemos en $x = -3$: $p(-3) = 16, p(0) = -2$. Evaluando en $x = -2$; $p(-2) = 0$, determinando la raíz $x = -2$. Luego, dividiendo por el factor lineal $(x + 2)$:

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

Denominemos $q(x) = x^3 + x^2 - x - 1$, que es de grado impar con $M = 1, a_3 = 1$. Admite, entonces, una raíz en el intervalo $]-2, 2[$. Evaluando en $x = -1$, se obtiene $p(-1) = 0$, luego $x_2 = -1$ es raíz de $q(x)$. Dividiendo q por el factor $x + 1$:

$$p(x) = (x + 2)q(x) = (x + 2)(x + 1)(x^2 - 1),$$

obteniéndose la factorización $p(x) = (x + 2)(x - 1)(x + 1)^2$ y las raíces $x = -2, x = -1$ (doble), $x = 1$ $\blacksquare$

2. Descomposición de fracciones racionales.

Consideremos el cociente polinomial $h(x) = \frac{x^2+6}{x^3+x^2-2x}$, suponiendo que los polinomios pertenecen a $\mathbb{R}[x]$. Una expresión de este tipo la denominaremos *fracción racional* (observe que el grado del denominador es mayor que el del numerador). Pero, ¿qué podemos hacer con ella, aparte de mirarla?, pues bien, se *descompone* en factores "elementales". Para ello factorizemos el denominador en polinomios irreductibles:

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

Vemos que los factores son "lineales" (polinomios de grado 1). En tal caso escribimos

$$h(x) = \frac{a}{x} + \frac{b}{x-1} + \frac{c}{x+2}$$

$$\Leftrightarrow \quad h(x) = \frac{a(x-1)(x+2) + bx(x+2) + cx(x-1)}{x(x-1)(x+2)}$$

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

Como $\mathbb{R}$ es un cuerpo infinito, podemos igualar los coeficientes de ambos numeradores, obteniendo

$$\begin{array}{llll} a+b+c = 1 & b+c = 4 & b = 7/3 \\ a+2b-c = 0 \Rightarrow & 2b-c = 3 & \Rightarrow \ c = 5/3 \\ -2a = 6 & a = -3 & a = -3, \end{array}$$

de donde,

$$h(x) = \frac{-3}{x} + \frac{7}{3(x-1)} + \frac{5}{3(x+2)},$$

que corresponde a la descomposición de $h(x)$ en factores elementales.

Ahora bien, en el caso anterior el polinomio del denominador se descompuso en polinomiales irreductibles de grado uno ¿qué sucede si aparecen allí polinomios de grado dos? Consideremos, por ejemplo, $h(x) = \frac{x^2-6x+8}{x^3-x^2-4}$. Descomponiendo el denominador en $\mathbb{R}[x]$:

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

Además, $x^2 + x + 2$ es irreductible en $\mathbb{R}[x]$, puesto que sus raíces son $\frac{-1 \pm i\sqrt{7}}{2} \in \mathbb{C}$.

En este caso, el factor irreductible cuadrático aparece con un factor lineal, $bx + c$, en la descomposición elemental:

$$h(x) = \frac{a}{x-2} + \frac{bx+c}{x^2+x+2}.$$

Igualando términos semejantes, obtenemos el sistema:

$$a + b = 1, a - 2b + c = -6, 2a - 2c = 8,$$

de donde, $a = -12, b = 13, c = 32$, obteniendo la descomposición:

$$h(x) = \frac{-12}{x-2} + \frac{13x+32}{x^2+x+2} \quad \blacksquare$$

Determinar factorizaciones como las anteriores corresponde, en última instancia, a determinar soluciones de sistemas de ecuaciones, donde las incógnitas corresponden a las constantes que aparecen en las fracciones elementales. Veamos que esto es, al menos, posible en el caso particular $h(x) = \frac{g(x)}{f(x)}$, con $f, g \in \mathbb{R}[x], gr(f) = 3, gr(g) \leq 2$ y las raíces de $f, \{x_1, x_2, x_3\}$, son distintas. En esta situación afirmamos que $\forall g \in \mathbb{R}[x], gr(g) \leq 2$, existen constantes $a_1, a_2, a_3 \in \mathbb{R}$ tales que:

$$h(x) = \frac{a_1}{x-x_1} + \frac{a_2}{x-x_2} + \frac{a_3}{x-x_3}.$$

En efecto, consideremos $g(x) = b_0 + b_1 x + b_2 x^2, b_i \in \mathbb{R}, i = 1, 2, 3$. Igualando coeficientes se obtiene el sistema de tres ecuaciones:

$$\begin{aligned} a_1 \quad + a_2 \quad + a_3 \quad &= b_2 \\ -(x_2+x_3)a_1 - (x_1+x_3)a_2 - (x_1+x_2)a_3 &= b_1 \\ x_2x_3a_1 \quad + x_1x_3a_2 + \quad x_1x_2a_3 \quad &= b_0. \end{aligned}$$

Eliminando la variable a_1 de la segunda y tercera ecuación:

$$\begin{aligned} a_1 \quad + a_2 \quad + a_3 \quad &= b_2 \\ -(x_2-x_1)a_2 + (x_3-x_1)a_3 &= b_1 + (x_2+x_3)b_2 \\ x_3(x_1-x_2)a_2 \quad + x_2(x_1-x_3)a_3 \quad &= b_0 - x_2x_3b_2. \end{aligned}$$

Eliminando la variable a_2 de la tercera ecuación:

$$\begin{aligned} a_1 \quad + a_2 \quad + a_3 \quad &= b_2 \\ (x_2-x_1)a_2 + (x_3-x_1)a_3 &= b_1 + (x_2+x_3)b_2 \\ (x_3-x_1)(x_3-x_2)a_3 &= b_0 + x_3^2b_2 + x_3b_1. \end{aligned}$$

Como las raíces $\{x_1, x_2, x_3\}$ son distintas, el sistema anterior tiene solución, cualesquiera sean los coeficientes $\{b_0, b_1, b_2\} \in \mathbb{R}$. Basta despejar a_3, a_2, a_1, desde la tercera a la primera ecuación $\blacksquare$

Recordemos que $f \in \mathbb{R}[x]$ siempre se puede descomponer en un producto de factores lineales y cuadráticos irreductibles (ver (6.61)):

$$f(x) = (x-x_1)^{r_1}...(x-x_s)^{r_s}(a_1x^2+b_1x+c_1)^{p_1}...(a_mx^2+b_mx+c_m)^{p_m}$$

$$r_i \geq 1, \ i = 1, ..., s; \quad p_i \geq 1 \quad i = 1, ..., m.$$

En tal caso, si $gr(g) \leq gr(f)$, siempre es posible descomponer $h(x) = \frac{g(x)}{f(x)}$ como sigue:

$$h(x) = \sum_{j=1}^{r_1} \frac{a_{1j}}{(x-x_1)^j} + ... + \sum_{j=1}^{r_s} \frac{a_{sj}}{(x-x_s)^j} \tag{6.65}$$

$$+ \sum_{j=1}^{p_1} \frac{b_{1j}x + c_{1j}}{(a_1x^2+b_1x+c_1)^j} + ... + \sum_{j=1}^{p_m} \frac{b_{mj}x + c_{mj}}{(a_mx^2+b_mx+c_m)^j}.$$

Es decir, cada factor, con argumento lineal, de la forma $(x-x_i)^{r_i}$, de la factorización de f, da orígen a r_i fracciones elementales:

$$\frac{a_{i1}}{(x-x_i)} + \frac{a_{i2}}{(x-x_i)^2} + ... + \frac{a_{ir_i}}{(x-x_i)^{r_i}}.$$

Cada factor, con argumento cuadrático, irreductible $(a_kx^2+b_kx+c_k)^{p_k}$, da orígen a p_k fracciones elementales:

$$\frac{b_{k1}x + c_{k1}}{(a_kx^2+b_kx+c_k)} + \frac{b_{k2}x + c_{k2}}{(a_kx^2+b_kx+c_k)^2} + ... + \frac{b_{kp_k}x + c_{kp_k}}{(a_kx^2+b_kx+c_k)^{p_k}}.$$

La demostración de este resultado puede hacerse verificando que el sistema asociado, cuyas incógnitas son las constantes, tiene solución cualquiera sea el polinomio $g \in \mathbb{R}[x]$, $gr(g) \leq gr(f)$. La demostración es larga y requiere un buen conocimiento sobre la resolución general de sistemas de ecuaciones, tema que abordaremos en el próximo capítulo.

Ejercicios.

1. Factorize en fracciones elementales
   (a) $\frac{x^2+12x-1}{x^3+3x^2-4}$
   (b) $\frac{x^3}{(x^2+1)^4}$

(c) $\frac{2x^3+1}{x^5+2x^3+x}$

(d) $\frac{x^2-6x+1}{x^3-7x^2+15x-9}$

2. Utilizando el algoritmo de división de polinomios, demuestre que si $gr(g) \geq gr(f)$ puede escribirse:

$$h(x) = \frac{g(x)}{f(x)} = q(x) + \frac{r(x)}{f(x)}, \quad gr(r) < gr(f)$$

y, en consecuencia, descomponer h en la forma: $h(x) = q(x) + \sum_{i=1}^{q} s_i(x)$, donde s_i son fracciones elementales.

CAPITULO VII

En esta matriz se forjaron
nuestros héroes.
(alocución castrense)

ALGEBRA MATRICIAL

Recordemos que una matriz, A, de m filas y n columnas con coeficientes en el cuerpo $\mathcal{K}$, es una tabla de doble entrada:

$$A = \begin{pmatrix} a_{11} \ldots\ldots a_{1n} \\ \vdots \qquad\quad \vdots \\ a_{m1} \ldots\ldots a_{mn} \end{pmatrix}, \qquad a_{ij} \in \mathcal{K}, \quad \forall i = 1, \ldots m, \; j = 1, \ldots, n.$$

Notamos también la matriz como $A = (a_{ij})$ y denominamos $M_{mn}(\mathcal{K})$ al conjunto de todas las matrices de m filas y n columnas con coeficientes en el cuerpo $\mathcal{K}$.

Dadas dos matrices $A \in M_{mn}(\mathcal{K}), B \in M_{m'n'}(\mathcal{K})$, diremos que son *iguales* si y sólo si:

$$(m = m') \wedge (n = n') \wedge (\forall i \in \{1, \ldots, m\}, \forall j \in \{1, \ldots, n\}, a_{ij} = b_{ij}). \qquad (7.1)$$

La idea es construir una estructura algebraica sobre $M_{mn}(\mathcal{K})$ a partir de las operaciones definidas en el cuerpo $\mathcal{K}$. De manera análoga al procedimiento empleado con matrices booleanas y de permutación, se define la *suma* de dos matrices como sigue:

Dadas $A, B \in M_{mn}(\mathcal{K}) : A+B = (a_{ij}+b_{ij})$. (7.2)

Por ejemplo, en $(\mathbb{R}, +, \cdot)$:

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & -1 & -2 \end{pmatrix} + \begin{pmatrix} 0 & -1 & 2 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 5 \\ 3 & 0 & 0 \end{pmatrix}.$$

Es fácil verificar que $(M_{mn}(\mathcal{K}), +)$ tiene estructura de grupo abeliano: la suma es asociativa y conmutativa, como herencia de las mismas propiedades en el cuerpo $\mathcal{K}$. El neutro aditivo es

$$O = \begin{pmatrix} 0 \ldots\ldots 0 \\ \vdots \quad\; \vdots \\ 0 \ldots\ldots 0 \end{pmatrix} \in M_{mn}(\mathcal{K}).$$

El inverso aditivo de $A = (a_{ij})$ es $-A = (-a_{ij})$.

Por ejemplo, en $M_{23}(\mathbb{C})$:

$$\begin{pmatrix} i & 0 & 0 \\ 1 & -i & 0 \end{pmatrix} + \begin{pmatrix} -i & 0 & 0 \\ -1 & i & 0 \end{pmatrix} =$$

$$= \begin{pmatrix} i-i & 0+0 & 0+0 \\ 1-1 & -i+i & 0+0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = O.$$

Luego,

$$-\begin{pmatrix} i & 0 & 0 \\ 1 & -i & 0 \end{pmatrix} = \begin{pmatrix} -i & 0 & 0 \\ -1 & i & 0 \end{pmatrix}.$$

Dadas $A = (a_{ij}) \in M_{mr}(\mathcal{K})$, $B = (b_{ij}) \in M_{rn}(\mathcal{K})$ se define el producto $C = AB$ como

$$C = (c_{ij}),\ c_{ij} = \sum_{k=1}^{r} a_{ik} b_{kj} \quad \forall i, j. \tag{7.3}$$

Claramente, $C \in M_{mn}(\mathcal{K})$.

Ejemplos:

- En $(\mathbb{R}, +, \cdot)$,

$$A = \begin{pmatrix} 1 & -1 & 0 \\ 1 & 2 & 1 \end{pmatrix} \in M_{23}(\mathbb{R})$$

$$B = \begin{pmatrix} 1 & 2 & -1 & 0 \\ 0 & 2 & -1 & 0 \\ 1 & 0 & -1 & 0 \end{pmatrix} \in M_{34}(\mathbb{R})$$

$$\Rightarrow C = A \cdot B = \begin{pmatrix} 1 & -1 & 0 \\ 1 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & -1 & 0 \\ 0 & 2 & -1 & 0 \\ 1 & 0 & -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & 6 & -4 & 1 \end{pmatrix} \in M_{24}(\mathbb{R}).$$

- En $(\mathbb{Z}_3, \oplus, \cdot)$,

$$A = \begin{pmatrix} [0] & [1] & [0] \\ [2] & [2] & [1] \\ [0] & [1] & [2] \end{pmatrix} \in M_{33}(\mathbb{Z}_3)$$

$$B = \begin{pmatrix} [1] \\ [2] \\ [1] \end{pmatrix} \in M_{31}(\mathbb{Z}_3)$$

$$\Rightarrow \quad C = AB = \begin{pmatrix} [2] \\ [1] \\ [1] \end{pmatrix} \in M_{31}(\mathbb{Z}_3).$$

- En $(\mathbb{C}, +, \cdot)$,

$$A = (-i,\ i,\ 0) \in M_{13}(\mathbb{C})$$

$$B = \begin{pmatrix} i \\ 1 \\ 0 \end{pmatrix} \in M_{31}(\mathbb{C})$$

$$\Rightarrow \quad C = AB = (-i \cdot i + i \cdot 1 + 0 \cdot 0) = (1 + i) \in M_{11}(\mathbb{C}) \cong \mathbb{C}.$$

La multiplicación de matrices no es necesariamente conmutativa. Por ejemplo, en $M_{22}(\mathbb{R})$:

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

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

Dos propiedades importantes de la multiplicación son las siguientes:
la multiplicación es asociativa; si $A \in M_{mn}(\mathcal{K}), B \in M_{nq}(\mathcal{K}), C \in M_{qs}(\mathcal{K})$, entonces:

$$A(BC) = (AB)C \in M_{ms}(\mathcal{K}) \tag{7.4}$$

· *distribuye con respecto a* $+$: dadas $A \in M_{mn}(\mathcal{K}), B, C \in M_{ns}(\mathcal{K})$, entonces

$$A \cdot (B + C) = AB + AC \in M_{ms}(\mathcal{K}). \tag{7.5}$$

La asociatividad se verifica de manera similar al caso de matrices con elementos 0's y 1's (vea párrafo (5.8.4)). Demostremos entonces la distributividad. Denominando $E = A(B + C)$, se tiene:

$$e_{ij} = \sum_{k=1}^{n} a_{ik}(b_{kj} + c_{kj}) \quad \forall i \in \{1, ..., m\}, j \in \{1, ..., s\}.$$

Como, en $\mathbb{R}$, la multiplicación distribuye con respecto a la suma:

$$e_{ij} = \sum_{k=1}^{n} (a_{ik} b_{kj} + a_{ik} c_{kj})$$

$$= \sum_{k=1}^{n} a_{ik} b_{kj} + \sum_{k=1}^{n} a_{ik} c_{kj}.$$

De la definición de multiplicación matricial, se obtiene $E = AB + AC$ ■

Un caso particular muy importante es el de las *matrices cuadradas*, es decir con igual número de filas y columnas. Como vimos en (5.8.4), $(M_{nn}(\mathcal{K}),\cdot)$ admite un neutro multiplicativo, denominado *matriz identidad:*

$$I=\begin{pmatrix}1&0&\cdots&0\\0&1&\cdots&0\\&&\ddots&\\0&0&\cdots&1\end{pmatrix}=(\delta_{ij});\quad \delta_{ij}=\begin{cases}0 & \text{si } i\neq j\\ 1 & \text{si } i=j.\end{cases}$$

En efecto, dada $A\in M_{nn}(\mathcal{K})$:

$$AI=\begin{pmatrix}a_{11}\ldots\ldots a_{1n}\\ \vdots\quad\vdots\\ a_{n1}\ldots\ldots a_{nn}\end{pmatrix}\begin{pmatrix}1&0&\cdots&0\\0&1&\cdots&0\\&&\ddots&\\0&0&\cdots&1\end{pmatrix}$$

$$=(\sum_{k=1}^{n}a_{ik}\delta_{kj})=(a_{ij}\delta_{jj})=(a_{ij})=A \quad \blacksquare$$

De los resultados anteriores concluímos que

$$(M_{nn}(\mathcal{K}),+,\cdot)\textit{es un anillo con unidad (existe neutro para }\cdot). \tag{7.6}$$

Dado que $(M_{un}(\mathcal{K},\cdot)$ tiene un elemento neutro I, es interesante preguntarse si sus elementos poseen inverso. En el contexto particular de matrices cuadradas, $A\in M_{nn}(\mathcal{K})$ *es invertible* si y sólo si existe $X\in M_{nn}(\mathcal{K})$ tal que:

$$AX=XA=I. \tag{7.7}$$

De existir una matriz X que satisfaga (7.7) la notaremos $X=A^{-1}$.

Pero, no todas las matrices cuadradas tienen inverso multiplicativo, por ejemplo, en $M_{22}(\mathbb{R})$, la matriz $\begin{pmatrix}1&2\\2&4\end{pmatrix}$ no tiene inverso. En efecto, si existiese el inverso, digamos $\begin{pmatrix}x_1&x_2\\x_3&x_4\end{pmatrix}$, debería verificarse:

$$\begin{pmatrix}1&2\\2&4\end{pmatrix}\begin{pmatrix}x_1&x_2\\x_3&x_4\end{pmatrix}=\begin{pmatrix}1&0\\0&1\end{pmatrix}$$

$$\Leftrightarrow\quad\begin{pmatrix}x_1+2x_3&x_2+2x_4\\2x_1+4x_3&2x_2+4x_4\end{pmatrix}=\begin{pmatrix}1&0\\0&1\end{pmatrix}$$

$$\Leftrightarrow\quad\begin{aligned}x_1+2x_3&=1\\x_2+2x_4&=0\\2x_1+4x_3&=0\\2x_2+4x_4&=1\end{aligned}$$

De la primera ecuación, multiplicada por 2, obtenemos: $2(x_1+2x_3)=2$. Pero de la tercera ecuación, $2x_1+4x_3=0$. De esta contradicción concluímos que el sistema no tiene solución $\blacksquare$

En otros casos existe inverso, por ejemplo, en $M_{22}(\mathbb{R})$,

$$\begin{pmatrix}0&1\\1&0\end{pmatrix}^{-1}=\begin{pmatrix}0&1\\1&0\end{pmatrix}$$

En efecto:

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

O bien, en $M_{22}(\mathbb{C})$,

$$\begin{pmatrix}i&0\\0&-i\end{pmatrix}^{-1}=\begin{pmatrix}-i&0\\0&i\end{pmatrix}$$

En efecto:

$$\begin{pmatrix}i&0\\0&-i\end{pmatrix}\begin{pmatrix}-i&0\\0&i\end{pmatrix}=\begin{pmatrix}-i^2&0\\0&-i^2\end{pmatrix}=\begin{pmatrix}1&0\\0&1\end{pmatrix}$$

También del párrafo (5.8.4), sabemos que las matrices de permutación son invertibles. En efecto, sea $A=(a_{ij})$ una matriz de permutación, es decir, que tiene un uno y sólo un uno, por filas y por columnas. Consideremos la traspuesta (intercambio de filas y columnas definido en el capítulo III), ${}^tA=(b_{ij})$. Calculemos $C=A^tA$. Se tiene

$$c_{ij}=\sum_{k=1}^{n}a_{ik}b_{kj}.$$

Como ${}^tA=(b_{ij})$ consiste en intercambiar las filas por columnas, se tiene que $b_{kj}=a_{jk}$:

$$c_{ij}=\sum_{k=1}^{n}a_{ik}a_{jk}.$$

Si $i \neq j$, el valor $a_{ik}a_{jk} = 0$. En caso contrario, tendríamos $a_{ik} = a_{jk} = 1$, es decir, la columna k tendría dos unos, lo cual es una contradicción. Concluímos entonces que $c_{ij} = 0$, $\forall i \neq j$.

Si $i = j$:

$$c_{ii} = \sum_{k=1}^{n} a_{ik} \cdot a_{ik} = \sum_{k=1}^{n} a_{ik}^2.$$

Como $a_{ik} \in \{0,1\}$ entonces $c_{ii} = \sum_{k=1}^{n} a_{ik} = 1$, pues la suma por filas y columnas es exactamente uno.

Hemos probado, entonces, que $C = A^t A = I$, luego A es invertible y su inversa es $A^{-1} = {}^tA$ ■

7.1 Matrices particulares.

Diremos que $A \in M_{nn}(\mathcal{K})$ es *diagonal* si y sólo si $a_{ij} = 0$, $\forall i \neq j$:

$$A = \begin{pmatrix} a_{11} & & & 0 \\ & a_{22} & & \\ & & \ddots & \\ 0 & & & a_{nn} \end{pmatrix} \tag{7.8}$$

es *triangular superior* si y sólo si $a_{ij} = 0$ si $i > j$:

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & a_{nn} \end{pmatrix} \tag{7.9}$$

es *triangular inferior* si y sólo si $a_{ij} = 0$ si $i < j$:

$$A = \begin{pmatrix} a_{11} & 0 & & \cdots & 0 \\ a_{21} & a_{22} & 0 & \cdots & 0 \\ \vdots & & & \ddots & 0 \\ a_{n1} & a_{n2} & \cdots & \cdots & a_{nn} \end{pmatrix}. \tag{7.10}$$

Ejemplos.

$A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$, $I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ son matrices diagonales.

$A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & 1 \\ 0 & 0 & 2 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 2 & 0 \\ 2 & -1 & 3 \end{pmatrix}$ son matrices triangulares, superior e inferior respectivamente.

Dada una matriz $A \in M_{mn}(\mathcal{K})$ notaremos su i-ésima fila como:

$$A_{i\bullet} = (a_{i1}, a_{i2}, ..., a_{in}) \tag{7.11}$$

y su j-ésima columna:

$$A_{\bullet j} = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix} \tag{7.12}$$

Podemos escribir entonces la matriz: $A = (A_{\bullet 1}, A_{\bullet 2}, ..., A_{\bullet n})$, denominada *notación por columnas.* O bien:

$$A = \begin{pmatrix} A_{1\bullet} \\ A_{2\bullet} \\ \vdots \\ A_{m\bullet} \end{pmatrix}, \qquad \text{correspondiente a la } \textit{notación por filas.}$$

Dada una constante $\lambda \in \mathcal{K}$, definimos la matriz A *ponderada* por λ:

$$\lambda A = (\lambda a_{ij}); \tag{7.13}$$

por ejemplo en $M_{23}(\mathbb{R})$:

$$3 \cdot \begin{pmatrix} 1 & -1 & 0 \\ 2 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 3 & -3 & 0 \\ 6 & 6 & 3 \end{pmatrix}.$$

Veamos ahora qué sucede al multiplicar por la derecha o izquierda una matriz por otra diagonal:

$$DA = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 1 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 & 4 \\ 6 & 0 & 3 \end{pmatrix}$$

constatamos que la primera fila aparece multiplicada por $d_{11} = 2$ y la segunda por $d_{22} = 3$.

$$AD = \begin{pmatrix} 1 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 6 \\ 4 & 0 & 3 \end{pmatrix}.$$

Aquí, la primera columna de A aparece multiplicada por 2, la segunda por 1, la tercera por 3. En general:

$$\begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \begin{pmatrix} a_{11} & \cdots & a_{1p} \\ \vdots & & \\ a_{n1} & \cdots & a_{np} \end{pmatrix} = \begin{pmatrix} \lambda_1 a_{11} & \dots & \lambda_1 a_{1p} \\ \lambda_2 a_{21} & \cdots & \lambda_2 a_{2p} \\ \vdots & & \vdots \\ \lambda_n a_{n1} & \cdots & \lambda_n a_{np} \end{pmatrix}$$

$$\begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & & \\ b_{p1} & \cdots & b_{pn} \end{pmatrix} \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} = \begin{pmatrix} \lambda_1 b_{11} & \lambda_2 b_{12} & \cdots & \lambda_n b_{1n} \\ \vdots & \vdots & & \vdots \\ \lambda_1 b_{p1} & \lambda_2 b_{p2} & \cdots & \lambda_n b_{pn} \end{pmatrix}.$$

De forma más compacta, si la matriz diagonal es $D = diag(\lambda_1, ..., \lambda_n)$

$$DA = \begin{pmatrix} \lambda_1 \ A_{1\bullet} \\ \vdots \\ \lambda_n \ A_{n\bullet} \end{pmatrix} \tag{7.14}$$

$$BD = (\lambda_1 B_{\bullet 1}, ..., \lambda_n B_{\bullet n}). \tag{7.15}$$

Demostremos (7.14):

$$\text{Sea} \quad D = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} = (d_{ij}); d_{ij} = \begin{cases} \lambda_i & \text{si } i = j \\ 0 & \text{si } i \neq j, \end{cases}$$

luego,

$$DA = (\sum_{k=1}^{n} d_{ik} a_{kj}) = (d_{ii} a_{ij}) = (\lambda_i a_{ij})$$

$$= \begin{pmatrix} \lambda_1 a_{11} & \dots & \lambda_1 a_{1p} \\ & \vdots & \\ \lambda_n a_{n1} & \cdots & \lambda_n a_{np} \end{pmatrix} \quad \blacksquare$$

Otra propiedad, que utilizaremos más adelante, es la siguiente:

el producto de matrices triangulares inferiores (superiores) es triangular inferior (superior). (7.16)

Verifiquemos el caso triangular superior. Sean

$$T_1 = \begin{pmatrix} a_{11} & \cdots & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & a_{nn} \end{pmatrix}, \quad T_2 = \begin{pmatrix} b_{11} & \cdots & \cdots & b_{1n} \\ 0 & b_{22} & \cdots & b_{2n} \\ & & \ddots & \vdots \\ 0 & \cdots & 0 & b_{nn} \end{pmatrix}$$

Luego $C = T_1 \cdot T_2 = (c_{ij})$, donde: $c_{ij} = \sum_{j=1}^{n} a_{ik} b_{kj}$. Como T_1 y T_2 son triangulares superiores: $(a_{i\ell} = 0) \wedge (b_{i\ell} = 0) \ \forall \ell < i$. Supongamos $j < i$, luego

$$c_{ij} = \sum_{k=1}^{i-1} a_{ik} b_{kj} + \sum_{k=i}^{n} a_{ik} b_{kj}.$$

En el primer término $k < i \Rightarrow a_{ik} = 0$. En el segundo término $j < i \leq k \Rightarrow b_{kj} = 0$, luego $\forall j < i, \ c_{ij} = 0$. Lo cual prueba que la matriz C es triangular superior $\blacksquare$

7.2 Potencias, traspuestas, inversas.

Tal como lo hicimos en capítulos anteriores con matrices de 0's y 1's definimos por recurrencia la potencia de una matriz:

Dada $A \in M_{nn}(\mathcal{K})$:

$$A^{\circ} = I, \ A^n \doteq A \cdot A^{n-1}, \quad n \geq 1. \tag{7.17}$$

Por ejemplo; dada $A \in M_{33}(\mathbb{Z}_3)$:

$$A = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 0 \\ 1 & 1 & 2 \end{pmatrix}, \quad \text{(los coeficientes son clases en } \mathbb{Z}_3 : x \equiv [x])$$

$$A^2 = A \cdot A = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 0 \\ 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 0 \\ 1 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 2 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

$$A^3 = A \cdot A^2 = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 0 \\ 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 1 \\ 0 & 2 & 1 \\ 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 & 0 \\ 2 & 1 & 2 \\ 0 & 1 & 1 \end{pmatrix}$$

Recordemos que dada una matriz $A = (a_{ij}) \in M_{mn}(\mathcal{K})$, se define su *traspuesta* como ${}^tA = (a_{ji})$. Por ejemplo:

$$A = \begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}, \quad {}^tA = \begin{pmatrix} 1 & 0 & 1 \\ 2 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

$$A = (1,\ -1,\ 0,\ 0,\ 1), \quad {}^tA = \begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$$A = \begin{pmatrix} 1 & 2 & 1 \\ 2 & 0 & 1 \\ 1 & 1 & 4 \end{pmatrix}, \quad {}^tA = \begin{pmatrix} 1 & 2 & 1 \\ 2 & 0 & 1 \\ 1 & 1 & 4 \end{pmatrix}$$

En el último caso vemos que $A = {}^tA$. Diremos que una matriz $A \in M_{nn}(\mathcal{K})$ es

$$\textit{simétrica} \text{ si y sólo si } A = {}^tA. \tag{7.18}$$

Es fácil verificar que A es simétrica si y sólo si:

$$a_{ij} = a_{ji} \qquad \forall i, j = 1, ..., n. \tag{7.19}$$

Algunas propiedades de la trasposición de matrices son las siguientes:

$$^t({}^tA) = A, \qquad \forall A \in M_{mn}(\mathcal{K}) \tag{7.20}$$

$$^t(A \cdot B) = {}^tB \cdot {}^tA \tag{7.21}$$

$$\text{Si } D \in M_{nn}(\mathcal{K}) \text{ es diagonal: } {}^tD = D. \tag{7.22}$$

Demostremos (7.21):

Sea $C = A \cdot B$, $Y = {}^tC = {}^t(A \cdot B)$. En la posición (i, j) de la matriz Y aparece el término c_{ji} de la matriz C:

$$y_{ij} = c_{ji} = \sum_{k=1}^{n} a_{jk} b_{ki}.$$

Consideremos $X = {}^tB\ {}^tA$. El término x_{ij} está dado por la multiplicación de la i-ésima fila de ${}^tB$ por la j-ésima columna de ${}^tA$. Pero:
- la i-ésima fila de ${}^tB$ corresponde a la i-ésima columna de $B : (b_{1i}, ..., b_{ni})$.

- la j-ésima columna de ${}^tA$ corresponde a la j-ésima fila de $A : (a_{j1}, ..., a_{jn})$.
Luego,

$$x_{ij} = (b_{1i}, b_{2i}, ..., b_{ni}) \begin{pmatrix} a_{j1} \\ a_{j2} \\ \vdots \\ a_{jn} \end{pmatrix} = \sum_{k=1}^{n} b_{ki} a_{jk} = y_{ij};$$

de donde $Y = X$ ■

Algunas propiedades elementales de matrices invertibles son las siguientes:

Sean $A, B \in M_{nn}(\mathcal{K})$ invertibles, entonces

$$\textit{La inversa es única.} \tag{7.23}$$

$$(AB)^{-1} = B^{-1}A^{-1} \tag{7.24}$$

$$(A^n)^{-1} = (A^{-1})^n \qquad \forall n \geq 0 \tag{7.25}$$

$$({}^tA)^{-1} = {}^t(A^{-1}). \tag{7.26}$$

En efecto:

(7.23) Supongamos A invertible y $X, Y \in M_{nn}(\mathcal{K})$ tales que:

$$AX = XA = I$$
$$AY = YA = I$$

luego, $Y(AX) = Y \cdot I \Leftrightarrow (YA)X = Y \Leftrightarrow IX = Y \Leftrightarrow X = Y$.

(7.24) $AB(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AIA^{-1} = AA^{-1} = I$. Como la inversa es única $(AB)^{-1} = B^{-1}A^{-1}$.

(7.25) Se verifica para $n = 0, 1$. Supongamos cierto para n y demostremos para $n + 1$:

$$(A^{n+1})^{-1} = (A^n \cdot A)^{-1} = A^{-1}(A^n)^{-1},$$

por hipótesis de inducción

$$= A^{-1}(A^{-1})^n = (A^{-1})^{n+1}.$$

(7.26) Se tiene $A \cdot A^{-1} = I$, trasponiendo:

$$ {}^t(AA^{-1}) = {}^tI \Leftrightarrow {}^t(A^{-1}) \cdot {}^tA = I $$

finalmente, por unicidad de la inversa: $({}^tA)^{-1} = {}^t(A^{-1})$ ∎

7.3 Matrices elementales.

Un tipo particular de matrices de permutación (ver párrafo 5.8.4) en $M_{nn}(\mathcal{K})$ es el siguiente:

$$ I_{pq} = \begin{pmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & \bigcirc & \\ & & 1 & & & & & & \\ & & & 0 & \cdots & \cdots & \cdots & 1 & \\ & & & \vdots & 1 & & & \vdots & \\ & & & & & 1 & & & \\ & & & \vdots & & & 1 & \vdots & \\ & & & 1 & \cdots & \cdots & \cdots & 0 & \\ & & & & & & & & 1 \\ & & \bigcirc & & & & & & & \ddots \\ & & & & & & & & & & 1 \end{pmatrix} \begin{matrix} \\ \\ \\ \text{fila } p \\ \\ \\ \\ \text{fila } q \\ \\ \\ \\ \end{matrix} \qquad (7.27) $$

La matriz I_{pq} se construye a partir de la identidad, permutando el orden de las filas p y q. Por ejemplo, en $M_{44}(\mathbb{R})$:

$$ I_{24} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \qquad I_{13} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} $$

Veamos ahora lo que sucede al multiplicar una matriz A, por la derecha o izquierda, por una matriz de permutación I_{pq}.

En el ejemplo anterior, sea $A = (a_{ij}) \in M_{43}(\mathbb{R})$

$$ I_{24} \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \\ a_{41} & a_{42} & a_{43} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \\ a_{41} & a_{42} & a_{43} \end{pmatrix} $$

$$ = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{41} & a_{42} & a_{43} \\ a_{31} & a_{32} & a_{33} \\ a_{21} & a_{22} & a_{23} \end{pmatrix} $$

La matriz resultante corresponde a permutar las filas 2 y 4 de A.

Análogamente, sea $B \in M_{34}(\mathbb{R})$:

$$ \begin{pmatrix} b_{11} & b_{12} & b_{13} & b_{14} \\ b_{21} & b_{22} & b_{23} & b_{24} \\ b_{31} & b_{32} & b_{33} & b_{34} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} b_{11} & b_{14} & b_{13} & b_{12} \\ b_{21} & b_{24} & b_{23} & b_{22} \\ b_{31} & b_{34} & b_{33} & b_{32} \end{pmatrix}. $$

la matriz resultante es B con las columnas 2 y 4 permutadas.

En general, dada $I_{pq} \in M_{nn}(\mathcal{K}), A \in M_{ns}(\mathcal{K}), B \in M_{qn}(\mathcal{K})$:

$I_{pq}A$ corresponde a la matriz A con las filas p y q permutadas. (7.28)

BI_{pq} corresponde a la matriz B con las columnas p y q permutadas. (7.29)

Recordemos que, por ser una matriz de permutación, I_{pq} es invertible y además $I_{pq}^{-1} = I_{pq}$. En efecto, el multiplicar por la izquierda I_{pq} por sí misma, corresponde a intercambiar sus filas $I_{p\bullet}, I_{q\bullet}$, con lo cual se obtiene la identidad ∎

Tomemos ahora la matriz $A \in M_{44}(\mathbb{R})$ y sea:

$$ E_{24}(\lambda, \beta) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & \lambda & 0 & \beta \end{pmatrix} \qquad \beta \neq 0. $$

Esta matriz se construye a partir de la identidad, colocando el valor λ en la posición (4,2) y β en la posición (4,4).
Al multiplicar por la izquierda A por $E_{24}(\lambda, \beta)$:

$$ E_{24}(\lambda, \beta) \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \\ a_{41} & a_{42} & a_{43} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & \lambda & 0 & \beta \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \\ a_{41} & a_{42} & a_{43} \end{pmatrix} $$

$$= \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \\ \lambda a_{21} + \beta a_{41} & \lambda a_{22} + \beta a_{42} & \lambda a_{23} + \beta a_{43} \end{pmatrix}.$$

La matriz, $E_{24}(\lambda, \beta)A$ es el resultado de sumar a la fila 4 de A, ponderada por β, la fila 2 de A ponderada por λ.

En general, definimos la *matriz elemental* $E_{pq}(\lambda, \beta) \in M_{nn}(\mathcal{K})$:

$$E_{pq}(\lambda,\beta) = \begin{pmatrix} 1 & & & & & & & & \\ & \ddots & & & & & \bigcirc & & \\ & & 1 & & & & & & \\ & & & \ddots & & & & & \\ & & \vdots & & 1 & & & & \\ 0 & \cdots & \lambda & \cdots & & \beta & & & \\ \vdots & & \vdots & & & & 1 & & \\ \vdots & & \vdots & & & & & \ddots & \\ 0 & \cdots & 0 & \cdots & \cdots & \cdots & \cdots & 0 & 1 \end{pmatrix} \quad \begin{matrix} \lambda, \beta \in \mathcal{K} \\ \beta \neq 0 \\ p < q \end{matrix} \tag{7.30}$$

$$\begin{matrix} & \uparrow & & \uparrow & \\ & p & & q & \end{matrix}$$

Dada una matriz $A \in M_{ns}(\mathcal{K})$, se tiene:

$$C = E_{pq}(\lambda,\beta) \cdot A = \begin{pmatrix} 1 & & & & & & & \\ & \ddots & & & & & \bigcirc & \\ & & 1 & & & & & \\ & & & \cdots & & & & \\ & & \vdots & & 1 & & & \\ & & \lambda & \cdots & & \beta & & \\ & & & & & & 1 & \\ & & & & & & & \ddots \\ & & & & & & & & 1 \end{pmatrix} \begin{pmatrix} a_{11} & \cdots & a_{1s} \\ \vdots & & \vdots \\ a_{p1} & \cdots & a_{ps} \\ \vdots & & \vdots \\ a_{q1} & \cdots & a_{qs} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{ns} \end{pmatrix}$$

$$\begin{pmatrix} a_{11} & \cdots & a_{1s} \\ \vdots & & \vdots \\ a_{q-11} & \cdots & a_{q-1s} \\ \vdots & & \vdots \\ \lambda a_{p1} + \beta a_{q1} & \cdots & \lambda a_{ps} + \beta a_{qs} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{ns} \end{pmatrix} \leftarrow q \tag{7.31}$$

o, en notación por filas:

$$C_{i\bullet} = A_{i\bullet} \qquad \forall i \neq q$$
$$C_{q\bullet} = \lambda A_{p\bullet} + \beta A_{q\bullet}$$

Se tiene, entonces, que el efecto sobre A, de la premultiplicación por $E_{pq}(\lambda, \beta)$ es una matriz que sólo difiere de A en la fila q: ésta es la suma de la fila p ponderada por λ y la fila q ponderada por β. Es importante observar que las matrices $E_{pq}(\lambda, \beta)$ son *triangulares inferiores* y además *invertibles*. Su inversa es la siguiente:

$$E_{pq}^{-1}(\lambda,\beta) = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & \bigcirc & & \\ & & 1 & & & & \\ & -\frac{\lambda}{\beta} & \cdots & \frac{1}{\beta} & & \cdots & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}$$

$$\begin{matrix} \uparrow & & \uparrow \\ p & & q \end{matrix}$$

En efecto, es directo de la definición que:

$$E_{pq}^{-1}(\lambda,\beta) = E_{pq}(-\frac{\lambda}{\beta}, \frac{1}{\beta}).$$

Luego, $C = E_{pq}(-\frac{\lambda}{\beta}, \frac{1}{\beta})E_{pq}(\lambda, \beta)$ es la matriz cuya fila q es la suma de la fila p de $E_{pq}(\lambda, \beta)$, ponderada por $-\frac{\lambda}{\beta}$ y la fila q de $E_{pq}(\lambda, \beta)$, ponderada por $\frac{1}{\beta}$. Es decir,

$$C_{q\bullet} = -\frac{\lambda}{\beta}(0...0\ \underset{p}{\uparrow}\ 0...1...0) + \frac{1}{\beta}(0...\lambda\ \underset{p}{\uparrow}\ 0...0\ \underset{q}{\uparrow}\ \beta\ 0...0)$$

$$= (0...0\ \underset{p}{\uparrow}\ \frac{-\lambda}{\beta}\ 0...0) + (0...\frac{\lambda}{\beta}\ \underset{p}{\uparrow}\ 0...0\ \underset{q}{\uparrow}\ 1\ 0...0)$$

luego:

$$C_{q\bullet} = (0...0\ \underset{q}{\uparrow}\ 1\ 0...0)$$

además, $\forall i \neq q$

$$C_{i\bullet} = (0...0\ \underset{i}{\uparrow}\ 1\ 0...0).$$

Ergo $C = I$, la matriz identidad ■

7.4 Sistemas lineales y escalonamiento de matrices.

Las matrices elementales son de gran utilidad en la resolución de sistemas de ecuaciones lineales. Consideremos, a modo de ejemplo, el sistema de ecuaciones de primer grado en $\mathbb{R}$

$$\begin{aligned} x_1 + 2x_2 + x_3 + x_4 &= 2 \qquad (1)\\ -2x_1 + 3x_2 - x_3 &= -1 \qquad (2)\\ x_1 \quad + x_3 + x_4 &= 1 \qquad (3)\end{aligned}$$

Para resolverlo utilizamos la eliminación de variables, pero en forma ordenada, desde la primera variable de la izquierda y desde arriba hacia abajo:

1. Eliminamos la variable x_1 en las ecuaciones (2) y (3); para ello multiplicamos la primera por dos y la sumamos a la segunda obteniendo:

$$\begin{aligned} x_1 + 2x_2 + x_3 + x_4 &= 2\\ 7x_2 + x_3 + 2x_4 &= 3\\ x_1 \quad + x_3 + x_4 &= 1\end{aligned}$$

Luego, multiplicamos la primera por -1 y la sumamos a la tercera:

$$\begin{aligned} x_1 + 2x_2 + x_3 + x_4 &= 2\\ 7x_2 + x_3 + 2x_4 &= 3\\ -2x_2 \quad\quad &= -1.\end{aligned}$$

2. Continuamos ahora con x_2, pero a partir de la segunda ecuación. Multiplicando la segunda por $\frac{2}{3}$ y sumándola a la tercera se obtiene:

$$\begin{aligned} x_1 + 2x_2 + x_3 + x_4 &= 2\\ 7x_2 + x_3 + 2x_4 &= 3\\ \frac{2}{7}x_3 + \frac{4}{7}x_4 &= -\frac{1}{7}.\end{aligned}$$

Ya no es posible eliminar más variables. Ahora, desde la última hasta la primera ecuación, despejamos en función de x_4:

$$x_3 = -\frac{4}{2}x_4 - \frac{1}{2} = -2x_4 - \frac{1}{2}$$

$$x_2 = \frac{1}{7}(-x_3 - 2x_4 + 3) = \frac{1}{7}(2x_4 + \frac{1}{2} - 2x_4 + 3) = \frac{1}{2}$$

$$x_1 = -2x_2 - x_3 - x_4 + 2 = -2\frac{1}{2} + 2x_4 + \frac{1}{2} - x_4 + 2 = x_4 + \frac{3}{2}.$$

Obteniéndose la solución:

$$\begin{aligned} x_1 &= \frac{3}{2} + x_4\\ x_2 &= \frac{1}{2}\\ x_3 &= -\frac{1}{2} - 2x_4\\ x_4 &= x_4.\end{aligned}$$

Así, para cualquier valor real de x_4, obtenemos una solución del sistema. Existen, entonces, infinitas soluciones (recuerde que $\mathbb{R}$ es infinito), dependiendo de los valores de x_4. La variable x_4 se denomina *independiente* y x_1, x_2, x_3 variables *dependientes*.

En general, en un cuerpo $\mathcal{K}$, un sistema *lineal* de m *ecuaciones* y n *incógnitas* consiste en determinar los valores de las variables $x_1, ..., x_n \in \mathcal{K}$ tales que:

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= b_1\\ \vdots \qquad\qquad &\vdots \qquad \vdots\\ a_{m1}x_1 + \cdots + a_{mn}x_n &= b_m,\end{aligned}$$

donde los coeficientes, a_{ij}, y el lado derecho, b_j, son elementos del cuerpo $\mathcal{K}$.

Definiendo la matriz:

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \in M_{mn}(\mathcal{K})$$

y la m-tupla (*lado derecho*) y n-tupla de *incógnitas*

$$b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in \mathcal{K}^m, \quad x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathcal{K}^n.$$

Podemos escribir el sistema matricialmente:

$$Ax = b. \tag{7.32}$$

En este contexto A se denomina la *matriz de coeficientes* y b, el *lado derecho* del sistema.

Realizar el procedimiento de eliminación de variables descrito en el ejemplo precedente, con el fin de resolver el sistema, es equivalente a producir "ceros" en la matriz aumentada $(A|b)$, (agregando b como nueva columna). En el ejemplo anterior:

$$(A|b) = \begin{pmatrix} 1 & 2 & 1 & 1 & 2 \\ -2 & 3 & -1 & 0 & -1 \\ 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Eliminar x_1 de la segunda ecuación es equivalente a producir un cero en la posición (2,1) de $(A|b)$. Para ello se multiplica la primera fila por -2 y se suma a la segunda fila. Para eliminar x_1 de la tercera: ecuación se multiplica la primera fila por -1 y se suma a la tercera

$$(A|b) \to \begin{pmatrix} 1 & 2 & 1 & 1 & 2 \\ 0 & 7 & 1 & 2 & 3 \\ 1 & 0 & 1 & 1 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 1 & 1 & 2 \\ 0 & 7 & 1 & 2 & 3 \\ 0 & -2 & 0 & 0 & -1 \end{pmatrix}.$$

Eliminar x_2 en la tercera ecuación a partir de la segunda es equivalente a multiplicar la segunda fila por $\frac{2}{7}$ y sumarla a la tercera:

$$\to \begin{pmatrix} 1 & 2 & 1 & 1 & 2 \\ 0 & 7 & 1 & 2 & 3 \\ 0 & 0 & \frac{2}{7} & \frac{4}{7} & -\frac{1}{7} \end{pmatrix} = (\tilde{A}|\tilde{b}).$$

Así, el sistema inicial es equivalente al sistema $\tilde{A}x = \tilde{b}$.

Conviene señalar que en el procedimiento anterior la operación de base ha sido:

sumar a una fila q, la fila p ponderada por un número $\lambda \in \mathcal{K}$. (7.33)

De la definición de matrices elementales sabemos que esto es equivalente a premultiplicar por la izquierda por la matriz $E_{pq}(\lambda, 1)$. Veamos esto en el mismo ejemplo.

1. Producir un cero en la posición (2,1) de $(A|b)$:

$$E_{12}(2,1)(A|b) = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 1 & 1 & 2 \\ -2 & 3 & -1 & 0 & -1 \\ 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 1 & 1 & 2 \\ 0 & 7 & 1 & 2 & 3 \\ 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

2. Producir un cero en la posición (3,1):

$$E_{13}(-1,1)E_{12}(2,1)(A|b) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 1 & 1 & 2 \\ 0 & 7 & 1 & 2 & 3 \\ 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 1 & 1 & 1 \\ 0 & 7 & 1 & 2 & 3 \\ 0 & -2 & 0 & 0 & -1 \end{pmatrix}.$$

3. Producir un cero en la posición (3,2) desde la posición (2,2):

$$E_{23}(\tfrac{2}{7},1)E_{13}(-1,1)E_{12}(2,1)(A|b) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \frac{2}{7} & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 1 & 1 & 2 \\ 0 & 7 & 1 & 2 & 3 \\ 0 & -2 & 0 & 0 & -1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 1 & 1 & 2 \\ 0 & 7 & 1 & 2 & 3 \\ 0 & 0 & \frac{2}{7} & \frac{4}{7} & -\frac{1}{7} \end{pmatrix}.$$

Se concluye, entonces, que la operación de eliminación de variable puede realizarse mediante la pre-multiplicación de $(A|b)$ por matrices elementales. Hay casos en que también es necesario utilizar matrices de permutación de filas. Por ejemplo, si se tiene

$$(A|b) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 2 & 0 & 1 \end{pmatrix}$$

vemos que, como $a_{22} = 0$, no es posible "producir" ceros en la segunda columna, a partir de a_{22}. Luego intercambiamos el orden de las filas (¡claramente, esto no cambia el sistema de ecuaciones asociado!). Por ejemplo, colocamos la cuarta fila en la segunda posición y la segunda en la cuarta. Esto es equivalente a premultiplicar por I_{24}:

$$I_{24}(A|b) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 2 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

lo cual nos permite seguir produciendo ceros.

Consideremos ahora $A \in M_{mn}(\mathcal{K})$, definimos la matriz *escalonada* asociada a la matriz A, como $\tilde{A} \in M_{mn}(\mathcal{K})$, tal que:

$$\tilde{A} = \begin{pmatrix} \tilde{a}_{11} & \tilde{a}_{12} & \cdots & \tilde{a}_{1i_2} & \cdots & \cdots & \cdots & \cdots & \tilde{a}_{1n} \\ & & & \tilde{a}_{2i_2} & \cdots & \cdots & \cdots & \cdots & \tilde{a}_{2n} \\ & & & & & \ddots & & & \vdots \\ & & & & & & & \tilde{a}_{si_s} & \cdots & \tilde{a}_{sn} \\ & & & & & & & & & \\ & \bigcirc & & & & & & \bigcirc & & \end{pmatrix} \tag{7.34}$$

donde los elementos $\tilde{a}_{11} \neq 0$, $\tilde{a}_{2i_2} \neq 0, ..., \tilde{a}_{si_s} \neq 0$, se denominan *pivotes*.

La matriz $\tilde{A}$ se obtiene mediante la premultiplicación de A por matrices elementales:

$$\tilde{A} = (\prod_j E_j)A, \tag{7.35}$$

donde E_j es una matriz elemental de suma o de permutación de filas.

Además, recordemos que las matrices elementales son invertibles. Esta propiedad es crucial para probar que el sistema original, $Ax = b$, y el obtenido

después del escalonamiento, $\tilde{A}x = \tilde{b}$, son *equivalentes* (tienen idéntico conjunto de soluciones). En efecto,

Dada una matriz C invertible, entonces:

$$a \in K^n \textit{es solución de } Ax = b \textit{ si y sólo si es solución de } (CA)x = Cb. \tag{7.36}$$

La demostración es simple:

$\Longrightarrow$) Si $Aa = b \Longrightarrow C(Aa) = Cb \Longrightarrow (CA)a = Cb$.

$\Longleftarrow$) Supongamos $(CA)a = Cb$. Como C es invertible, se tiene $C^{-1}(CA)a = C^{-1}(Cb) \Longleftrightarrow Aa = b$ ∎

Como las matrices elementales son invertibles y el producto de matrices invertibles también lo es, concluímos que los sistemas $Ax = b$ y $\tilde{A}x = \tilde{b}$ son equivalentes.

7.5 Solución general de sistemas lineales.

Dado el sistema $Ax = b, A \in M_{mn}(\mathcal{K}), b \in \mathcal{K}^m, x \in \mathcal{K}^n$, al escalonarlo (escalonando $(A|b)$) obtenemos:

$$(\tilde{A}|\tilde{b}) = \begin{pmatrix} \tilde{a}_{11} & \cdots & & \tilde{a}_{1i_2} & \cdots & \cdots & \cdots & \tilde{a}_{1n} & \tilde{b}_1 \\ 0 & \cdots & 0 & \tilde{a}_{2i_2} & & & & \vdots & \vdots \\ \vdots & & \vdots & \vdots & \ddots & & & \vdots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & \tilde{a}_{si_s} & \cdots & \tilde{a}_{sn} & \tilde{b}_s \\ 0 & \cdots & 0 & 0 & \cdots & 0 & \cdots & 0 & \tilde{b}_{s+1} \\ \vdots & & & \vdots & & & & \vdots & \vdots \\ 0 & \cdots & & 0 & \cdots & 0 & \cdots & 0 & \tilde{b}_m \end{pmatrix} \tag{7.37}$$

donde los elementos $\tilde{a}_{11}, \tilde{a}_{2i_2}, ..., \tilde{a}_{si_s}$ son no nulos. Claramente, si existe un índice $j \geq s+1$ tal que $\tilde{b}_j \neq 0$, el sistema no tiene solución, ya que se tendría una ecuación incompatible: $0 = \tilde{b}_j \neq 0$.

Luego, el sistema tiene solución si y solo si $\tilde{b}_k = 0 \; \forall k \geq s+1$. En efecto, si $\tilde{b}_k = 0, \forall k \geq s+1$, se obtiene la(s) solución(es) despejando desde la s-ésima ecuación hasta la primera en función de las variables independientes.

Notemos además que

$$\textit{si existe solución, y en la matriz } \tilde{A} \textit{ hay algún peldaño de largo mayor o igual a dos, entonces existe más de una solución.} \tag{7.38}$$

En efecto, supongamos que la k-ésima fila de $\tilde{A}$ es un peldaño de largo superior a uno:

$$\begin{pmatrix} \tilde{a}_{11} & \cdots & & \tilde{a}_{1i_{k+1}} & \cdots & \cdots & \cdots & \cdots & \tilde{a}_{1n} \\ & \ddots & & \cdots & \cdots & & & & \vdots \\ 0 & \cdots & \tilde{a}_{ki_k} & \tilde{a}_{ki_k+1} & \tilde{a}_{ki_k+2} & & \cdots & \cdots & \tilde{a}_{kn} \\ 0 & 0 & 0 & 0 & \tilde{a}_{k+1i_{k+1}} & \cdots & \cdots & \cdots & \tilde{a}_{k+1n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & & & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & \tilde{a}_{si_s} & \cdots & \tilde{a}_{sn} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \tilde{b}_1 \\ \vdots \\ \vdots \\ \tilde{b}_s \\ 0 \\ \vdots \\ \vdots \\ 0 \end{pmatrix}$$

1. Si la columna $\tilde{A}_{\bullet i_k+1}$ es nula, entonces el sistema $\tilde{A}x = \tilde{b}$ no depende de la variable x_{i_k+1}, luego ésta puede tomar cualquier valor en $\mathcal{K}$, existiendo tantas soluciones como sea la cardinalidad del cuerpo $\mathcal{K}$.

2. Si $\tilde{A}_{\bullet i_k+1}$ no es nula, podemos despejar las variables asociadas a los pivotes $x_{i_1} = x_1,\ x_{i_2}, ..., x_{i_k}$:

$$x_{i_\ell} = \frac{1}{\tilde{a}_{\ell i_\ell}}(\tilde{b}_\ell - \sum_{j=i_\ell+1}^{n} \tilde{a}_{\ell j}x_j),\ 1 \leq \ell \leq k.$$

Como $i_\ell < i_k + 1$ entonces x_{i_ℓ} depende de $\tilde{a}_{\ell i_k+1}x_{i_k+1}$. Además, x_{i_k+1} no depende de las variables x_j, $\forall j \geq i_k + 2$, pues su coeficiente es nulo a partir de la fila $k+1$. Luego, para cada valor de $x_{i_k+1} \in \mathcal{K}$ se obtiene una solución del sistema ■

Un corolario directo del resultado anterior es:

si $n > m$ (número de incógnitas mayor que el número de ecuaciones), entonces, el sistema tiene más de una solución. (7.39)

En efecto, como $n > m$ siempre existe en la matriz escalonada, $\tilde{A}$, un peldaño de largo superior o igual a dos. De no ser así se tendría

$$\tilde{A} = \begin{pmatrix} \tilde{a}_{11} & \tilde{a}_{12} & \cdots & \tilde{a}_{1n} \\ 0 & \tilde{a}_{22} & \cdots & \tilde{a}_{2n} \\ \vdots & 0 & & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \tilde{a}_{mn} \end{pmatrix}$$

de donde $m = n$ ■

Observemos que si el cuerpo $\mathcal{K}$ es infinito (por ejemplo $\mathcal{K} = \mathbb{R}$ o $\mathcal{K} = \mathbb{C}$), la existencia de un peldaño de largo ≥ 2, implica que existen *infinitas soluciones.*

Un caso particular importante es cuando el lado derecho del sistema es nulo, $b = 0$. Hablamos entonces de un *sistema homogéneo*, $Ax = 0$. Vemos que, en este caso, siempre existe *al menos* una solución, la trivial $x = 0 \in \mathcal{K}^n$.

Podemos resumir nuestro estudio de sistemas en el cuadro siguiente:

	Sistema homogéneo ($b = 0$)		Sistema no-homogéneo ($b \neq 0$)	
Dimensión	$n \leq m$	$n > m$	$n \leq m$	$n > m$
Número soluciones	$1, > 1$	> 1	$0, 1, > 1$	$0, > 1$
$\mathcal{K}$ cuerpo infinito	$1, \infty$	∞	$0, 1, \infty$	$0, \infty$.

Donde "> 1" debe leerse "más de una solución" y "∞" como infinitas soluciones.

Ejemplo: Resolvamos el sistema

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ -1 & 2 & 0 & -1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & -1 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Escalonando:

$$(A|b) \to \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 3 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & -2 & 0 & 0 & -1 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 3 & 1 & 0 & 1 & 1 \\ 0 & 0 & \frac{2}{3} & 0 & \frac{2}{3} & -\frac{1}{3} \\ 0 & 0 & \frac{2}{3} & 0 & -\frac{1}{3} & \frac{2}{3} \end{pmatrix} \to$$

$$\to \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 3 & 1 & 0 & 1 & 1 \\ 0 & 0 & \frac{2}{3} & 0 & \frac{2}{3} & -\frac{1}{3} \\ 0 & 0 & 0 & 0 & -1 & 1 \end{pmatrix}.$$

Obtenemos:

$$x_5 = -1$$
$$x_3 = \frac{3}{2}(-\frac{1}{3} - \frac{2}{3}x_5) = -\frac{1}{2} - x_5 = -\frac{1}{2} + 1 = \frac{1}{2}$$
$$x_2 = \frac{1}{3}(1 - x_3 - x_5) = \frac{1}{3}(1 - \frac{1}{2} + 1) = \frac{1}{2}$$
$$x_1 = 1 - x_2 - x_3 - x_4 - x_5 = 1 - \frac{1}{2} - \frac{1}{2} - x_4 + 1 = 1 - x_4.$$

La solución general es:

$$x_1 = 1 - x_4, x_2 = \frac{1}{2}, x_3 = \frac{1}{2},\ x_4 = x_4, x_5 = -1.$$

Existen entonces infinitas soluciones ($n = 5 > 4 = m$), de acuerdo a los valores de la variable independiente $x_4 \in \mathbb{R}$.

7.6 Sistemas cuadrados y algoritmo de Gauss.

Supongamos que el número de ecuaciones es igual al número de incógnitas ($n = m$), en este caso el sistema se escribe:

$$Ax = b,\ A \in M_{nn}(\mathcal{K}), x, b \in \mathcal{K}^n.$$

Escalonemos el sistema y sea $\tilde{A}$ la matriz escalonada, sin considerar el nuevo lado derecho $\tilde{b}$:

$$\tilde{A} = \begin{pmatrix} \tilde{a}_{11} & \cdots & \tilde{a}_{1n} \\ & \ddots & \\ \bigcirc & & \tilde{a}_{nn} \end{pmatrix}$$

donde entre los elementos de la diagonal, $\tilde{a}_{ii}$, podrían haber algunos nulos. Señalemos que en el caso de matrices cuadradas el proceso de escalonamiento se denomina *algoritmo de Gauss*. Un resultado importante, que relaciona matrices invertibles, solución de sistemas y el algoritmo de Gauss, es el siguiente:

Las proposiciones siguientes son equivalentes:

$$A \text{ es invertible.} \tag{7.40}$$

$$\forall b \in \mathcal{K}^n, Ax = b \text{ tiene solución única.} \tag{7.41}$$

$$\prod_{i=1}^{n} \tilde{a}_{ii} \neq 0. \tag{7.42}$$

Demostración. (7.40) $\Longrightarrow$ (7.41).

Si A es invertible $\Longrightarrow \exists A^{-1} \Longrightarrow (A^{-1}A)x = A^{-1}b \Longleftrightarrow x = A^{-1}b$, luego el sistema tiene solución.

Si $x^1, x^2 \in \mathcal{K}^n$ son soluciones:

$$Ax^1 = Ax^2 \Longleftrightarrow (A^{-1}A)x^1 = (A^{-1}A)x^2 \Longleftrightarrow x^1 = x^2.$$

(7.41) $\Longrightarrow$ (7.42). Sea $\tilde{A}$ la matriz escalonada asociada a A tal que admite algún pivote nulo. Consideremos en este caso el que está más abajo en la diagonal, es decir $k = \max\{i/\tilde{a}_{ii} = 0\}$, luego $\forall j > k$, $\tilde{a}_{jj} \neq 0$. Se tiene entonces:

$$\tilde{A} = \begin{pmatrix} \tilde{a}_{11} & & & & & & \tilde{a}_{1n} \\ & \ddots & & & & & \vdots \\ & & \tilde{a}_{k-1k-1} & \tilde{a}_{k-1k} & \tilde{a}_{k-1k+1} & \cdots & \tilde{a}_{k-1n} \\ & & 0 & 0 & \tilde{a}_{kk+1} & \cdots & \tilde{a}_{kn} \\ & & & & \tilde{a}_{k+1k+1} & \cdots & \tilde{a}_{k+1n} \\ & \bigcirc & & & & \ddots & \vdots \\ & & & & & & \tilde{a}_{nn} \end{pmatrix}$$

donde $\tilde{a}_{k+1k+1} \neq 0, ..., \tilde{a}_{nn} \neq 0$.

Si $\tilde{a}_{kk+1} \neq 0$, podríamos utilizarlo como pivote para eliminar $\tilde{a}_{k+1k+1}$, lo cual contradice el hecho que en la escalonada $\tilde{A}$, $\tilde{a}_{jj} \neq 0\ \forall j > k$. Pero si $\tilde{a}_{kk+1} = 0$, permutando las filas k y $k+1$ se obtiene

$$I_{kk+1}\tilde{A} = \begin{pmatrix} \tilde{a}_{11} & & & & & & \\ & \ddots & & & & & \\ & & \tilde{a}_{k-1k-1} & \tilde{a}_{k-1k} & \tilde{a}_{k-1k+1} & \cdots & \tilde{a}_{k-1n} \\ & & 0 & 0 & \tilde{a}_{k+1k+1} & \cdots & \tilde{a}_{k+1n} \\ & & & & 0 & \cdots & \tilde{a}_{kn} \\ & \bigcirc & & & 0 & \ddots & \\ & & & & & \ddots & \vdots \\ & & & & & & \tilde{a}_{nn} \end{pmatrix}$$

que contiene un pivote nulo en la fila $k+1$, lo que contradice el hecho que k es la fila de mayor índice donde esto ocurre. Luego, la única posibilidad es que $k = \max\{j/\tilde{a}_{jj} = 0\} = n$ (así no hay contradicción). Pero en este caso, si tomamos el lado derecho ${}^t(0, ..., 0, 1)$ se obtiene el sistema

$$\begin{pmatrix} a_{11} & & \cdots & \tilde{a}_{1n} \\ & \ddots & & \\ \bigcirc & & \tilde{a}_{n-1n-1} & \tilde{a}_{n-1n} \\ & & & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

cuya última ecuación es incompatible $0 \cdot x_n = 1$, luego el sistema, $\tilde{A}x = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$,

no tiene solución, lo cual contradice la hipótesis.

(7.42) $\Longrightarrow$ (7.40). Supongamos $\prod_{i=1}^{n} \tilde{a}_{ii} \neq 0$. Demostrar que A es invertible es equivalente a exhibir $X \in M_{nn}(\mathcal{K})$ tal que: $AX = I$, o de manera equivalente:

$$A \begin{pmatrix} x_{1i} \\ x_{2i} \\ \vdots \\ x_{ni} \end{pmatrix} = e^i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \leftarrow i - \text{ésima posición} \quad 1 \leq i \leq n.$$

Escalonando cada uno de estos sistemas, obtenemos:

$$\begin{pmatrix} \tilde{a}_{11} & \cdots & \tilde{a}_{1n} & \tilde{e}_1^i \\ & \ddots & & \\ \bigcirc & & \tilde{a}_{nn} & \tilde{e}_n^i \end{pmatrix} \quad i \leq i \leq n.$$

Como $\prod_{i=1}^{n} \tilde{a}_{ii} \neq 0$, entonces el sistema

$$\begin{pmatrix} \tilde{a}_{ii} & \cdots & \tilde{a}_{1n} \\ & \ddots & \vdots \\ \bigcirc & & \tilde{a}_{nn} \end{pmatrix} \begin{pmatrix} x_{1i} \\ \vdots \\ x_{ni} \end{pmatrix} = \begin{pmatrix} \tilde{e}_1^i \\ \vdots \\ \tilde{e}_n^i \end{pmatrix}$$

tiene la solución única:

$$x_{ni} = \frac{\tilde{e}_n^i}{\tilde{a}_{nn}}, \; x_{n-1i} = \frac{1}{\tilde{a}_{n-1n-1}}(\tilde{e}_{n-1}^i - \tilde{a}_{n-1n}x_{ni}),$$

$$\vdots$$

$$x_{1i} = \frac{1}{\tilde{a}_{11}}(\tilde{e}_1^i - \sum_{j=2}^{n} \tilde{a}_{1j}x_{ji}), \quad i \leq i \leq n.$$

Luego, para cada lado derecho, e^i, el sistema tiene solución única, determinándose entonces la matriz X tal que $AX = I$ ■

7.7 Cálculo de inversas y sistemas con varios lados derechos.

En la demostración anterior (parte (7.42) $\Rightarrow$ (7.40)), calculamos A^{-1}, resolviendo $Ax = e^i$, donde el lado derecho sólo tiene un 1 en la i-ésima componente:

$$e^i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \qquad 1 \leq i \leq n.$$

Para resolver estos sistemas no es necesario escalonar n veces la matriz A, basta partir con A aumentada con los n lados derechos $(A|e^1, e^2, ..., e^n) = (A|I)$ y escalonarla.

Obviamente, este principio no sólo es válido para el cálculo de inversas, también lo podemos usar para sistemas donde se tiene la misma matriz A asociada a varios lados derechos $\{b^1, ..., b^p\}$.

Para el cálculo de la inversa podemos ir un poco más lejos. Consideremos, a modo de ejemplo

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

luego:

$$(A|I) = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & -1 & 2 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Escalonando:

$$(A|I) \rightarrow \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & -1 & 2 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & -2 & 2 & 0 & 1 & -1 \\ 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

$$\rightarrow \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & -2 & 2 & 0 & 1 & -1 \\ 0 & 0 & 2 & 1 & \frac{1}{2} & \frac{1}{2} \end{pmatrix}.$$

En este paso ya estamos en condiciones de resolver los tres sistemas. Pero podemos aún pivotear, ahora sobre la diagonal, sin alterar la solución (ya que multiplicamos por matrices invertibles):

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & -2 & 2 & 0 & 1 & -1 \\ 0 & 0 & 2 & 1 & \frac{1}{2} & -\frac{1}{2} \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 1 & 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & -2 & 2 & 0 & 1 & -1 \\ 0 & 0 & 2 & 1 & \frac{1}{2} & -\frac{1}{2} \end{pmatrix}$$

$$\to \begin{pmatrix} 1 & 0 & 1 & 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & -2 & 0 & -1 & \frac{1}{2} & -\frac{1}{2} \\ 0 & 0 & 2 & 1 & \frac{1}{2} & -\frac{1}{2} \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & -\frac{1}{2} & \frac{1}{4} & \frac{3}{4} \\ 0 & -2 & 0 & -1 & \frac{1}{2} & -\frac{1}{2} \\ 0 & 0 & 2 & 1 & \frac{1}{2} & -\frac{1}{2} \end{pmatrix}.$$

Finalmente, premultiplicando por la matriz invertible:

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -\frac{1}{2} & 0 \\ 0 & 0 & \frac{1}{2} \end{pmatrix}.$$

Se tiene:

$$(I|\tilde{I}) = \begin{pmatrix} 1 & 0 & 0 & -\frac{1}{2} & \frac{1}{4} & \frac{3}{4} \\ 0 & 1 & 0 & \frac{1}{2} & -\frac{1}{4} & \frac{1}{4} \\ 0 & 0 & 1 & \frac{1}{2} & \frac{1}{4} & -\frac{1}{4} \end{pmatrix}.$$

Obteniendo los sistemas de solución trivial:

$$I\begin{pmatrix} x_{11} \\ x_{21} \\ x_{31} \end{pmatrix} = \begin{pmatrix} -\frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \end{pmatrix}, I\begin{pmatrix} x_{12} \\ x_{22} \\ x_{32} \end{pmatrix} = \begin{pmatrix} \frac{1}{4} \\ -\frac{1}{4} \\ \frac{1}{4} \end{pmatrix}, I\begin{pmatrix} x_{13} \\ x_{23} \\ x_{33} \end{pmatrix} = \begin{pmatrix} \frac{3}{4} \\ \frac{1}{4} \\ -\frac{1}{4} \end{pmatrix},$$

de donde:

$$X = A^{-1} = \begin{pmatrix} -\frac{1}{2} & \frac{1}{4} & \frac{3}{4} \\ \frac{1}{2} & -\frac{1}{4} & \frac{1}{4} \\ \frac{1}{2} & \frac{1}{4} & -\frac{1}{4} \end{pmatrix}.$$

En efecto:

$$AA^{-1} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & -1 & 2 \\ 1 & 1 & 0 \end{pmatrix}\begin{pmatrix} -\frac{1}{2} & \frac{1}{4} & \frac{3}{4} \\ \frac{1}{2} & -\frac{1}{4} & \frac{1}{4} \\ \frac{1}{2} & \frac{1}{4} & -\frac{1}{4} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Luego, para calcular la inversa de $A \in M_{nn}(\mathcal{K})$ basta aplicar el algoritmo de Gauss sobre la matriz $(A|I)$. Una vez que se ha obtenido la matriz triangular superior $\tilde{A}$, realizar el mismo procedimiento para los elementos sobre la diagonal. Finalmente, se premultiplica por una matriz diagonal para obtener la identidad en el lugar de $\tilde{A}$.

¿Qué sucede si una matriz A no es invertible? Sabemos que necesariamente aparecerá, al escalonar, un pivote nulo "irreparable". Por ejemplo:

$$(A|I) = \begin{pmatrix} 1 & 0 & 2 & 1 & 0 & 0 \\ 1 & 1 & 2 & 0 & 1 & 0 \\ 1 & 0 & 2 & 0 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 2 & 1 & 0 & 0 \\ 0 & 1 & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & -1 & 0 & 1 \end{pmatrix}$$

y los sistemas $\tilde{A}x = \begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix}, \tilde{A}x = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ son incompatibles.

Pero, en ocasiones hay pivotes nulos "reparables". Por ejemplo:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & -1 & -1 & 1 & 0 \\ 0 & -1 & -1 & -1 & 0 & 1 \end{pmatrix}.$$

Acá el elemento $\tilde{a}_{22} = 0$, pero podemos, premultiplicando por la matriz de permutación I_{23}, intercambiar las filas 2 y 3, obteniendo:

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

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

$$\Longrightarrow A^{-1} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & -1 \\ 1 & -1 & 0 \end{pmatrix}.$$

Luego,

si en el algoritmo de Gauss determinamos $\tilde{a}_{kk} = 0$ tal que $\tilde{a}_{jk} = 0\ \forall j > k$, entonces no existe la matriz inversa. (7.43)

Esto se deduce directamente del hecho que existe A^{-1} si y sólo si $\prod_i \tilde{a}_{ii} \neq 0$.

7.8 Factorización LU.

Supongamos que al escalonar $A \in M_{nn}(\mathcal{K})$ no encontramos pivotes nulos (¡no permutamos filas!). Se obtiene entonces

$$\begin{pmatrix} \tilde{a}_{11} & \cdots & \tilde{a}_{1p} \\ & \ddots & \\ \bigcirc & & \tilde{a}_{nn} \end{pmatrix} = (\prod_j E_j)A,$$

donde cada una de las matrices E_j es de la forma:

$$\begin{pmatrix} 1 & & & \\ & \ddots & & \bigcirc \\ & \lambda & 1 & \\ \cdots & \cdots & & \ddots \\ 0 & & & 1 \end{pmatrix}, \quad \lambda \in \mathcal{K}.$$

Luego, las matrices E_j son triangulares inferiores, invertibles y con unos en la diagonal. Despejando:

$$A = (\prod_j E_j)^{-1} \begin{pmatrix} \tilde{a}_n & \cdots & \tilde{a}_{1n} \\ & \vdots & \\ \bigcirc & & \tilde{a}_{nn} \end{pmatrix}.$$

Como el producto y la inversa de matrices triangulares inferiores es triangular inferior es fácil verificar que

$$L = (\prod_j E_j)^{-1} = \begin{pmatrix} 1 & & \\ \ell_{21} & \ddots & \bigcirc \\ \cdots & \ddots & \ddots \\ \ell_{n1} & \cdots & \ell_{nn-1} 1 \end{pmatrix}$$

de donde obtenemos la *factorización LU*:

$$A = L \cdot U = \begin{pmatrix} 1 & & & \\ \ell_{21} & \ddots & & \bigcirc \\ \vdots & & \ddots & \\ \ell_{n1} & \cdots & \ell_{n-1} & 1 \end{pmatrix} \begin{pmatrix} \tilde{a}_{11} & \cdots & \tilde{a}_{1n} \\ & \ddots & \\ \bigcirc & & \tilde{a}_{nn} \end{pmatrix} \tag{7.44}$$

Concluímos entonces que, si al escalonar A no se realizan permutaciones, A puede factorizarse como el producto de una matriz L, triangular inferior

con unos en la diagonal, y una matriz U, triangular superior, donde los pivotes figuran en la diagonal.

Más aún, como $\prod_{i=1}^{n} \tilde{a}_{ii} \neq 0$, podemos escribir

$$A = LDU \tag{7.45}$$

$$= \begin{pmatrix} 1 & & & \\ \ell_{21} & \ddots & \bigcirc & \\ \vdots & & \ddots & \\ \ell_{n1} & \cdots & \ell_{nn-1} & 1 \end{pmatrix} \begin{pmatrix} \tilde{a}_{11} & & \bigcirc & \\ & \ddots & & \\ \bigcirc & & \tilde{a}_{nn} & \end{pmatrix} \begin{pmatrix} 1 & \frac{\tilde{a}_{12}}{\tilde{a}_{11}} & \cdots & \frac{\tilde{a}_{1n}}{\tilde{a}_{11}} \\ & \ddots & & \\ \bigcirc & & 1 & \frac{\tilde{a}_{n-1n}}{\tilde{a}_{n-1n}} \\ & & & 1 \end{pmatrix}$$

donde L es triangular inferior con unos en la diagonal, D es diagonal (formada por los pivotes del escalonamiento) y U es triangular superior con diagonal de unos.

Veamos un ejemplo:

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

$$E_{13}(-1,1)A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 2 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & -1 \end{pmatrix}$$

$$E_{23}(-1,1)E_{13}(-1,1)A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 2 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & -2 \end{pmatrix} = U.$$

Luego: $A = E_{13}^{-1}(-1,1)E_{23}^{-1}(-1,1)U$

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

$$= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & -2 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -2 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

$$= LDU.$$

7.9 Complejidad del algoritmo de Gauss.

Una medida de la calidad de un algoritmo es el tiempo que éste requiere en un computador. Para muchos algoritmos, en particular para Gauss, el tiempo está asociado al número de operaciones aritméticas que debe realizar. Este número es una medida de lo que se denomina *complejidad* del algoritmo.

Analicemos entonces, en esta óptica, el algoritmo de Gauss. Consideraremos solamente las multiplicaciones y las divisiones que éste realiza para *triangularizar* (llevar a la forma triangular) una matriz (las sumas y restas son de ejecución muy rápida en el computador y este tiempo es despreciable con respecto al asociado a las otras dos operaciones).

1. Para producir un cero, utilizando como pivote a_{11}, en la posición (2,1) es necesario realizar la división $\frac{a_{21}}{a_{11}} = \lambda$, y posteriormente multiplicar $n-1$ elementos (sin contar a_{11}, ya que sabemos que él produce el cero):

$$\lambda a_{12}, ..., \lambda a_{1n}$$

Es decir, el "0" en la posición (2,1) "cuesta" $n-1$ multiplicaciones más 1 división $= n$ operaciones. Concluímos que, en el peor de los casos, producir los $n-1$ ceros de la primera columna requieren $(n-1)n$ operaciones.

De manera análoga, para la i-ésima columna cada "0" cuesta 1 división más $n-i$ multiplicaciones $= n-i+1$ operaciones y para producir los $n-i$ ceros se requieren $(n-i)(n-i+1)$ operaciones.

Se tiene, entonces, que el número total de operaciones es:

$$\sum_{i=1}^{n}(n-i)(n-i+1) = \frac{n^3}{3} + \text{ términos de orden menor.}$$

Observemos que la complejidad de Gauss, medida como número de operaciones, no difiere demasiado del cálculo de un producto matricial A^2, que requiere n^3 multiplicaciones. Si desea "bucear" en este tópico, no deje de leer el tema 2, al final del capítulo.

Ejercicios.

1. Demuestre rigurosamente la asociatividad y la distributividad de $\cdot$ con respecto a $+$ en las matrices de $n \times n$ sobre un anillo conmutativo $(\mathcal{R}, +, \cdot)$.
2. Sea $A = (a_{ij}) \in M_{nn}(\mathbb{R})$ tal que $a_{ii} = 1$, $a_{i,i+1} = -1$, a_{n1}, $a_{1n} = -1$, y el resto de los coeficientes nulos. Determine el valor de Ax, ${}^tyA$, AB para $x, y \in \mathbb{R}^n$, $B \in M_{nn}(\mathbb{R})$ arbitraria.
3. (a) Dadas las matrices

$$A = \begin{pmatrix} 2 & -2 & -2 \\ -2 & 2 & 2 \\ -1 & 1 & 1 \end{pmatrix} \text{ en } M_{33}(\mathbb{R})$$

y

$$B = \begin{pmatrix} 1 & -i & -1 \\ i & 1 & i \\ 1 & -i & 1 \end{pmatrix} \text{ en } M_{33}(\mathbb{C}),$$

determine A^n y B^n en función de n (justifique).

(b) Sean A, B, $A^{-1}+B$ y $A+B^{-1}$ matrices invertibles. Demuestre que

$$(A^{-1}+B)^{-1} = A(A+B^{-1})^{-1}B^{-1}.$$

(c) Si A es matriz triangular superior en $M_{33}(\mathbb{R})$ tal que $a_{ii} = 1$ para $i = 1,2,3$ y $N = A - I$ (I: matriz identidad), demuestre que $N^3 = 0$ y $A^{-1} = I - N + N^2$.

4. Sea $\mathcal{K}$ un cuerpo. Sea el conjunto de matrices en $M_{nn}(\mathcal{K})$:

$$M_{pq} = (m_{ij}), \quad m_{ij} = \begin{cases} 1 & \text{si } i = p,\ j = q \\ 0 & \text{si no} \end{cases}$$

(a) Demuestre que $\forall A \in M_{nn}(A)$: $A = a_{11}M_{11} + a_{12}M_{12} + ... + a_{nn}M_{nn}$

(b) Demuestre que $\forall p, q$, M_{pq} no es invertible.

(c) Sea $\mathcal{K}^{nm}$ el conjunto de las nm-tuplas con valores en un cuerpo $\mathcal{K}$ y sean las operaciones: $\forall x, y \in \mathcal{K}^{nm}$: $X + Y = (x_i + y_i)$ $= (x_1 + y_1, ..., x_{nm} + y_{nm})$.

$X \cdot Y = (x_1, ..., x_{nm}) \begin{pmatrix} y_1 \\ \vdots \\ y_{nm} \end{pmatrix}$, multiplicación de matrices de $(1 \times nm)$ por $(nm \times 1)$.

Demuestre que $(M_{nn}(\mathcal{K}),+) \cong (\mathcal{K}^{nm},+)$. ¿Son isomorfos $(M_{nn}(\mathcal{K}),\cdot)$ y $(\mathcal{K}^{nm},\cdot)$?

(d) Estudie los productos $M_{ij}M_{kp}$; $i,j,k,p \in \{1,...,n\}$. Además, dados i_0,i_1,i_2,i_3, ¿$M_{i_0i_1}M_{i_1i_2}M_{i_2i_3} = M_{i_0i_3}$?

5. Verifique si son o no invertibles en $M_{nn}(\mathbb{R})$ y/o $M_{nn}(\mathbb{C})$:

$$\begin{pmatrix} a & \cdots & a \\ 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & 0\cdots & 0 \end{pmatrix}, \begin{pmatrix} a & a\cdots a \\ \vdots & & \vdots \\ a & a\cdots a \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & & n \\ 0 & 1 & 0 & 0 & \cdots & & 0 \\ 0 & 0 & 1 & 0 & \cdots & & 0 \\ & & & & & & \vdots \\ & & & & \ddots & & \\ & & & & & 1 & 0 \\ 2 & 4 & 6 & \cdots & \cdots & & 2n \end{pmatrix}, \quad \begin{pmatrix} i & i^2 & i^3 \\ i^2 & 0 & 1 \\ i^3 & 1 & 0 \end{pmatrix}.$$

6. Sean $X,Y \in M_{n1}(\mathbb{R})$ e I la matriz identidad en $M_{nn}(\mathbb{R})$. Demuestre que la inversa de $I - X\,{}^tY$ es $I + \frac{X\,{}^tY}{1-{}^tXY}$.

7. Sea $A = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$

(a) Demuestre que $\forall n \in \mathbb{N}, n \geq 3$:

$$A^n = pA^2 - (p-1)I \quad \text{si } n = 2p$$
$$A^n = pA^2 + A - pI \quad \text{si } n = 2p+1.$$

(b) Para las sucesiones $(u_n),(v_n),(w_n)$, que verifican las relaciones de recurrencia:

$$u_n = u_{n-1}$$
$$v_n = v_{n-1} + w_{n-1}$$
$$w_n = v_{n-1}$$

deduzca de (a) el valor de u_n, v_n y w_n en función de n (y su paridad), y en función de u_1, v_1 y w_1.

8. Demuestre que: $\forall A \in M_{nn}(R)\ \exists B,C \in M_{nn}(R)$, triangulares superior e inferior tales que: $A = B + C$. ¿Esta descomposición es única? Discuta.

¿Es posible factorizar en $M_{22}(\mathbb{R})$ una matriz como producto de una triangular superior y otra inferior:

$$\text{¿} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \begin{pmatrix} x' & 0 \\ y' & z' \end{pmatrix} \quad ?$$

Discuta el problema.

9. Sea $MTS = \{A/A \in M_{nn}(R)$, triangulares superiores $\}$.
(a) Demuestre que $(MTS,+)$ es un subgrupo abeliano de $(M_{nn}(R),+)$.
(b) Estudie $(MTS,\cdot)$. ¿Cuáles son sus propiedades?

10. Dado el conjunto $M_{nn}(\mathbb{R})$ y la aplicación:

$$\varphi : M_{nn}(\mathbb{R}) \to M_{nn}(\mathbb{R})$$
$$A \to I_{pq}A; \quad p < q$$

I_{pq}: matriz de permutación.
(a) Demuestre que φ es un homomorfismo.
(b) ¿Es un isomorfismo?
(c) Demuestre que $\varphi^2 = \varphi \circ \varphi = id$ (función identidad).

11. (a) Demuestre que dado: $M = \{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} / a,b \in \mathbb{R}\}$,
$(M,+,\cdot) \cong (\mathbb{C},+,\cdot)$.
(b) Sea:

$$M = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, \right.$$
$$\left. \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\}.$$

Demuestre que $(M,\cdot)$ es un grupo.

12. Sea DIA el conjunto de las matrices diagonales de $n \times n$. Demuestre que $(DIA,+,\cdot)$ es un subanillo de $(M_{nn}(\mathbb{R}),+,\cdot)$.
Sea $DIA(0) = \{D \in DIA/d_{ii} \neq 0, \quad \forall i = 1,...,n\}$.
Demuestre que $(DIA(0),\cdot)$ es un grupo abeliano.
¿es $(DIA(0) \cup \left\{ \begin{pmatrix} 0\cdots 0 \\ \vdots\ \vdots \\ 0\cdots 0 \end{pmatrix} \right\},+,\cdot)$ un cuerpo?

Sea $\varphi : DIA \to \mathbb{R}^n$, tal que:

$$\begin{pmatrix} \lambda_1 & & 0 \\ & \cdots & \\ 0 & & \lambda_n \end{pmatrix} \to (\lambda_1,\lambda_2,...\lambda_n)$$

Estudie la función φ (morfismos, etc).

(a) Demuestre que: $D \in DIA$ es invertible $\Leftrightarrow \lambda_i \neq 0 \ \forall i = 1, ..., n$.

(b) Verifique que $D^q = \begin{pmatrix} \lambda_1^q & & 0 \\ & \ddots & \\ 0 & & \lambda_n^q \end{pmatrix} \quad \forall q \geq 0.$

13. Sea T el conjunto de las matrices triangulares inferiores de $n \times n$ sobre $\mathbb{R}$. Demuestre que: $U \in T$ es invertible $\Leftrightarrow u_{ii} \neq 0 \quad \forall i = 1, ..., n$.
(b) Sea $T(0) = \{U \in T / u_{ii} = 0 \ \forall i = 1, ..., n\}$ el conjunto de las matrices triangulares superiores estrictas, es decir $u_{ij} = 0$ si $i \leq j$. Demuestre que $\forall U \in T(0)$, $\exists p \in \mathbb{N}$, $p \leq n$ tal que $U^p = 0$ (es decir, las matrices triangulares estrictas son *nilpotentes*).
14. Sean $A, B \in M_{nn}(\mathbb{R})$ simétricas, demuestre:
(a) $A \cdot B$ es simétrica $\Leftrightarrow AB = BA$.
Diremos que $A \in M_{nn}(\mathbb{R})$ es *antisimétrica* si y sólo si: ${}^tA = -A$.
(b) Demuestre que si A es antisimétrica, entonces $a_{ii} = 0 \ \forall i = 1, ..., n$.
(c) Demuestre que $\forall A \in M_{nn}(\mathbb{R})$: $A = C + D$; $C, D \in M_{nn}(\mathbb{R})$, donde C es simétrica y D es antisimétrica. ¿Es esta factorización única?
15. Considere el sistema de ecuaciones:

$$\begin{aligned} x_1 + 3x_2 + 5x_3 + 6x_4 &= 1 \\ 2x_1 + 4x_2 + 7x_3 + x_4 &= 3 \\ 2x_2 + 3x_3 + 11x_4 &= b \end{aligned}$$

(a) Pruebe que dicho sistema tiene solución para un único valor b^*, de b.
(b) Si $b = b^*$ resuelva el sistema.
16. Sea $A \in M_{nn}(\mathbb{R})$. Una matriz $B \in M_{nn}(\mathbb{R})$ se dice *inversa generalizada* de A si $A \cdot B \cdot A = A$. Encuentre una inversa generalizada de A, si:
(a) $A(A + I)(A + 2I) = 0$.
(b) $(A - I)^3 = A - I$.
17. Sea $A = (a_{ij}) \in M_{nn}(\mathbb{R})$, invertible y $B = (1 + a_{ij})$. Sea $M = (m_{ij})$ tal que $m_{ij} = 1 \ \forall i, j$. Pruebe que

$$B^{-1} = A^{-1} - \frac{A^{-1} M A^{-1}}{1 + \sum_i \sum_j a'_{ij}} \quad \text{donde } (a'_{ij}) = A^{-1}.$$

18. Sean $A \in M_{nm}(\mathbb{R})$ y $B \in M_{mn}(\mathbb{R})$.
(a) Muestre que, si las inversas existen, entonces
$(I + AB)^{-1} = I - A(I + BA)^{-1} B$.

(b) Sea $C = (c_{ij})$ con $c_{ij} = \begin{cases} 1 & \text{si } i = j \\ \rho & \text{si } i \neq j \end{cases} \quad i, j = 1, ..., n.$
Escriba C de la forma $I + AB$ y encuentre su inversa.
19. Encuentre la solución general de los sistemas:

(a) $\begin{bmatrix} 0 & 1 & -1 & 2 & -2 & 1 \\ -1 & -1 & -2 & 3 & -1 & -1 \\ -1 & 0 & -3 & 5 & -3 & 0 \\ 1 & 0 & 2 & -1 & 2 & -2 \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ \vdots \\ x_6 \end{bmatrix} = \begin{bmatrix} -7 \\ 4 \\ -3 \\ 8 \end{bmatrix}.$

(b)
$$\begin{aligned} x_2 - 2x_3 + 3x_4 &= 0 \\ x_1 - 3x_2 + 2x_3 + x_4 &= 0 \\ x_1 - x_2 - 2x_3 + 7x_4 &= 0 \\ x_1 + 4x_3 + 10x_4 &= 0. \end{aligned}$$

20. Resuelva completamente el sistema lineal

$$\begin{aligned} \beta x_1 - \beta x_2 - \beta x_3 - \beta x_4 - \beta x_5 &= 0 \\ \alpha x_1 + \alpha x_2 + \alpha x_3 + \alpha x_4 &= \alpha \\ \alpha x_1 + \alpha x_2 + \alpha x_3 &= 0 \\ \beta x_1 - \beta x_2 &= \alpha \\ \gamma x_5 &= 0 \end{aligned}$$

analizando todos los posibles valores que pueden tomar $\alpha, \beta, \gamma \in \mathbb{R}$.
21. Sea $A = (a_{ij}) \in M_{nn}(\mathbb{R})$ tal que $a_{ij} = \begin{cases} i & \text{si } j \geq i \\ j & \text{si } j < i \end{cases}$
¿Puede descomponer A de la forma LU?
22. Encuentre la descomposición LU de las siguientes matrices:

$$(a) \begin{pmatrix} 4 & 1 & 0 \\ 1 & 4 & 1 \\ 0 & 1 & 4 \end{pmatrix} \qquad (b) \begin{pmatrix} -1 & 2 & 1 \\ 3 & 0 & 2 \\ -1 & 2 & 0 \end{pmatrix}$$

$$(c) \begin{pmatrix} -1 & 2 & 4 & 1 \\ -3 & 4 & 0 & 1 \\ 1 & -1 & 2 & 0 \\ 3 & -1 & -1 & 2 \end{pmatrix} \qquad (d) \begin{pmatrix} 4 & 0 & -1 & 1 \\ 1 & -1 & 0 & 2 \\ 2 & 0 & 0 & 1 \\ 7 & -1 & -1 & 5 \end{pmatrix}.$$

23. Sean $A \in M_{nn}(\mathbb{R})$ invertible y $u \in \mathbb{R}^n$. Analice la posibilidad de invertir la matriz $B = \begin{pmatrix} A & u \\ {}^t u & \alpha \end{pmatrix}$, para distintos valores de α y, cuando sea posible, calcule la inversa. Indicación: aplique el método de Gauss para escalonar.

*24. Determine la fórmula de la descomposición LU para una matriz tridiagonal simétrica:

$$A = \begin{pmatrix} \alpha_1 & \beta_1 & & & & & \\ \beta_1 & \alpha_2 & \beta_2 & & & & \\ & \ddots & \ddots & \ddots & & & \\ & & \ddots & \ddots & \ddots & & \\ & & & \ddots & \ddots & \beta_{n-1} & \\ & & & & \beta_{n-1} & \alpha_n & \end{pmatrix}$$

25. Sean $u_1, u_2, ..., u_m \in \mathbb{R}^n$ tales que ${}^t u_i u_i = 1$. Sea $Q = (u_1|u_2|...|u_m)$. Demuestre que ${}^t QQ = I$, pero que $Q\,{}^t Q$ no necesariamente es igual a I. Más aún, $Q\,{}^t Q = I$ si y sólo si $n = m$.

*26. Sea $A^{(k)} = (a_{ij}^{(k)})$ la matriz en el paso k-ésimo del método de Gauss aplicado a $A = (a_{ij}) \in M_{nn}(\mathbb{R})$, A invertible. Sea $a_k = \max_{i,j} |a_{ij}^{(k)}|$ y $a = \max_{0 \le k \le n-1} a_k$.

(a) Pruebe que si $A = (a_{ij})$, con

$$a_{ij} = \begin{cases} 1 & \text{si } i = j \text{ ó } j = n \\ 0 & \text{si } j > i \text{ y } j \neq n \\ -1 & \text{si } j < i \end{cases}$$

entonces $a \le 2^{n-1} a_0$.

(b) Pruebe que si $A = (a_{ij})$ con $a_{ij} = 0, j < i$, entonces $a \le (n-1)a_0$

(c) Si A es tridiagonal, $A = \begin{pmatrix} \alpha_1 & \beta_2 & & & & & \\ \gamma_1 & \alpha_2 & \beta_2 & & & & \\ & \ddots & \ddots & \ddots & & & \\ & & \ddots & \ddots & \ddots & & \\ & & & \ddots & \ddots & \beta_n & \\ & & & & \gamma_n & \alpha_n & \end{pmatrix}$,

entonces $a \le 2a_0$.

Indicación: Use inducción sobre $k, 0 < k \le n-1$.

*27. Sea $A \in M_{p+n,m+n}(\mathbb{R})$, particionada de tal manera que $A = \begin{pmatrix} P & Q \\ R & S \end{pmatrix}$ con $R = I \in M_{nn}(\mathbb{R}), S = 0 \in M_{nm}(\mathbb{R})$. Determine el número efectivo

de sumas y multiplicaciones requeridas para calcular AB, donde $B \in M_{m+n,q}(\mathbb{R})$.

TEMAS CAPITULO VII

1. La melancolía.

2. Del maquiavelismo matricial a la Strassen.

1. La melancolía.

1.1. Matrices mágicas.

En el grabado de Alberto Durero "La melancolía" (1514), figuran, entre otros objetos, una calavera, varios libros, un filósofo y una matriz:

$$A = \begin{pmatrix} 16 & 3 & 2 & 13 \\ 5 & 10 & 11 & 8 \\ 9 & 6 & 7 & 12 \\ 4 & 15 & 14 & 1 \end{pmatrix}$$

Acaso, una clave para dilucidar "La melancolía" sea A. ¿Qué hay allí?, reflexione algunos minutos antes de seguir leyendo. ¿Ya? Bien, es fácil verificar que la suma por filas, columnas y diagonales de A es constante, $s(A) = 34$. Una matriz cuadrada con estas cualidades se denomina mágica. En lenguaje matricial, diremos que $A \in M_{nn}(\mathbb{R})$ es *mágica* si y sólo si existe $s(A) \in \mathbb{R}$ tal que: $\forall i, j \in \{1, ..., n\}$

$$\sum_{j=1}^{n} a_{ij} = \sum_{i=1}^{n} a_{ij} = s(A) \tag{7.46}$$

$$\sum_{k=1}^{n} a_{kk} = \sum_{k=1}^{n} a_{kn-k+1} = s(A). \tag{7.47}$$

En el caso, más relajado, en que A sólo verifique la propiedad (7.46), se dice que es *semi-mágica.*

Veamos algunas propiedades de estas matrices. Para ello notemos M_n el conjunto de matrices mágicas y SM_n el conjunto de las semi-mágicas. Es obvio que $M_n \subseteq SM_n \subseteq M_{nn}(\mathbb{R})$. ¿Qué sucede si sumamos dos matrices mágicas (semi-mágicas)?
Sean las matrices $A = (a_{ij})$, $B = (b_{ij})$ mágicas (semi-mágicas), luego $C = (c_{ij}) = (a_{ij} + b_{ij})$ verifica

$$\sum_{i=1}^{n} c_{ij} = \sum_{i=1}^{n} a_{ij} + \sum_{i=1}^{n} b_{ij} = s(A) + s(B)$$

$$\sum_{j=1}^{n} c_{ij} = \sum_{j=1}^{n} a_{ij} + \sum_{j=1}^{n} b_{ij} = s(A) + s(B)$$

$$\sum_{i=1}^{n} c_{ii} = \sum_{i=1}^{n} a_{ii} + \sum_{i=1}^{n} b_{ii} = s(A) + s(B)$$

$$\sum_{i=1}^{n} c_{in-i+1} = \sum_{i=1}^{n} a_{in-i+1} + \sum_{i=1}^{n} b_{in-i+1} = s(A) + s(B).$$

Luego, la suma de matrices mágicas (semi-mágicas) es mágica (semi-mágica).

¿Qué sucede al multiplicar dos matrices mágicas (semi-mágicas)?

Sea la matriz mágica:

$$A = \begin{pmatrix} 0 & 1 & -1 \\ -1 & 0 & 1 \\ 1 & -1 & 0 \end{pmatrix}.$$

La matriz producto,

$$A^2 = A \cdot A = \begin{pmatrix} -2 & 1 & 1 \\ 1 & -2 & 1 \\ 1 & 1 & -2 \end{pmatrix}$$

¡es sólo semi-mágica, no mágica! Entonces, no se cumple siempre que el producto de matrices mágicas sea mágico. Pero veamos el caso de las semi-mágicas: sean $A, B \in SM_n$ y sea $C = AB$. Supongamos que $s(A)$ y $s(B)$ son los valores de la suma de filas o columnas de A y B respectivamente y calculemos estos valores para C:

$$\sum_{j=1}^{n} c_{ij} = \sum_{j=1}^{n}\sum_{k=1}^{n} a_{ik}b_{kj}$$
$$= \sum_{k=1}^{n} a_{ik} \sum_{j=1}^{n} b_{kj} = \sum_{k=1}^{n} a_{ik}s(B) = s(A)s(B)$$

de manera análoga:

$$\sum_{i=1}^{n} c_{ij} = \sum_{i=1}^{n}\sum_{k=1}^{n} a_{ik}b_{kj} = \sum_{k=1}^{n} b_{kj}s(A) = s(A)s(B).$$

Luego, C es semi-mágica y $s(C) = s(A)s(B)$. Es decir, el conjunto SM_n con las operaciones suma y multiplicación de matrices, $(SM_n, +, \cdot)$, es cerrado.

Más aún, $(SM_n, +)$ es un grupo abeliano:

- La matriz O es obviamente mágica y es elemento neutro para $+$.
- La suma hereda, de $(M_{nn}(\mathbb{Z}), +)$, la asociatividad y la conmutatividad.
- Dada $A \in SM_n$, su inverso aditivo es $-A = (-a_{ij})$, que es semi-mágica, pues $s(-A) = -s(A)$.

También es directo que $(M_n, +)$ es un grupo abeliano (verifíquelo).

¿Qué sucede con la multiplicación en $(SM_n, \cdot)$? Sabemos que $\cdot$ es asociativa y no es conmutativa. El neutro es la matriz identidad, I, que es

claramente semi-mágica ($s(I) = 1$) pero no toda matriz mágica admite inversa, por ejemplo: la matriz semimágica (y mágica) $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ no es invertible (verifíquelo para todo $n \geq 2$).

De lo anterior concluimos que $(SM_n, +, \cdot)$ es un anillo con unidad ■

1.2. Matrices mágicas simétricas.

Sea MS_n el conjunto de matrices mágicas simétricas. Es fácil verificar que $(MS_n, +)$ es un subgrupo abeliano de $(M_n, +)$ (verifíquelo).

Estudiemos el caso particular $n = 3$. Vamos a probar el resultado siguiente: $\forall A \in MS_3$,

$$A = \lambda \begin{pmatrix} 1 & -1 & 0 \\ -1 & 0 & 1 \\ 0 & 1 & -1 \end{pmatrix} + \frac{s(A)}{3} \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}; \qquad \lambda \in \mathbb{R}.$$

donde $\beta C = (\beta c_{ij})$, $\beta \in \mathbb{R}$.

O, de manera equivalente:

toda matriz simétrica y mágica de 3×3 *puede factorizarse como la suma de dos matrices simétricas mágicas* $A = B + C$, *con* $s(B) = 0, s(C) = s(A)$.

La demostración es simple. No es difícil darse cuenta que $A = (a_{ij})$ se descompone como sigue:

$$A = \begin{pmatrix} a_{11} - \frac{s}{3} & a_{12} - \frac{s}{3} & a_{13} - \frac{s}{3} \\ a_{21} - \frac{s}{3} & a_{22} - \frac{s}{3} & a_{23} - \frac{s}{3} \\ a_{31} - \frac{s}{3} & a_{32} - \frac{s}{3} & a_{33} - \frac{s}{3} \end{pmatrix} + \begin{pmatrix} \frac{s}{3} & \frac{s}{3} & \frac{s}{3} \\ \frac{s}{3} & \frac{s}{3} & \frac{s}{3} \\ \frac{s}{3} & \frac{s}{3} & \frac{s}{3} \end{pmatrix} \tag{7.48}$$

donde $s = s(A)$.

Claramente, ambas matrices que figuran en la factorización son mágicas y simétricas. La primera de suma nula y la segunda con suma $s(A)$.

Veamos ahora cómo podemos escribir una matriz mágica y simétrica de 3×3, B, de suma nula ($s(B) = 0$). Como B es simétrica y mágica de suma nula, se tiene:

$$0 = b_{13} + b_{22} + b_{31} = 2b_{13} + b_{22},$$

de donde $b_{13} = -\frac{b_{22}}{2}$. Además,

$$b_{12} = -b_{11} - b_{13} = -b_{11} + \tfrac{b_{22}}{2}, \quad b_{33} = -b_{11} - b_{22}$$

$$b_{23} = -b_{13} - b_{33} = b_{11} + b_{22} - b_{13} = b_{11} + \tfrac{3}{2}b_{22}.$$

Por otra parte, $b_{32} = -b_{12} - b_{22} = b_{11} - \frac{b_{22}}{2} - b_{22} = b_{11} - \frac{3}{2}b_{22}$.

Como $b_{32} = b_{23}$, obtenemos $b_{22} = 0$. De lo anterior concluímos que B se escribe:

$$B = \begin{pmatrix} b_{11} & -b_{11} & 0 \\ -b_{11} & 0 & b_{11} \\ 0 & b_{11} & -b_{11} \end{pmatrix} = b_{11} \begin{pmatrix} 1 & -1 & 0 \\ -1 & 0 & 1 \\ 0 & 1 & -1 \end{pmatrix} \tag{7.49}$$

De las ecuaciones (7.48) y (7.49) se obtiene el resultado ■

Ejercicios.

1. Dada una matriz, A, mágica y simétrica de $n \times n$, con coeficientes enteros, discuta la afirmación siguiente: $s(A)$ y n tienen la misma paridad (ambos pares o ambos impares).
2. Estudie y caracterice el conjunto de matrices mágicas (semi-mágicas) simétricas (antisimétricas) de 2×2. (Observación: A es antisimétrica si y sólo si $a_{ij} = -a_{ji}\ \forall i, j$).
3. Sea MA_3 el conjunto de matrices mágicas antisimétricas de 3×3. Dada $A \in MA_3$ calcule $s(A)$. Demuestre que $\forall A \in MA_3$, $\exists \lambda \in \mathbb{R}$ tal que:

$$A = \lambda \begin{pmatrix} 0 & 1 & -1 \\ -1 & 0 & 1 \\ 1 & -1 & 0 \end{pmatrix}.$$

2. Del maquiavelismo matricial a la Strassen.

Al terminar el capítulo comentamos que para multiplicar dos matrices cuadradas en $M_{nn}(\mathcal{K})$, se requerían del orden de n^3 multiplicaciones. Este orden se obtiene directamente de la definición. En efecto, si $C = A \cdot B$, $A = (a_{ij}) \in M_{nn}(\mathcal{K})$ y $B = (b_{ij}) \in M_{nn}(\mathcal{K})$, entonces

$$c_{ij} = \sum_{k=1}^{n} a_{ik} \cdot b_{kj}$$

y es directo observar que para calcular cada uno de los n^2 coeficientes c_{ij} de C, requerimos n multiplicaciones. El total de productos suma entonces n^3.

Veremos a continuación que es posible reducir este número de multiplicaciones, a costa de la propia intuición, mediante un astuto algoritmo debido a Strassen, y que se basa en el enfoque "dividir para conquistar", que ya hemos usado en el capítulo II.

En primer lugar, observemos que el producto de dos matrices en $M_{nn}(\mathcal{K})$ puede realizarse por bloques. Esto quiere decir que si particionamos

$$A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \text{ y } B = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}$$

con submatrices A_{ij}, B_{ij} de dimensiones adecuadas, entonces:

$$C = A \cdot B = \begin{pmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{pmatrix},$$

donde

$$C_{ij} = A_{i1} \cdot B_{1j} + A_{i2} \cdot B_{2j} \quad i, j = 1, 2.$$

Por ejemplo, si $n = 5$, en $\mathbb{R}$:

$$A = \begin{pmatrix} 0 & 1 & 2 & 1 & 0 \\ 3 & 0 & -1 & 0 & 1 \\ 2 & 1 & 3 & 0 & 1 \\ 1 & 0 & -2 & 1 & 0 \\ 1 & 2 & 0 & -1 & 0 \end{pmatrix} \text{ y } B = \begin{pmatrix} 2 & 0 & -1 & 3 & 0 \\ -1 & 0 & 1 & 2 & 0 \\ 3 & -1 & 0 & 1 & 1 \\ 2 & 0 & 1 & 1 & 1 \\ -3 & 0 & -1 & 0 & 2 \end{pmatrix}$$

$$\Rightarrow \quad C = \begin{pmatrix} 7 & -2 & 2 & 5 & 3 \\ 0 & 1 & -4 & 8 & 1 \\ 9 & -3 & -2 & 11 & 5 \\ -2 & 2 & 0 & 2 & -1 \\ -2 & 0 & 0 & 6 & -1 \end{pmatrix}.$$

Pero, además:

$$A_{11} = \begin{pmatrix} 0 & 1 \\ 3 & 0 \\ 2 & 1 \end{pmatrix} \in M_{32}(\mathbb{R}), \quad A_{12} = \begin{pmatrix} 2 & 1 & 0 \\ -1 & 0 & 1 \\ 3 & 0 & 1 \end{pmatrix} \in M_{33}(\mathbb{R}),$$

$$A_{21} = \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix} \in M_{22}(\mathbb{R}), \quad A_{22} = \begin{pmatrix} -2 & 1 & 0 \\ 0 & -1 & 0 \end{pmatrix} \in M_{23}(\mathbb{R}),$$

$$B_{11} = \begin{pmatrix} 2 & 0 & -1 \\ -1 & 0 & 1 \end{pmatrix} \in M_{23}(\mathbb{R}), \quad B_{12} = \begin{pmatrix} 3 & 0 \\ 2 & 0 \end{pmatrix} \in M_{22}(\mathbb{R}),$$

$$B_{21} = \begin{pmatrix} 3 & -1 & 0 \\ 2 & 0 & 1 \\ -3 & 0 & -1 \end{pmatrix} \in M_{33}(\mathbb{R}), \quad B_{22} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 0 & 2 \end{pmatrix} \in M_{32}(\mathbb{R}).$$

Así,

$$C_{11} = A_{11} \cdot B_{11} + A_{12} \cdot B_{21} = \begin{pmatrix} -1 & 0 & 1 \\ 6 & 0 & -3 \\ 3 & 0 & -1 \end{pmatrix} + \begin{pmatrix} 8 & -2 & 1 \\ -6 & 1 & -1 \\ 6 & -3 & -1 \end{pmatrix}$$

$$= \begin{pmatrix} 7 & -2 & 2 \\ 0 & 1 & -4 \\ 6 & -3 & -2 \end{pmatrix}$$

$$C_{12} = A_{11} \cdot B_{12} + A_{12} \cdot B_{22} = \begin{pmatrix} 2 & 0 \\ 9 & 0 \\ 8 & 0 \end{pmatrix} + \begin{pmatrix} 3 & 3 \\ -1 & 1 \\ 3 & 5 \end{pmatrix} = \begin{pmatrix} 5 & 3 \\ 8 & 1 \\ 11 & 5 \end{pmatrix}$$

$$C_{21} = A_{21} \cdot B_{11} + A_{22} \cdot B_{21} = \begin{pmatrix} 2 & 0 & -1 \\ 0 & 0 & 1 \end{pmatrix} + \begin{pmatrix} -4 & 2 & 1 \\ -2 & 0 & -1 \end{pmatrix} = \begin{pmatrix} -2 & 2 & 0 \\ -2 & 0 & 0 \end{pmatrix}$$

$$C_{22} = A_{21} \cdot B_{12} + A_{22} \cdot B_{22} = \begin{pmatrix} 3 & 0 \\ 7 & 0 \end{pmatrix} + \begin{pmatrix} -1 & -1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} -2 & -1 \\ 6 & -1 \end{pmatrix}.$$

Naturalmente, un par de matrices que se multiplican puede ser particionado en una cantidad variable de submatrices (no necesariamente cuatro), cuidando para ello que las dimensiones de las submatrices sean consistentes, con el fin de que el producto pueda realizarse. Establezca, como ejercicio, el conjunto de fórmulas (y dimensiones) para el producto de dos matrices de $M_{nn}(\mathcal{K})$ $(n > 6)$, particionadas cada una en seis submatrices.

¿Hemos obtenido alguna ganancia, en términos de reducir el número de multiplicaciones, al considerar el producto de dos matrices por bloques? No nos apresuremos. La verdad es que no hay ganancia todavía, pues no hemos señalado cómo realizar astutamente el producto de dos submatrices (¡ahí está la clave!).

Consideremos el caso en que $n = 2^k, k = 1, 2, \ldots$ Es obvio que en el caso $n = 1$ no hay mucho que hacer. La idea aquí es construir un procedimiento recursivo de multiplicación sobre el valor de k.

El producto de dos matrices de $M_{22}(\mathcal{K})$, según Strassen, se puede realizar de modo de reducir el número de multiplicaciones de 8 a 7. En efecto, dadas $A = (a_{ij})$ y $B = (b_{ij}) \in M_{22}(\mathcal{K})$, el cálculo de $C = A \cdot B$, se hace de la manera siguiente:

Algoritmo de Strassen: $(n = 2)$

- Calcule

$$\begin{aligned} x_1 &= (a_{11} + a_{22}) \cdot (b_{11} + b_{22}) \\ x_2 &= (a_{21} + a_{22}) \cdot b_{11} \\ x_3 &= a_{11} \cdot (b_{12} - b_{22}) \\ x_4 &= a_{22} \cdot (b_{21} - b_{11}) \\ x_5 &= (a_{11} + a_{12}) \cdot b_{22} \\ x_6 &= (a_{21} - a_{11}) \cdot (b_{11} + b_{12}) \\ x_7 &= (a_{12} - a_{22}) \cdot (b_{21} + b_{22}). \end{aligned} \tag{7.50}$$

- Defina $C = (c_{ij})$, como sigue:

$$\begin{aligned} c_{11} &= x_1 + x_4 - x_5 + x_7 \\ c_{12} &= x_3 + x_5 \\ c_{21} &= x_2 + x_4 \\ c_{22} &= x_1 + x_3 - x_2 + x_6. \end{aligned}$$

No le será difícil constatar, que efectivamente $C = A \cdot B$. Lo más importante, sin embargo, es que el número de multiplicaciones en (7.50) es ...7.

En apariencia el resultado es sumamente ocioso, pero, como decía Aristóteles, "el ocio engendra la maravilla" y esta maravilla aparece cuando utilizamos el viejo y querido principio recursivo. Supongamos, entonces, que disponemos del algoritmo de Strassen para el caso de $n = 2^{k-1}$ (hipótesis inductiva). Deseamos efectuar el producto $A \cdot B$, en $M_{nn}(\mathcal{K})$ con $n = 2^k$. Consideremos para ello, la partición de A y B en bloques de tamaño $\frac{n}{2} \times \frac{n}{2}$, es decir

$$A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}, \; B = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}$$

con $A_{ij}, B_{ij} \in M_{\frac{n}{2},\frac{n}{2}}(\mathcal{K}), i, j = 1, 2$.

Es directo probar (¡hágalo!) que el resultado del producto $A \cdot B$, por bloques, es:

$$C = \begin{pmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{pmatrix}$$

donde las submatrices $C_{ij} \in M_{\frac{n}{2},\frac{n}{2}}(\mathcal{K})$ se pueden calcular por un procedimiento similar a (7.50). Este procedimiento es el siguiente:

- Calcule

$$\begin{aligned} X_1 &= (A_{11} + A_{22}) \cdot (B_{11} + B_{22}) \\ X_2 &= (A_{21} + A_{22}) \cdot B_{11} \\ X_3 &= A_{11} \cdot (B_{12} - B_{22}) \\ X_4 &= A_{22} \cdot (B_{21} - B_{11}) \\ X_5 &= (A_{11} + A_{12}) \cdot B_{22} \\ X_6 &= (A_{21} - A_{11}) \cdot (B_{11} + B_{12}) \\ X_7 &= (A_{12} - A_{22}) \cdot (B_{21} + B_{22}). \end{aligned} \tag{7.51}$$

- Defina

$$\begin{aligned} C_{11} &= X_1 + X_4 - X_5 + X_7 \\ C_{12} &= X_3 + X_5 \\ C_{21} &= X_2 + X_4 \\ C_{22} &= X_1 + X_3 - X_2 + X_6. \end{aligned}$$

Aquí, $X_j \in M_{\frac{n}{2},\frac{n}{2}}(\mathcal{K})$ y $C_{ij} \in M_{\frac{n}{2},\frac{n}{2}}(\mathcal{K})$ $i, j = 1, 2$.

Observemos que $X_1, ..., X_7$ son productos de submatrices de $M_{\frac{n}{2},\frac{n}{2}}(\mathcal{K})$, que podemos realizar, según la hipótesis inductiva, mediante el algoritmo de Strassen ... el fecundo en ardides.

Bien, lo que hemos hecho es demostrar, inductivamente, la existencia de un procedimiento particular para obtener el producto de dos matrices de $M_{nn}(\mathcal{K})$, para $n = 2^k, k = 1, 2, ...$

¿Dónde está la reducción en el número de multiplicaciones? Supongamos que $m(n)$, $n = 2^k$, es el número de multiplicaciones que requiere el procedimiento. Es de observar que este número será 7 veces el número requerido para el producto de dos submatrices de $M_{\frac{n}{2},\frac{n}{2}}(\mathcal{K})$. Luego, se obtiene la ecuación de recurrencia

$$m(2^k) = 7 \cdot m(2^{k-1})$$

a la que se agrega la condición inicial, dada por (7.50) para $k = 1$: $m(2) = 7$.

Es muy fácil notar que la solución de la ecuación de recurrencia es $m(2^k) = 7^k$

$$\begin{aligned} &\iff m(n) = 7^k \\ &\iff log_2 m(n) = k \cdot log_2 7 \\ &\iff m(n) = 2^{k log_2 7} \\ &\iff m(n) = n^{log_2 7}, \text{ con } n = 2^k. \end{aligned}$$

Así, de un número de multiplicaciones del orden de n^3 pasamos a uno de orden $n^{log_2 7}$, lo cual significa, si recordamos que $log_2 7 = 2,80735...$, que por ejemplo, para $n = 100$, nos ahorramos más de la mitad de las multiplicaciones si usamos el algoritmo de Strassen en vez del usual. Compruébelo.

Quedan, entre otros, dos casos importantes que discutir. Vayan éstos como ejercicios.

Ejercicios.

1. Comparación del número de sumas en el algoritmo de Strassen y en el algoritmo clásico del producto de dos matrices.
   (a) Sea $s(n)$ el número de sumas (o restas) requeridos en el producto $A \cdot B$, $A, B \in M_{nn}(\mathcal{K}), n = 2^k, k = 1, 2, ...$ Muestre que $s(n)$ obedece a la ecuación de recurrencia:

$$\begin{aligned} s(2^k) &= 7s(2^{k-1}) + 18(2^{k-1})^2 \\ s(2) &= 18. \end{aligned}$$

(b) Verifique que la solución a la ecuación anterior es $s(2^k) = 6\cdot(7^k - 4^k)$ y que entonces

$$s(2^k) < 6 \cdot 7^k < n^3 - n^2, \quad (n = 2^k)$$

para n es suficientemente grande.

(c) Concluya que, salvo para valores pequeños de n, el algoritmo de Strassen requiere menos sumas que el algoritmo clásico para el producto de matrices y que, por ende, tal algoritmo no reduce el número de multiplicaciones a costa del aumento de las sumas (cuando n es grande).

2. Extienda el uso del algoritmo de Strassen para el producto $A \cdot B$, $A, B \in M_{nn}(\mathcal{K})$, para n cualquiera.
(Indicación: considere k tal que $2^{k-1} < n \leq 2^k$ y matrices $\tilde{A}, \tilde{B}$, definidas a partir de A y B, agregando $2^k - n$ columnas y filas nulas).

SOLUCIONARIO

Capítulo I.

4. (a) $(p \wedge q) \vee (\bar{p} \wedge \bar{q})$.
(b) Cualquier tautología que use $-, \vee$ ó $\wedge$.
7. (b) $p \wedge q \wedge \bar{r}$.
(c) tal es la expresión más simple.
9. Red $\Longleftrightarrow (\bar{p} \wedge q) \vee [(\overline{p \wedge q}) \wedge \bar{r}]$.
Luz $\Longleftrightarrow [p \wedge (\bar{r} \vee q)] \vee [\bar{p} \wedge (\bar{q} \wedge \bar{r})]$.
13. (c) y (d). Razone por contradicción.
20. ¿Qué le parece $C[\mathcal{P}(A)] = \mathcal{P}(U) \setminus \mathcal{P}(A)$?
22. (b) Falso.
(c) Verdadera.
25. Consta de dos proposiciones: la negación de $(\exists x \in U)$ en conjunción con la negación de la unicidad.
26. $\bigcup\limits_{i \in \mathbb{N}_+} A_i = \mathbb{R}$, $\bigcap\limits_{i \in \mathbb{N}_+} A_i = [-2, 3]$.

Capítulo II.

2. Pruebe primero, por inducción, que $2n < 2^n$, $n > 5$. Use esto para probar, por inducción, que $2n + 1 < 2^n$, $n > 5$. Por último, lo anterior le sirve para probar, por inducción, el ejercicio.
3. (a) Es obvio si n es par. Al aplicar la inducción note que si n es par, entonces $n + 1$ es impar y viceversa.
(b) Si $n \geq 14$, la hipótesis inductiva indica que $n = 3p+8q$, $p, q \in \mathbb{N}$. De aquí: $n+1 = 3(p+3)+8(q-1)$. (Si $q > 0$), o bien, $n+1 = 3(p-5)+8\cdot 2$ (si $q = 0$ y notamos que $p > 5$, para $n \geq 14$).
5. (a) La idea es probar que si $|x| = n$, al agregar un elemento (distinto) a x y ahora $|x| = n + 1$, entonces $|\mathcal{P}(x)|$ aumenta en 2^n conjuntos.
(b) Lo importante es probar para $n = 2$. En el paso de n a $n + 1$ use ese resultado.
7. (a) y (b) pueden probarse simultáneamente por inducción. Note que (a) se refiere a n impar y (b) a n par.
(c) y (d) también pueden probarse simultáneamente, con la misma observación anterior.
9. (a) La suma vale $\alpha \cdot n$ con $\alpha = 2$, $\forall n \in \mathbb{N}$.
(b) Despeje a_{n+1} de la fórmula de recurrencia y use la hipótesis.
(c), (d) y (e). De la definición de suma: $\sum\limits_{k=1}^{n+1} a_k = \sum\limits_{k=1}^{n} a_k + a_n$. Use

la hipótesis inductiva para la suma del lado derecho y luego sume el término a_n.

10. (a) y (d) se siguen de la definición recurrente de producto.
(b) Aquí, para aplicar la hipótesis inductiva $P(n) \Rightarrow P(n+1)$, realice el cambio de variable $j = k+1$ y aplique la hipótesis inductiva.
(c) Además de la defnición de producto, debe usar la definición de suma; ¡no confunda los índices!

12. Debe probar que $q_n \neq 0\ \forall n$. La igualdad $n_n = \frac{q_n}{q_{n-1}}$ es directa.

13. Observe que se pide demostrar que $\sum_{i=1}^{2^{k+1}} i^p I_x(i) = \sum_{i=1}^{2^{k+1}} i^p I_y(i)$
$p = 1, ..., k$, donde
$I_x(i) = \begin{cases} 1 & \text{si } i \text{ es índice de } x \text{ en la fila } k \\ 0 & \text{si no} \end{cases}$
$I_y(i) = \begin{cases} 1 & \text{si } i \text{ es índice de } y \text{ en la fila } k \\ 0 & \text{si no} \end{cases}$
y que la indicación se traduce en $I_x(i+2^k) = I_y(i), I_y(i+2^k) = I_x(i)$.

15. (a) El número es 76.544.
(b) Los números son 8, 12 y 18.

17. Encuentre una expresión para s y s' en términos de a_0 y la diferencia d.

20. Basta probar que, si $a_k > 0\ \forall k$, entonces la secuencia $(a_k)_{k\in N}$ es decreciente, es decir $a_{k-1} > a_k\ \forall k > 1$. Además, del hecho que $a_k^2 d^2 < 1$ (donde d es la diferencia de la progresión aritmética asociada a a_k, $(k \in \mathbb{N})$ se tiene, por inducción sobre n, la proposición.

21. (a) Dado n, use inducción sobre m.
(b) Considere el desarrollo del binomio de Newton de $(x+b)^n$ con $a = -b = 1$.
(c) De la definición recursiva de C_n^k, se tiene
$C_{2n}^n + C_{2n}^{n-1} = C_{2n+1}^n$
como $C_{2n+1}^n = C_{2n+1}^{2n+1-n} = C_{2n+1}^{n+1}$
entonces $C_{2n+1}^n = \frac{1}{2} C_{2n+2}^{n+1}$. q.e.d.
(d) Use inducción sobre n y recuerde que
$(C_{n+1}^k)^2 = (C_n^{k-1} + C_n^k)^2 = (C_n^{k-1})^2 + 2C_n^k C_n^{k-1} + (C_n^k)^2$.
(e) Muestre que $\sum_{k=0}^{n} \frac{(-1)^k C_n^k}{(k+2)(k+3)} = \frac{1}{(n+1)(n+2)(n+3)} \cdot \sum_{k=0}^{n} (-1)^k (k+1) C_{n+3}^{k+3}$
realice el cambio $j = k+3$ en la suma del lado derecho y calcúlela.

23. (a) La idea es escribir los desarrollos de los binomios $\{(1+x^2)^2 - 1\}^{2n}$ y $x^{2n}(2+x)^{2n}$, igualar los coeficientes que acompañan una potencia particular de x.
(b) Es directa de la propiedad y del desarrollo del binomio $(1+x)^{n+1}$, por medio de un cambio de índice.

27. $n = 2$ y $n = 3$.

Tema 4.2- II.

2. $\frac{n(n-1)}{2}$.
3. Nota que $m, n \geq 2$. Si $C_{n,n}$ es el número de cortes $C_{n,m} = m + n - 2$.
5. Resuelva análogamente al último corte de pizza del tema.

Tema 4.3- II.

1. Trivial, aplique la propiedad telescópica a la suma.
3. Idem 1.
4. Por inducción es sencillo.
5. Fije m y use inducción sobre n. Luego fije n y haga lo mismo.
6. Trivial, por inducción.
7. Ni tan difícil, use inducción.

Capítulo III.

2. (b) Esto es efectivo. Use 1. y 2(a).
4. R={$(0,5),(0,8),(1,7),(2.6),(3,3),(3,5),(4,4),(5,3),(6,2),(7,1),(8,0)$}.
6. Refleja, simétrica, pero no transitiva:
Ejemplo:$M_R = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$
11. (a) $2^{(n^2)}$, (b) $2^{n(n-1)}$, (c) $2^{\frac{n(n+1)}{2}}$, (d) $2^{\frac{n-(n+1)}{2}} + n(n-1)$.
14. (a) Falso.
(b) Falso.
17. (a) Indicación: use la definición y propiedades de conjuntos.
(b) ($\Leftarrow$) trivial.
($\Rightarrow$) Use (a).
21. Si $n = a \cdot b$ entonces $a \leq \sqrt{n}$ o $b \leq \sqrt{n}$ (lo contrario es contradictorio). Si $a \leq \sqrt{n}$, basta considerar p primo cualquiera de la descomposición en factores primos de a.
22. $mcd(1154, 322) = 14$, $mcd(236, 28) = 4$.
25. (a) Razone recursivamente: si $q = q_n$, anote $q_n = p_1^{\alpha_1} \cdot q_{n-1}$ y encuentre una fórmula recursiva para el número de divisiones en esta factorización.
(b) Similar a parte (a).

Tema 3-III.

1. (a) $x = 7$ es solución particular, luego, el conjunto solución es $\{7, 10, 13, 16, 19, 22\}$.
(b) No tiene solución.
(c) $n = 1 \Rightarrow \{0, 1, 2, 3, 4\}$
$n = 2 \Rightarrow \{3, 4, 5, 6, 7\}$

$n = 3 \Rightarrow \{16, 17, 18, 19, 20\}$
$n = 4 \Rightarrow \{51, 52, 53, 54, 55\}$.

Tema 4-III.

2. $q \leq n$.
3. (a) iRj tiene que ver con un "camino" de i a j.
6. El problema corresponde a encontrar $k' \geq 1$, $k' \in \mathbb{N}$ tal que $M^{k'} = I$, $(I = (\delta_{ij}) \in M_{nn}(\{0,1\})$. Conviene usar los resultados del tema, asociando a M un grafo $G = (U, V)$, con $U = \{1, 2, ..., n\}$.

Capítulo IV.

1. (a) No es función.
   (b) Es función.
   (c) No es función.
   (d) Es función.
   (e) No es función (ver ejercicio 2).

4. (b) $A/\mathcal{R} = \{\{1\}, \{3\}\} \cup \{\{2k, 2k+3\}/k = 1, 2, ...; 2k+3 \leq n\} \cup \{\{n-1\}/n$ es impar$\} \cup \{\{n\}, \{n-2\}/n$ par $\}$.
7. $f(f(X)) = A \cap (B \cup (A \cap (B \cup X))$
   $= A \cap ((B \cap A) \cup (B \cup X)) = (A \cap B) \cup (A \cap (B \cup X))$.
   Como $A \cap B \subset A \cap (B \cup X)$, entonces $f(f(X)) = A \cap (B \cup X) = f(X)$.
10. (a) f no es inyectiva $(f(1) = f(2))$; f es epiyectiva luego, no es biyectiva.
    (b) $f^2(x) = \lceil \frac{x}{4} \rceil$, donde $\lceil a \rceil$ denota el entero superior más próximo al real a.
12. Por ejemplo: $A = \{1, 2, 3\}$, $A' = \{2, 3\}$, $B = A$ y f como en el ejercicio 10.
17. (a) Pruebe que $f(i) = (f(0) + i) \bmod (n)$. Para ello le conviene probar, además, que en general $\forall a, b \in \mathbb{N}$ $(a \bmod (n) + b \bmod (n)) \bmod (n) = (a + b) \bmod (n)$.
    (b) Existen n funciones cíclicas para $A = \{0, 1, ..., n-1\}$.
18. Divida el triángulo equilátero en cuatro triángulos equiláteros de lado un medio.
23. Si I_n es el número de inversiones en S_n: $I_n = \frac{n(n-1) \cdot n!}{4}$. (Encuentre una fórmula recursiva para I_n).
26. Use el resultado del ejercicio 17.
28. Suponga que X es finito. Tome una biyección f y obtenga una contradicción.

Tema 1-IV.

2. (a) Considere $f : \times_{i=1}^{n} A^i \to \mathbb{N}^n$; $(x_1, ..., x_n) \to (f_1(x_1), ..., f_n(x_n))$, donde $f_j : A_j \to \mathbb{N}$ es biyección.
   (b) Use el hecho que la unión enumerable de conjuntos enumerables es enumerable.
6. Considere $H_k = \{0, 1, 2, ..., k\}$. Pruebe que $F \subseteq \bigcup_{k \in \mathbb{N}} H_k$ y use el resultado del ejercicio 5.

Capítulo V.

2. (a) $\mathbb{Z}_2$ y $\mathbb{Z}_3$ son cuerpo. Se hereda entonces: asociatividad, conmutatividad, existencia de neutro $(0, 1)$, inverso.
   (b) El producto x en $\mathbb{R}^3$ resulta asociativo, no posee neutro (luego no hay inverso), ni es conmutativo. (Verifique que $(x_1, x_2, x_3) \times (y_1, y_2, y_3) = -(y_1, y_2, y_3) \times (x_1, x_2, x_3)$).
3. (a) Considere $x = e$, $y = f$, $n = f$, $v = e$.
   (b) Considere $y = n = e$ y use el resultado de (a).
   (c) Considere $n = e$, y use (a), (b) para la asociatividad y considere $x = e$, $v = e$ y use (a), (b) para la conmutatividad.
5. Sólo álgebra de números reales. Recuerde que $(\mathbb{R}, +, \cdot)$ es cuerpo.
7. Para $(P(X), A)$ la clave está en que $(A \cap S) \setminus B = (A \cap S) \setminus (B \cap S)$.
   Para $(P(X), \cap)$ el resultado es trivial.
9. (a) No es homomorfismo.
   (b) No es, en general, homomorfismo. Si G es abeliano $\varphi = id$ (que es isomorfismo).
10. (a) Conmutatividad. Ver (c) del ejercicio 3, para el caso $x = n$, $y = v$.
    (b) Inductivamente $n = c$ se tiene: $(a \cdot b)^{n+1} = (a \cdot b)^n \cdot (a \cdot b) = (a^n \cdot b^n) \cdot (a \cdot b) = a^{n+1} \cdot b^{n+1}$, de asociatividad y conmutatividad de $(G, \cdot)$.
12. Suponga lo contrario, y obtenga una contradicción.
13. Si $f, g \in G$, $f * g = h/ * g$
    $\Longrightarrow \quad f = h * g/ * f$
    $\Longrightarrow \quad e = h * (g * f)/h*$
    $\Longrightarrow \quad h = g * f$.
    $f * g = g * h$.
15. Como $\phi = G' \subseteq G$, basta probar que $\forall f, g \in G^1$ se tiene $f \cdot g^{-1} \in G^1$, lo cual es simple.
18. (a) $y \in H \Rightarrow g = g * e \in g * H$ (e neutro).
    Además, $f \in g * H \Rightarrow f = g * h (h \in H)$

(pues $g \in H \wedge H$ es cerrado) $g * H = H$.
(b) La misma idea de (a).

20. Sea φ el isomorfismo.
G cíclico $\Leftrightarrow \exists a \in G, \forall x \in G, \exists n \in \mathbb{Z}$ tal que $x = a * a * \cdots * a$ (n veces)
$\Rightarrow \varphi(x) = \varphi(a) * \varphi(a) * \cdots \varphi(a)$ (n veces).
Como φ es biyectiva, si x es cualquiera en G, $\varphi(x)$ es cualquiera en ϵ, luego ϵ es cíclico (y viceversa).

22. Los divisores de cero en $(\mathbb{Z}_\infty, \oplus, \cdot)$ son [2] y [4]. Puede escribir las tablas de Pitágoras y encontrar el isomorfismo pedido explícitamente. Resulta que $(\mathbb{Z}_\infty, \oplus, \cdot)$ no es isomorfo a $(\mathbb{Z}_2 \times \mathbb{Z}_*, +, \cdot)$, (compare las tablas de Pitágoras correspondientes).

24. Las tablas son

$+$	e	h	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

$\cdot$	a	b	c	d
a	a	a	a	a
b	a	a	a	a
c	a	a	c	d
d	a	b	c	d

de donde $(A, +\cdot)$ no es conmutativo y $(A, +, \cdot)$ no posee unidad.

26. (a) Sea $x \neq 0$ (neutro de $(A, +)$), $x + x = y \in A$
$\Rightarrow (x + x) \cdot y = y \cdot y = y$
$\Rightarrow x + x = 1$ (neutro de $A, +, \cdot$), por la unicidad del neutro. Luego, $x = -x$.
(b) $(x + y) \cdot (x + y) = x + y$. Por distributividad
$x^2 + xy + yx + y^2 = x + y \Leftrightarrow x + xy + yx + y = x + y$.
Como $(A, +)$ es abeliano
$\Leftrightarrow xy + yx = 0 \Leftrightarrow xy = -(yx)$.
De (a): $xy = yx$.
(c) $(x \cdot y) \cdot (x + y) = x \cdot y \cdot x + x \cdot y \cdot y$. Conmutando: $(x \cdot y)(x + y) = yx + xy = 0$ (de (b)).

30. (a) Si $z = 1 - x$ es nilpotente, sea n el natural más pequeño tal que $z^n = 0$. Entonces $1 + z + z^2 + ... + z^{n-1}$ es inverso de x.
(b) ($\Leftarrow$) Si $n = k^2 d$, entonces $[kd]$ es nilpotente.
($\Rightarrow$) Sea $[x]$ nilpotente, $0 < x < n$, y r el natural más pequeño tal que $[x]^r = [0]$. Entonces $x^r = \beta n$, $1 \leq \beta < n$ de donde $x^2 \cdot x^{r-2} = \beta n$ $(r - 2 \geq 0)$.
Como x^2 no divide a β (r es el exponente más pequeño, etc) entonces x^2 divide a n.

31. Al probar que $(A, \cdot)$ es grupo abeliano, lo que falta es la existencia de inverso. Razone por contradicción, asumiendo que $A = \{a_1, ..., a_n\}$.

33. La conmutatividad en $(K, \cdot)$ se tiene al distribuir por la derecha y por la izquierda la expresión de la indicación, $\forall x, y \in K$. Luego, la exigencia de conmutatividad a priori no es necesaria.

34. (a) $x = [1]$.
(b) $x = [1]$, $y = [0]$.

Tema 3-V.

2.

$\cdot$	a	b	ab
a	a	ab	ab
b	ab	b	ab
ab	ab	ab	ab

en $(\{a, b\}^* / \sim, \cdot)$

3. (a) Directo.
(b) $v \in V$, $a \in AA$, $ab \in AB$, $ba \in BA$, $b \in BB$.

Tema 4-V.

1. Solución directa, según el esquema usado en la aplicación expuesta en el tema.
2. $f_{A \setminus B} = f_A \cdot f_{\bar{B}} = f_A \cdot (1 \oplus f_B)$.
3. Idem 1.
4. $A \leq B \Leftrightarrow A = A \cap B \Leftrightarrow f_A = f_{A \cap B} = f_A \cdot f_B$.

Capítulo VI.

1. Considere los cambios $w = z - 8i \wedge zu = z, -8$ y luego despeje.
2. Si $\theta = Arg(z) :=\frac{-1 \pm sec\theta}{ig\theta}$.
4. (i) Está claro que $\bar{z}_0 z + z_0 \bar{z} = 2Re(\bar{z}_0 z) \in \mathbb{R}$.
Escriba $x_0 = (x_0, y_0 \wedge z = (x, y)$ y desarrolle.
(ii) Si $z_n = x_n + iy_n$, considere $Im(z_n \overline{z_{n-1}})$.
5. $x = 2i, -i$.
6. Trivial $x = e^{i\frac{(4k+1)\pi}{12}}$.
7. (a) Use la fórmula de Moire.
(b) Idem (a), más propiedad.
(c) Directo. Si j varía con h, $w_k^{j-h} = 1$.
(d) Use que $\sum_{k=0}^{n-i} q^k = \frac{1-q^n}{1-q}$.
9. Desarrolle (aunque se aburra) el lado derecho y recuerde que $w^2 = \bar{w}$.
11. $|z| = 1$ y $|z + 1| = 1 \Rightarrow z = \frac{-1}{2} \pm \frac{\sqrt{3}}{2}i$ Si $z = \frac{-1}{2} + \frac{\sqrt{3}}{2}i = e^{i\frac{2\pi}{3}}$
$\Rightarrow z + 1 = e^{\frac{i\pi}{3}}$
De aquí: $(z + 1)^n = 1 \Rightarrow \frac{\pi}{3}n = 2k\pi \Rightarrow n = 6k$.
12. (a) $f(x) = (x + 2)(x^2 + 2) - (2x + 5)$
(b) $f(x) = (x^4 + 2x^2 + 1)(x^2 - 3x + 2) - 6x^3 + 5x^2 + 2x + 1$.
14. Trivial. Considere el discriminante $\Delta = b^2 - 4ac$, si $p(x) = ax^2 + bx + c$.

16. $z_0 = \frac{1}{2} + \frac{1}{4}i \Rightarrow p(z) = (z - z_0)(z - \bar{z}_0) = z^2 - z + \frac{5}{16}$.
17. (a) Se obtiene que $p(\alpha i) = p(-\alpha i) = 0$.
    (b) $a_0 = 16 \Rightarrow p(x) = (x-2)^4$.
18. $p(x) = (x+1)(x-4)(x^4+16)$.
20. $\frac{x^n - a^n}{x+a} = \sum_{i=1}^{n} (-1)^{i-1} a^{i-1} x^{n-i} + \frac{(-1)^n a - a^n}{x+a}$.
21. En $(\mathbb{Z}_4, \oplus, \cdot)$ considere $f = y = 2x \oplus 1$, por ejemplo.
22. Para encontrar $x \in \mathbb{R}$ tal que $p(x) = y$, estudie las raíces del polinomio $q(x) = p(x) - y$.
23. Si z_0, z_1, z_2 son vértices del triángulo ABC,
    $p(z) = (z - z + 0)(z - z_1)(z - z_2)$.
    (a) El centro de gravedad es $\frac{z_0+z_1+z_2}{3}$.
    (b) En este caso $|z_0 - z_0| = |z_2 - z_1| = |z_2 - z_0|$.
26. Use inducción sobre la fórmula recurrente.
27. (a) Pruebe que $x_0, x_1, ..., x_j$ son raíces de $\delta_{x_0,...,x_j}(p)$, que tiene grado n. Concluye que es el polinomio nulo.

Capítulo VII.

2. Si $x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$, $y = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}$, entonces

$$Ax = \begin{pmatrix} x_1 - x_2 - x_n \\ x_2 - x_3 \\ \vdots \\ x_{n-1} - x_n \\ x_n - x_1 \end{pmatrix},$$

$$^t yA = (y_n - y_1, y_2 - y_1, ..., y_{n-1} - y_{n-2}, y_n - y_{n-1} - y_1).$$

Si $A = (b_{ij})$
$A \cdot B = (c_{ij})$ con $c_{ij} = b_{ij} + b_{i+1,j} \quad \forall i, j, i \neq 1, n.$
$c_{1j} = b_{1j} - b_{2j} - b_{nj}$, $c_{nj} = b_{nj} - b_{n1}, \quad \forall j.$

3. (a) $A^n = 5^{n-1} \cdot A$, $n \geq 1$, $B^n = \begin{pmatrix} (2^{n-1}-1) & -(2^{n-1}-1)i & 1 \\ (2^n-1)i & (2^n-1) & i \\ (2^n-1) & -(2^n-1)i & 1 \end{pmatrix}$ para $n \geq 2$ (justificar por inducción).
4. (a) Trivial.
   (b) Escriba $M_{pq} \cdot B$, con $B = (b_{ij})$ cualquiera.

(c) El isomorfismo se basa en la manera de organizar filas y columnas de una matriz de $(M_{nn}(R), +)$. No es único. Por ejemplo:
$A = (a_{ij})$ con

$$\begin{array}{l} a_{11} \to a_{12} \to \cdots\cdots \to a_{1n} \\ \qquad\qquad\qquad\qquad\quad \downarrow \\ a_{2n} \leftarrow a_{2n-1} \leftarrow \cdots \leftarrow a_{21} \\ \downarrow \\ a_{31} \to \text{ etcétera.} \end{array}$$

Se asocia a $Y = (a_{11}, a_{12}, ..., a_{1n}, a_{21}, ..., a_{2n}, \cdots)$.

6. Multiplique: $(I - X\,{}^tY)(I + \frac{X\,{}^tY}{1 - {}^tXY})$ y recuerde que ${}^tXY = {}^tYX$ en $\mathbb{R}$.
7. (a) Use inducción sobre p.
   (b) Note que $\begin{pmatrix} u_n \\ v_n \\ w_n \end{pmatrix} = A \begin{pmatrix} u_{n-1} \\ v_{n-1} \\ w_{n-1} \end{pmatrix}$
9. (a) Use que $(MTS, +)$ es subgrupo si $\forall U, R \in MTS$, entonces $U + (-R) \in MTS$.
   (b) No existe inverso en $(MTS, \cdot)$, ni se tiene conmutatividad. Las demás propiedades se heredan de $M_{nn}(\mathbb{R})$.
11. (a) Considere $\varphi : \mathbb{C} \to M$, $a + ib \to \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$
    (b) Construya la tabla de Pitágoras y responda.
13. (a) Justifique por medio del algoritmo de Gauss.
    (b) Basta con probar $U^n = 0$. Use inducción sobre n. Se consideran $U \in T(0)$ (caso $(n+1) \times (n+1)$); observe que
    $U = \begin{bmatrix} V & n \\ {}^tc & 0 \end{bmatrix}$ $n \in \mathbb{R}^{n-1}, c =$ cero de $\mathbb{R}^{n-1}$, $V \in T(0)$ (de $n \times n$) y calcule U^{n+1}.
15. (a) Si $b^* = -1$, el sistema tiene solución.
    (b) $x = \begin{pmatrix} 3/2 \\ -1/2 \\ 0 \\ 0 \end{pmatrix} + \alpha \begin{pmatrix} -1/2 \\ -3/2 \\ 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} -11/2 \\ -11/2 \\ 0 \\ 1 \end{pmatrix} \quad \forall \alpha, \beta \in \mathbb{R}.$
17. Note que $B = M + A$. Multiplique.
19. (a) Use escalonamiento (intercambie filas si es necesario).
    (b) Idem (a).
20. Escalone y piense en la factibilidad de las operaciones, según los valores de α, β y γ.
21. $L = (\ell_{ij})$ con $\ell_{ij} = \begin{cases} 1 & \text{si } i \geq j \\ 0 & \text{si no} \end{cases}$
    $U = (u_{ij})$ con $u_{ij} = \begin{cases} 1 & \text{si } i \leq j \\ 0 & \text{si no} \end{cases}$

Justifique usando el hecho que $a_{ij} = \sum_{k=1}^{n} \ell_{ik} u_{kj} \quad \forall i, j$.

23. $B^{-1} = \begin{pmatrix} A^{-1} - \frac{A^{-1}u\ {}^tuA^{-1}}{\gamma} & -\frac{A^{-1}u}{\gamma} \\ -\frac{{}^tuA^{-1}}{\gamma} & \frac{1}{\gamma} \end{pmatrix}$, donde $\gamma = \alpha - {}^tuA^{-1}u$.

    Luego, es necesario que $\alpha \neq {}^tuA^{-1}u$.

24. Aplique el método para calcular LU y luego justifique considerando $a_{ij} = \sum_{k=1}^{n} \ell_{ik} u_{kj}$.

27. En total (sumas y productos), obviando los productos por 0 y 1, (que no son efectivos), se tiene $pq(2(m+n)-1)$ operaciones.

Tema 1-VII.

1. Considere $A = \begin{pmatrix} 2 & 2 & 2 \\ 2 & 2 & 2 \\ 2 & 2 & 2 \end{pmatrix}$

3. Si $A = \begin{pmatrix} 0 & a_{12} & a_{13} \\ -a_{12} & 0 & a_{23} \\ -a_{13} & -a_{23} & 0 \end{pmatrix} \in MA_3$, entonces $S(A) = 0$ y $a_{12} = -a_{13} = a_{23}$.

Tema 2-VII.

1. Si $s(n)$ es el número de sumas en el algoritmo de Strassen y $n = 2^k$, entonces:

$$s(2^1) = 18$$
$$s(2^k) = 7 \cdot s(2^{k-1}) + 18 \cdot (2^{k-1})^2$$

   de donde $s(2^k) = 6 \cdot (7^k - 4^k)$. De aquí, si $n = 2^k, s(n) < 6 \cdot n^{log_2 7} < n^3 - n^2$.

2. Si $2^{k-1} < n < 2^k$, complete con ceros las $2^k - n$ lineas y columnas de modo de obtener:

$$A' = \begin{bmatrix} & & & 0 & \cdots & 0 \\ & A & & \vdots & & \vdots \\ & & & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ & \ddots & & \vdots & & \vdots \\ 0 & & 0 & 0 & & 0 \end{bmatrix} \text{ y } B' = \begin{bmatrix} & & & 0 & \cdots & 0 \\ & B & & \vdots & & \vdots \\ & & & 0 & & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{bmatrix}$$
$$\underbrace{\qquad\qquad}_{2^k} \qquad\qquad \underbrace{\qquad\qquad}_{2^k}$$

   Aplique el algoritmo para calcular $A' \cdot B'$ y observe que el número de multiplicaciones es menor que $7n^{log_2 7}$.

REFERENCIAS

- Caractères de Divisibilité, Suite de Fibonacci,
N. Vorobieu, Colección "Initiations aux Mathématiques", Ed. MIR, Moscú, 1973.

- Nouvelles Orientations des Mathématiques,
I. Yaglom et al, Colección "Initiations aux Mathématiques", Ed. MIR, Moscú, 1975.

- La Inducción en Geometría,
G. Yaglom, Colección "Temas Matemáticos", Ed. Limusa-Wiley, 1961.

Texto en el cual nos inspiramos para la "Partición de la Atlántida" (tema del capítulo II). En este libro se tratan diversos problemas relacionados con la coloración de mapas y grafos. Si usted desea saber más sobre este bestiario se recomienda "The four-color problem" (T.S. Saaty, P.C. Kainen, DOVER, 1986).

- Mariages Stables,
D.E. Knuth, Presses de l'Université de Montréal, 1976.

Este librito reúne varias conferencias de Knuth, el fecundo en ardides. La agencia "La Solución" (Tema del capítulo III) nace de su primera conferencia.

Para los fanáticos del problema se recomienda el libro "The Stable marriage problem" (D. Gusfield, R.W. Irving, MIT-Press, 1989).

- Introduction à l'Algèbre,
R.V. Andrée, Ed. Gauthier Villars-Mouton, Paris, La Haye, 1968.

Texto de iniciación al álgebra con interesantes y abundantes ejercicios. El tema "Congruencias lineales" (capítulo III) se inspira en el capítulo II de este libro.

- Theorie des Graphes et Structures Sociales,
C. Flament, Ed. Gauthier Villars-Mouton, Paris-La Haye, 1968.

- Algèbre et Combinatoire,
Varios Autores, Coll. Cahiers Mathématiques, Vol 3, Ed. Gauthier Villars Mouton, Paris - La Haye, 1970.

En esta variada colección de textos algebraicos, se encuentra el artículo "Un exercise de calcul logique chez les indiens des prairies" (G.Th. Guibaud), al cual nos remitimos para el tema "Parentesco en la gran pradera", del capítulo III.

- Introduction à la théorie des groupes,
P.S. Alexandroff, Dunod, París, 1968.

- Éléments d'Algèbre Moderne,
A. Lentin, J. Rivaud, Vuibert, París, 1961.

- Introduction to Modern Abstract Algebra,
D. M. Burton, Addison-Wesley, 1967.

- Introduction à l'algèbre,
A. Kostrikin, Ed. MIR, Moscú, 1977.

Excelente obra de la desaparecida URSS y su sólida tradición matemática.

- Principes de Combinatoire,
C. Berge, Dunod, 1968.

- Deux Etudes Mathématiques sur la parenté,
I. Chevallard, CEDIC, IREM de Marsella, 1977.

Aquí aparece el modelo presentado en "Sobre parentela, casorios y tribus" (capítulo IV). Todo esto huele muchísimo a Levi-Strauss. Si está interesado, lea "Tristes Trópicos" del mismo autor... no se arrepentirá.

- Estructuras Algebraicas,
E. Gentile, Monografía Nº 3, Serie Matemática, OEA, 1967.

B^3: bueno, bonito, barato; aunque sospechamos agotado.

- Discrete mathematical structures and their applications,
H.S. Stone, The SRA Computer Sciences Series, 1973.

- Les estructures Vol 1-2,
R. Ziglom, Collection Formation des enseignants, Hermann, 1973.

Fecundo y formalísimo libro orientado a las estructuras algebraicas. ¡ FBI ! (francés, bueno, interesante).

- Mathématiques et Jeux d'Enfants,
N. Picard, Casterman/Poche, Francia, 1970.

Si lo lee con la seriedad de un niño habrá ganado mucho.

- Discrete and Combinatorial Mathematics,
R.P. Grimaldi, Addison-Wesley, 1985.

Excelentes ejercicios de naturaleza combinatoria y recursiva.

- Mathématiques venues d'ailleurs,
diversos autores rusos, Ed. Belin, Francia, 1982.

De aquí nace el affaire de los "Tallarines con Salsa" (tema capítulo II). Aparte de este caso, aparecen bellísimos problemas, en su mayoría abordables para el lector levemente fanático.

- Concrete Mathematics,
R. Graham, D. Knuth, O. Patashnik.
Addison-Wesley, 1988.

Un "atracón" de pizzas (tema del capítulo II) y otras hierbas recurrentes. Se recomienda sin reservas el primer capítulo.

- Mathematical Gems II-III,
Math. Assoc. of America 1976, 1985.

Multitud de interesantes temas y problemas. En Gems II aparece la cota para el número de operaciones del algoritmo de Euclides (tema "Sobre bases, Euclides y otras hierbas", capítulo III). En Gems III se presentan bellas y profundas propiedades de la sucesión de Fibonacci, en particular su interpretación como embaldosado (tema "Más recurrencias", capítulo II).

- Sand-Piles on line-graphs,
E. Goles, M.K. Kiwi, Theoretical Computer Science, 1983.

En este artículo se presentan algunos resultados y aplicaciones de las pilas de arena. Este modelo "playero" se trata en el tema "Ordenes son órdenes" (capítulo III). Señalamos que el orden parcial fue determinado por el Dr. Brilawski en 1973.

- The design and analysis of computer algorithms,
A. Aho, J. Hopcroft, J. Ullman, Addison-Wesley, 1974.

Texto dedicado a los algoritmos de naturaleza esencialmente discreta. Para los fanáticos: trata "in-extenso" el asunto de Strassen (tema del capítulo VII).

Aparte de las referencias anteriores, recomendamos, para ejercitarse y/o maravillarse, las siguientes obras:

- Teoría y problemas de álgebra moderna,
F. Ayres, Mc. Graw-Hill Latinoamericana, 1970.

Lo elemental y cualquier cantidad de ejercicios propuestos y resueltos (en la línea Schaum). No es suficiente para el nivel del libro.

- Teoría y Problemas de Matemáticas finitas.
S. Lipschitz, Mc.Graw-Hill, 1978.

- Theory and Problems of Abstract Algebra.
J. Fang, Schaum Publishing, 1963.

- Algebra.
Ch. Lehmann, Limusa 1986.

Presentación clásica. Lectura y ejercicios afines para inducción, complejos, progresiones y combinatoria. Nivel intermedio.

- The Theory of Groups.
I. Mc Donald, Oxford University Press, 1968.

Los tres primeros capítulos son interesantes. Traen ejemplos de grupos, subgrupos y resultados fundamentales (incluyendo morfismos). Ejercicios de variada dificultad.

- Algebra.
S. Lang, Addison-Wesley, 1971.

Estructuras a nivel profundo. No apto para cardíacos. (Aunque ni tanto).

- Algèbre M.P. et Spéciales AA.
M. Quiysanne, A. Colin, Francia, 1964.

Muy formal y compuesto. De lectura difícil, pero con ejercicios interesantísimos.

- Estructuras de matemáticas discretas para la computación.
B. Kolman, R. Busby, Prentice-Hall, 1986.

Otra onda: visión algorítmica elemental de los tópicos algebraicos. Son afines los capítulos 1 al 4 y 6.

GLOSARIO

Abeliano (grupo) 267
Algoritmo, noción de 68
de Euclides 144
de Gauss 394, 402
de la división 143
de "La solución" 189, 193, 194
de Strassen 421
Anillo(s), definición 262, 288, 289
de matrices 374
de polinomios 336, 338
conmutativos 289
conmutativos con unidad 289
propiedades de un 291
Argumento de un complejo 330
Argumento principal de un complejo 331
Asociatividad 22, 34, 253
Autómata Celular 315
Automorfismos 265
Base de un número 168
Binomio de Newton 80
Cambio de variables 71
Caminos en un grafo 179, 180
Cardinal de un conjunto 36, 233
de un producto cartesiano 125
del continuo 237
cardinalidad 233
Circuito lógico 51
en un grafo 184
Clases de congruencia módulo p 154
de equivalencia 153
Clasificación de estructuras 262
de relaciones 133
de funciones 211
Coeficientes binomiales 76, 78, 82, 105
polinomiales 337, 353
Coloración de mapas 98
Complejidad del algoritmo de Gauss 402
euclideana 170
Complejo(s), definición 323, 324
argumento de un 330

argumento principal de un 331
conjugado 325
cuerpo de los 324
parte imaginaria de 325
parte real de 325
potencias de 332
producto de 324
raíces de 333, 335
suma de 324
Complemento de un conjunto 31
Conectivos lógicos 19
Congruencias módulo p 154
Congruencias lineales 173
Conjugados 325, 352
Conjunción 20
Conjunto(s), definición 25
definición por comprensión 27
definición por extensión 27
igualdad de 27
cociente 154
de palabras 309
de partes 30, 238
enumerables 234
imagen 206
normal 59, 60
patológico 59, 60
singleton 27
universo 27, 31
vacío 27
disjuntos 32
finitos 36
infinitos 36, 233
diferencia de 31
diferencia simétrica de 35
intersección de 32, 41
partición de 41
pertenencia a un 25, 26
unión de 32, 41
Conmutatividad 23, 34, 253
Composición funciones 219, 220
Contrarecíproca 23

Cuantificadores lógicos 37
Cuerpo de los complejos 324
Cuerpo, definición 262, 293
Desigualdad triangular 329
Diagonalización de Cantor 237
Diagrama de Venn 33
Diferencia de progresión 74
Diferencia simétrica 35
Distributividad 23, 34, 253
Disyunción 20
Dividir para conquistar 68, 417
Divisibilidad en $\mathbb{N}$ 143
División de polinomios 340
Divisores de cero 292, 340
Doble implicación 21, 23
Dominio de funciones 205
de proposiciones 37
de relaciones 126
Ecuación de congruencia 173
Elemento absorbente 253
cancelable 256, 258
de un conjunto 25
idempotente 253
inverso 225, 226, 250, 253
neutro 250, 253
Emparejamiento 186
Equivalencia lógica 21
Escalonamiento de una matriz 386, 390
Estable 187
Estructura algebraica 252
de congruencia 259
de grupo 262, 267
de anillo 262, 289
de cuerpo 262, 293
de parentesco 241, 242
Estructuras isomorfas 265
Exogamia 240
Expresión de un número en base b 168
Extensión de una función 211
Factor izquierdo de un grupo 282, 283
Factorial de un número 76

Máximo común divisor de enteros 144
de polinomios 344
Módulo de un complejo 328
Morfismos 263
Negación lógica 19, 23
de cuantificadores 38
Notación aditiva 253, 288
multiplicativa 253, 288
por filas 377
por columnas 377
Números complejos 323
primos 148
primos relativos 147
naturales 26
enteros 26
racionales 26
irracionales 26
reales 26
Operación 226, 247, 252
Orden parcial 142
total 142
Orden de un grupo 268
Orden lexicográfico 141,142
Palabra 309
Palabra vacía 309
Paradoja de Russell 59, 241
Pares conjugados 352
Pares ordenados 121
Parte imaginaria de un complejo 325
real de un complejo 325
Partición de conjuntos 41, 153
Particiones ordenadas 195
Permutaciones 223, 224, 225
Permutación circular 286
Pertenencia a un conjunto 25, 26
Pila de una partición ordenada 195
Pivotes 390
Polinomio(s), definición formal 336
cociente 341
mónico 339, 344
resto 341

irreductibles 350, 351, 353
reductibles 350
multiplicación de 337
raíces de un 345, 346, 348
suma de 337
Potencia de un complejo 332
de una matriz 379
booleana de matriz 284
Preimagen de funciones 207
Principio de contradicción 23
de inducción matemática 63, 65, 66
del palomar 214
del tercero excluído 23
Producto cartesiano 123
de matrices 138, 275, 276, 376
de polinomios 337
Progresión aritmética 74
geométrica 75
Propiedad(es) de un anillo 291
de un grupo 268
telescópica 71
Proposición lógica 19
Raíces de la unidad 335
de un complejo 333
de un polinomio 345, 346, 348
Razón de progresión 75
Recorrido de funciones 205
Recurrencia de Fibonacci 116
Recurrencias 68
Reflexiones 250
Relación(es) binarias 126
de equivalencia 133, 150
de orden 133, 141
de orden parcial 142
de orden total 142
antisimétrica 133
refleja 133
simétrica 133
transitiva 133
representaciones de 128, 129
Representación de Cayley 272

Representación cartesiana 128, 134
Representación mediante un grafo 128, 135
Representación matricial 129, 136
Representaciones de una relación 128
Restricción de una función 210
Sistemas de ecuaciones 386, 391
lineales 386, 391
homogéneos de ecuaciones 393
no homogéneo de ecuaciones 393
cuadrados 394
Subconjunto propio 30
Subconjuntos 29
Subestructuras 258
Subgrupos 270, 271
Subgrupo propio 271
Sucesión de Fibonacci 116
Suma de complejos 323
real de cuadrados naturales 72
de cubos naturales 73
de matrices 371
de polinomios 337
Sumatorias 69, 70
Sumatorias múltiples 86
Tablas de preferencia 187
Tabla de Pitágoras 225, 257, 259, 273
Tablas de verdad 19
Tautología 22
Teorema de Cayley 272, 273
Teorema de Cantor 237
de D'Alembert 348
de Euler 97
de Lagrange 282, 284
de los cinco colores 99
fundamental de la aritmética 148
fundamental del álgebra 348
lógico 22
Torres de Hanoi 107
Traspuesta (matriz) 137
Triángulo de Pascal 78, 105
Unidad imaginaria 323, 327
Unión de conjuntos 32

Valor de verdad 19
Variable dependiente 387
independiente 387