conceptos básicos matemática moderna

*

CONCEPTOS BASICOS
DE MATEMATICA MODERNA

Queda hecho el depósito que marca la ley 11.723

Primera edición

Printed in Argentina Impreso en Argentina

Libro de edición argentina

conceptos básicos de matemática moderna

ROBERTO P. J. HERNANDEZ
ARMANDO O. ROJO
HEBE T. RABUFFETTI
MARIA ESTHER S. DE HERNANDEZ

EDITORIAL CODEX S. A.
BUENOS AIRES

ROBERTO P. J. HERNANDEZ

Profesor del Instituto Nacional Superior del Profesorado.
Miembro de la Comisión Nacional Argentina
para la enseñanza de la Matemática.

ARMANDO O. ROJO

Profesor del Instituto Nacional Superior del Profesorado
y del Colegio Nacional de Buenos Aires.

HEBE T. RABUFFETTI

Profesora del Instituto Nacional Superior del Profesorado
y del Profesorado Especializado
de la Escuela Normal Nº 1 de Buenos Aires.

MARIA ESTHER S. DE HERNANDEZ

Profesora del Colegio Nacional de Buenos Aires
y del Profesorado Especializado
de la Escuela Normal Nº 1 de Buenos Aires

ÍNDICE

PRIMERA PARTE

CAPITULO I — Lógica matemática

1. — Lógica simbólica y cálculo proposicional 3
2. — Notaciones y conectivos lógicos 4
3. — Conjunción o producto lógico 4
4. — Disyunción o suma lógica 5
5. — Negación 6
6. — Implicación material o condicional 7
7. — Condiciones necesarias y suficientes 8
8. — Bicondicional, doble implicación o equivalencia 9
9. — Tautologías, contradicciones y leyes del cálculo proposicional 10
10. — Implicaciones asociadas a una dada 11
11. — Razonamiento deductivo válido 13
12. — Funciones proposicionales y cuantificadores 14
Ejercicios 17

CAPITULO II — Teoría de conjuntos

1. — Conjuntos: su determinación 19
2. — Conjuntos especiales 22
3. — Relaciones entre conjuntos 24
4. — Operaciones entre conjuntos 27
5. — Propiedades de las operaciones entre conjuntos 31
6. — Cupla o par ordenado 33
7. — Producto cartesiano 35
Ejercicios 37

CAPITULO III — **Relaciones**

1. — Relación binaria ... 39
2. — Relación n-aria ... 43
3. — Propiedades de las relaciones binarias ... 43
4. — Relaciones de equivalencia ... 45
5. — Relaciones de orden ... 51
6. — Relaciones funcionales o aplicaciones ... 54

Ejercicios ... 59

CAPITULO IV — **Leyes algebraicas**

1. — Leyes de composición interna ... 63
2. — Propiedades de las leyes de composición interna ... 65
3. — Elementos particulares ... 72
4. — Composición de aplicaciones ... 76
5. — Leyes de composición externa ... 78
6. — Propiedades de las leyes de composición externa ... 79
7. — Homomorfismos. Isomorfismos ... 82

Ejercicios ... 87

CAPITULO V — **Estructuras algebraicas**

1. — Grupos ... 89
2. — Propiedades de los grupos ... 90
3. — Grupos finitos ... 93
4. — Subgrupos ... 97
5. — Semigrupos ... 97
6. — Grupos ordenados ... 98
7. — Anillos ... 98
8. — Propiedades de los anillos ... 100
9. — Subanillos ... 102
10. — Anillos de integridad ... 102
11. — Dominios de integridad ... 104
12. — Cuerpos ... 104
13. — Subcuerpos ... 106
14. — Espacios vectoriales ... 107
15. — Familia libre. Base y dimensión de un espacio vectorial ... 108

Ejercicios ... 113

CAPITULO VI — **Axiomática**

1. — El método matemático ... 115
2. — Ejemplo de un sistema axiomático ... 117
3. — Otro ejemplo de sistema axiomático ... 118
4. — Propiedades de los sistemas axiomáticos ... 120

Ejercicios ... 126

CAPITULO VII — **El número y sus generalizaciones**

1. — Evolución del concepto de número ... 127
2. — El número natural. Su fundamentación ... 128
3. — Fundamentación axiomática del número natural ... 128
4. — Adición y multiplicación de números naturales en el sistema de Peano ... 131
5. — Otros sistemas axiomáticos para el número natural ... 133
6. — Fundamentación del número natural por teoría de conjuntos ... 134
7. — Definición axiomática de las operaciones entre los números naturales ... 136
8. — Propiedades estructurales del conjunto de los números naturales ... 137
9. — Extensión del concepto de número ... 137
10. — El número entero ... 138

11. — Construcción de los enteros por el método genético 138
12. — Adición y multiplicación de números enteros 141
13. — Isomorfismo entre los números naturales y los enteros positivos 144
14. — Sustracción de números enteros 145
15. — Propiedades estructurales de los números enteros 147
16. — Construcción axiomática de los enteros 147
Ejercicios 149

CAPITULO VIII — Introducción a la aritmética trasfinita

1. — Definiciones y propiedades usuales 151
2. — Números cardinales y conjuntos numerables 153
3. — Comparación de números cardinales 154
4. — Propiedades de los conjuntos numerables 156
5. — Potencia del conjunto de los racionales 158
6. — Potencia del conjunto de los números reales 159
7. — Números algebraicos y trascendentes 160
8. — Potencia del conjunto de los números algebraicos 162
9. — Números trascendentes 163
10. — Potencia del conjunto de las funciones reales 164
Ejercicios 165

SEGUNDA PARTE

CAPITULO IX — De la geometría clásica a la geometría moderna

1. — Los Elementos 170
2. — La axiomática de Euclides 171
3. — El postulado V y la teoría del paralelismo 174
4. — Revisión crítica de la geometría en el siglo XIX 177
5. — La axiomatización de la geometría 180
6. — Formulación de Hilbert para la métrica euclidiana 183

CAPITULO X — Las estructuras geométricas

1. — Transformaciones geométricas 187
2. — Transformaciones métricas 188
3. — Grupo de transformaciones métricas 194
4. — Transformaciones proyectivas 195
5. — Grupo de transformaciones proyectivas 197
6. — Relaciones entre el grupo fundamental y el grupo proyectivo 198
7. — Las geometrías 200
8. — Las estructuras geométricas 201
9. — Metodología de las estructuras 203
10. — Aplicación del principio de Klein en la métrica y la proyectiva 204
11. — Geometrías elementales 207
12. — Otras estructuras geométricas 211

CAPITULO XI — Geometrías no euclidianas

1. — Geometría de Euclides 215
2. — La negación del axioma V 216
3. — Compatibilidad de la geometría euclídea 217
4. — Geometría absoluta 219
5. — Geometría de Lobatchefsky 222
6. — Compatibilidad de la geometría hiperbólica 223
7. — Geometrías de Riemann 228
8. — Resumen 230

CAPITULO XII — **Geometría vectorial**

1. — Desarrollo vectorial de la geometría 233
2. — Espacio vectorial de matrices columnas sobre el cuerpo de los reales 233
3. — Dependencia lineal de vectores en el plano 235
4. — Base canónica en R^2 236
5. — Cambio de base en R^2 237
6. — Geometría en el plano afín 238
7. — Geometría métrica euclidiana en el plano 242

APÉNDICE

CAPITULO XIII — **Polinomios**

1. — Espacio vectorial de polinomios 254
2. — Producto de polinomios 257
3. — Anillo de polinomios 257
4. — El proceso de sustitución 259
Ejercicios 261

CAPITULO XIV — **Los sistemas de numeración**

1. — La numeración 263
2. — Propiedades de los sistemas de numeración 269
3. — Operaciones en los sistemas de numeración 271
4. — Tablas de adición y multiplicación 273
5. — Pasaje entre sistemas 275
Ejercicios 278

CAPITULO XV — **Homotecia en el plano**

1. — Definición y propiedades elementales 279
2. — Transformación de rectas, semirrectas y segmentos 281
3. — Transformación de ángulos 284
4. — Transformación de circunferencias 285
5. — Aplicaciones 291
6. — Producto de dos homotecias 294
Ejercicios 297

CAPITULO XVI — **Aplicaciones vectoriales a la trigonometría**

1. — Las dos orientaciones del espacio y el producto vectorial 299
2. — Distributividad del producto vectorial respecto de la suma de vectores . 301
3. — Expresión canónica del producto vectorial 303
4. — Coseno de la suma y de la diferencia de dos ángulos 304
5. — Seno de la diferencia y de la suma de dos ángulos 305
6. — Teorema del seno 306
7. — Teorema del coseno 307
8. — Doble producto vectorial 308
9. — Producto escalar de dos productos vectoriales 309
10. — Teorema del coseno para los lados de un triángulo esférico 309
Ejercicios 310

Indice alfabético 312

LISTA DE SÍMBOLOS

$\wedge$	Conjunción
$\vee$	Disyunción (incluyente)
$\veebar$	Disyunción (excluyente)
$\sim$	Negación; relación de equivalencia
$\Rightarrow$	Implicación material
$\Leftrightarrow$	Equivalencia lógica
$/$	Tal que
$\forall$	Cuantificador universal
$\exists$	Cuantificador existencial
$\in$	Pertenencia
$\subseteq$	Inclusión amplia
$\subset$	Inclusión propia
$\emptyset$	Conjunto vacío
$\cup$	Unión
$\cap$	Intersección
$\triangle$	Diferencia simétrica
$\complement A$	Complemento de A
$\sim$	Equipotencia o coordinabilidad
$\mathcal{P}(E)$	Potencial de E
$\equiv$	Congruencia
$\doteq$	Equivalencia entre transformaciones
$\prec$	Precede
$\mid$	Divisor de

PRÓLOGO

La historia de la matemática nos enseña que, a través de todas las épocas, los reordenamientos de esta ciencia han tenido siempre un punto de partida común: el reemplazo de conceptos aceptados como primitivos e introducidos intuitivamente, por planteos más generales, que sirvieran de base para construir una imagen abstracta de los conceptos precedentemente considerados como intuitivos.

Desde este punto de vista, el fin del siglo XIX y el comienzo del siglo XX, representan momentos verdaderamente revolucionarios para la construcción matemática, a partir de la primera formulación de la teoría de conjuntos. Mediante la axiomatización y la formalización aplicadas a esa teoría conjuntista se llega a la reconstrucción de todos los conceptos matemáticos. Pero a diferencia de otros replanteos anteriores, este último implica la obtención de estructuras generales aplicables a todo tipo de entes matemáticos: un mismo esquema satisface a todas las ramas de la matemática; sólo es necesario reemplazar un ente por otro para desarrollar una u otra de esas ramas.

Es esta significación de la matemática, la que se da en llamar, actualmente, matemática moderna. Tal vez no sea ésta la designación más afortunada, puesto que ese modernismo se refiere a la construcción actual de nuestra ciencia y no al contenido. Matemática moderna debiera asociarse más bien a matemática univalente —una sola estructura comprendiendo todos los contenidos— en contraposición con la matemática clásica, típicamente multivalente.

Precisamente, por ser éste el alcance de la matemática, es que asignamos carácter de revolucionario al actual ordenamiento; terminó con las distintas matemáticas para hacer nacer una única ciencia. Y esta circunstancia hace que el fenómeno sea realmente irreversible por cuanto nunca como ahora se ha estado de lleno en el esquema acorde con el sentido que es propio a la esencia matemática.

No existiendo dudas respecto de qué debe entenderse hoy por matemática, tampoco puede haber indeterminación sobre qué debe enseñarse de esta ciencia. Lo que resta aún por precisar es "cómo", "cuándo" y "cuánto" debe enseñarse. La solución de este problema no es simple y probablemente sólo se obtendrá una respuesta satisfactoria, sujeta a perfeccionamientos sucesivos, a través de una intensa experimentación que permita ir acotando esos interrogantes.

La etapa educativa que agudiza esa indeterminación es la secundaria, ya que debe superar el carácter intuitivo informativo de la escuela primaria pero sin poder disponer todavía de una capacidad de abstracción en el educando que sólo puede esperarse en la etapa de los estudios superiores.

Surge así que es en la escuela secundaria —ya de por sí anacrónica en múltiples aspectos— donde debe llevarse a cabo esa experimentación sistemática a fin de poder renovar su estructura en el plazo más breve posible. Los profesores de matemática de la enseñanza media tienen por ello, ante sí, una tarea de trascendencia histórica que es imposible postergar o retacear.

Con la intención de colaborar con los colegas de la enseñanza secundaria, los autores concibieron un plan ambicioso: la publicación de una colección de obras de matemática moderna dirigida justamente hacia esos colegas y a los estudiantes en niveles superiores. Tal colección estará compuesta por las obras siguientes:

* Conceptos básicos de matemática moderna.
* Álgebra. Estructuras numéricas.
* Estructuras algebraicas.
* Introducción al análisis.
* Introducción a la geometría moderna.
* Geometría vectorial.

Este libro constituye, pues, el primer tomo de esa colección y pretende ser un extenso prólogo matemático de la misma. La primera y segunda parte contienen todos los elementos que hoy se estiman indispensables para la construcción de la matemática con su significación actual: la primera dirigida al álgebra; la segunda a la geometría. Naturalmente los temas tratados han sido introducidos con rigor, pero sin detalles exhaustivos, este último aspecto caracterizará los siguientes volúmenes específicos de esta colección.

Un apéndice final incluye el desarrollo de cuatro temas particulares, en el nivel en el que los autores entienden, pueden enseñarse en la escuela secundaria reorganizada.

Este libro y los que integrarán toda la colección, responden a un plan que configura una completa unidad para toda la obra. Independientemente de esa unidad, los autores conservan sus propias modalidades en los distintos volúmenes, condición que se anticipa también en este primer tomo, en el cual cada capítulo ha sido escrito por uno de los autores según el alcance y contenido previamente establecido por aquel plan, sin pretender siquiera uniformidad de estilo de redacción.

Los autores consideran que esa modalidad es una manera de presentarse individualmente a sus colegas, al iniciar una comunicación, que si bien por ahora vale sólo en el sentido autor-lector, desean fervorosamente sea establecida en los dos sentidos posibles.

El presente volumen tiene la siguiente distribución para la redacción final:

Capítulos IV, V, X y XIV : *Roberto P. J. Hernández*
Capítulos I, VIII, XII y XVI: *Armando O. Rojo*
Capítulos III, VI, XI y XIII : *Hebe T. Rabuffetti*
Capítulos II, VII, IX y XV : *María E. S. de Hernández*

LOS AUTORES

PRIMERA PARTE

CAPITULO I

Lógica Matemática

1. LÓGICA SIMBÓLICA Y CÁLCULO PROPOSICIONAL

El punto de partida de toda estructura matemática supone la necesidad de razonar en forma válida acerca de cosas trascendentes y singularmente importantes. Esto implica que ha de existir absoluta claridad y distinción en todo lo concerniente al razonamiento deductivo válido, esto es: significado de los términos usuales, uso de proposiciones, definiciones, teoremas, eliminación de las complicaciones y contingencias relativas a la vida cotidiana, reconocimiento y abandono de las falacias y ambigüedades, etc. Todo ello obliga a una gran simplificación y a la introducción de un simbolismo adecuado e inequívoco, que permite razonar válidamente mediante reglas fijadas con claridad, aunque sean arbitrarias.

Dos capítulos entrañablemente unidos dan este primer paso: la lógica simbólica y la teoría de conjuntos.

Vamos a desarrollar, en lo que sigue, los elementos más usuales en lógica matemática y que implícitamente estarán presentes en todo el texto.

Con miras a introducir el concepto de proposición, consideramos las siguientes oraciones:

(1) *¿Quién viene?*

(2) *Pase al frente.*

(3) *El aire es pesado.*

(4) *3 es un número par.*

(5) *Juan conoce a Pedro.*

(6) *Pedro es conocido por Juan.*

Se trata de seis oraciones diferentes: una pregunta, una orden, y cuatro declarativas. De las dos primeras no podemos decir que sean verdaderas ni falsas. En cambio, respecto de las cuatro últimas, que son declarativas, tiene sentido decir si son verdaderas o bien falsas. A éstas las llamamos proposiciones.

En una primera aproximación, podemos decir que proposición es toda oración declarativa, es decir, susceptible de ser verdadera o falsa. Sin embargo, no ha de creerse que oraciones declarativas distintas han de caracterizar proposiciones necesariamente diferentes; tal es el caso presentado en los ejemplos (5) y (6): ambas oraciones son distintas, pero tienen el mismo **significado;** por ello decimos que se trata de la misma proposición.

Definición

Proposición es el significado de toda oración declarativa.

Usualmente suele identificarse una proposición con cualquiera de las oraciones declarativas que admiten el mismo significado. En lógica bivalente, la nota esencial de toda proposición consiste en la posibilidad de ser verdadera, o bien falsa.

2. NOTACIONES Y CONECTIVOS LÓGICOS

Con las letras: p, q, r, etc., designaremos proposiciones cualesquiera. A partir de proposiciones simples obtendremos otras, simples o compuestas, es decir, operaremos con proposiciones; según sean tales operaciones utilizaremos los símbolos siguientes, llamados **conectivos lógicos:**

SÍMBOLO	OPERACIÓN ASOCIADA	SIGNIFICADO
$\wedge$	**Conjunción o producto lógico**	"y"
$\vee$	**Disyunción o suma lógica**	"o" (en sentido incluyente)
$\underline{\vee}$	**Diferencia simétrica**	"o" (en sentido excluyente)
$\sim$	**Negación**	"no", "no es cierto que"
$\Rightarrow$	**Implicación material**	"implica", "si... entonces..."
$\Leftrightarrow$	**Equivalencia**	"es equivalente a", "...si y sólo si..."

3. CONJUNCIÓN O PRODUCTO LÓGICO

Definición

Conjunción de las proposiciones p y q es la proposición compuesta p $\wedge$ q (p y q) que se obtiene uniéndolas, en el orden dado mediante la conjunción "y".

Esta definición se completa con una tabla, llamada de verdad, la cual establece la verdad o falsedad de la proposición compuesta en función de la verdad o falsedad de sus componentes. Dicha tabla de verdad es convencional, aunque su elección no resulta desvinculada de nuestra intuición.

Sean las proposiciones:

p: "Silvia estudia".

q: "Silvia camina".

La conjunción de ambas es:

$p \wedge q$: "Silvia estudia y camina".

La intuición nos dice que "$p \wedge q$" es verdadera cuando p y q lo son simultáneamente.

Adoptamos entonces la siguiente tabla de verdad para la conjunción:

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

En realidad, la tabla precedente es una definición de la conjunción. Por otra parte, expresiones como: "pero", "sin embargo", "aunque", utilizadas para unir dos proposiciones, tienen el mismo sentido conjuntivo que "y", y todas ellas admiten el símbolo lógico: "$\wedge$".

4. DISYUNCIÓN O SUMA LÓGICA

Definición

Disyunción de las proposiciones p y q **es la proposición compuesta** $p \vee q$ (p o q) **obtenida uniéndolas, en el orden dado, a través de la conjunción "o", con sentido incluyente.**

La palabra "o" en el lenguaje corriente es ambigua en el sentido de que puede denotar inclusión o exclusión. Por ejemplo:

"*No serán licenciados los soldados en caso de castigo o enfermedad*" (1)
"*A las 21 iré al cine o al teatro*" (2).

La proposición compuesta (1) significa evidentemente que los soldados que sólo han sido castigados, o que sólo han estado enfermos, o bien los que han padecido ambas cosas, no serán dados de baja; es claro entonces el sentido incluyente de la conjunción "o".

En la proposición (2), si un súceso se realiza el otro queda excluido, y es este sentido excluyente el que prevalece en función del mismo "o". Por ello es, no sólo conveniente, sino necesario, el empleo de un símbolo inequívoco para cada uno de dichos significados.

En el caso de la disyunción inclusiva, que es el más frecuente en matemática, la verdad de la proposición resultante queda asegurada con la verdad de una de sus componentes, y sólo es falsa cuando ambas lo son simultáneamente.

La tabla de verdad asociada a la disyunción es:

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

5. NEGACIÓN

Definición

Negación de una proposición p es la proposición $\sim p$ (no p), obtenida anteponiendo el adverbio "no" a la primera.

La tabla de verdad es:

p	$\sim p$
V	F
F	V

El símbolo "~" representa expresiones del tipo: "no", "no es cierto que", "no se da la posibilidad de que", "es falso que", etc.

6. IMPLICACIÓN MATERIAL O CONDICIONAL

Definición

Se llama implicación de las proposiciones p y q **a la proposición** $p \Rightarrow q$ **obtenida anteponiendo a la primera la palabra SI, y uniendo ambas mediante la palabra ENTONCES.**

Las proposiciones p y q se llaman **antecedente** y **consecuente,** respectivamente.

El tipo de implicación usual en matemática, y que desarrollaremos aquí, es material, en el sentido de que puede ocurrir que el consecuente no se derive lógicamente del antecedente; aunque si ello sucede, la implicación es formal y queda incluida en la primera.

Esta diferencia se pone de manifiesto a través de los siguientes ejemplos:

"SI un triángulo es equilátero, ENTONCES es isósceles."

"SI apruebo el examen, ENTONCES regreso a pie".

En el segundo caso, el consecuente no se deriva necesariamente del antecedente por cuanto se trata de una decisión personal, cosa que no ocurre en el primero.

Interesa inducir la tabla de verdad de la implicación, para lo cual investigaremos en qué condiciones se verificaría la falsedad de la misma. Sean las proposiciones:

p: *Claudio se porta bien.*

q: *Claudio va al cine.*

La proposición compuesta es:

$p \Rightarrow q$: *SI Claudio se porta bien, ENTONCES va al cine.*

Para Claudio sería inaceptable, es decir falso, que se porte bien y no lo lleven al cine. Los demás posibilidades son verdaderas. En matemática ocurre lo mismo: sólo interesa que sea falsa una implicación si el antecedente es verdadero y el consecuente falso.

Simbólicamente: $p \wedge \sim q$ es F

En consecuencia: $\sim(p \wedge \sim q)$ es V

Consideraremos entonces como equivalentes las proposiciones:

$$p \Rightarrow q \quad y \quad \sim(p \wedge \sim q)$$

En tal caso, la tabla de verdad de la implicación material se reduce a otras conocidas y la confeccionamos así:

p	q	~q	p ∧ ~q	~(p ∧ ~q)	p ⇒ q
V	V	F	F	V	V
V	F	V	V	F	F
F	V	F	F	V	V
F	F	V	F	V	V

Insistimos en que no es necesario que exista relación alguna entre el antecedente y el consecuente de la implicación material. Así, de acuerdo con la tabla anterior, si se tienen las proposiciones:

p: *"Buenos Aires es una ciudad uruguaya"*. F

q: *"2 es un número impar"*. F

La implicación o condicional:

"Si Buenos Aires es una ciudad uruguaya, entonces 2 es un número impar",

es verdadera.

7. CONDICIONES NECESARIAS Y SUFICIENTES

Sea la tabla de verdad de la implicación:

p	q	p ⇒ q
V	V	V
V	F	F
F	V	V
F	F	V

Hay tres casos en que p ⇒ q es V, y en ellos, si p es V, q también lo es; pero si p es F, q puede ser V o F. Suele decirse entonces, cuando p ⇒ q es V, que **"p es condición suficiente para q"** y que **"q es condición necesaria para p"**. Es decir: siendo p ⇒ q una proposición verdadera, se tiene:

 si p es V, entonces q es V (p es condición suficiente para q) y en el mismo caso, puede verificarse p sólo si se verifica q (q es condición necesaria para p).

Por ejemplo, dada la implicación verdadera:

"SI un triángulo es equilátero, ENTONCES es isósceles", podemos decir: (1) que un triángulo sea equilátero, es condición suficiente para que sea isósceles. Y también: (2) que un triángulo sea isósceles, es condición necesaria para que sea equilátero.

Son formas equivalentes a estas condiciones, las siguientes:

q si p (condición suficiente)

p sólo si q (condición necesaria)

8. BICONDICIONAL, DOBLE IMPLICACIÓN O EQUIVALENCIA

Sean las proposiciones:

p: *"ABC es un triángulo equilátero"*

q: *"ABC es un triángulo equiángulo"*

Si consideramos las implicaciones: $p \Rightarrow q$ y $q \Rightarrow p$, ocurre que cada proposición es condición necesaria y suficiente para la otra, en cuyo caso se dice que son equivalentes, cuestión que se denota con el símbolo $p \Leftrightarrow q$, que leeremos: "p si y sólo si q".

Definición

Dadas las proposiciones p y q, se llama doble implicación o bicondicional a la proposición $(p \Rightarrow q) \wedge (q \Rightarrow p)$.

Su tabla de verdad es, en consecuencia:

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

Resulta entonces, que el bicondicional es verdadero cuando p y q tienen el mismo valor de verdad, esto es, cuando ambas son simultáneamente verdaderas, o bien falsas. Cuando $p \Leftrightarrow q$ es V, suele decirse que **"p es condición necesaria y suficiente para q".**

9. TAUTOLOGÍAS, CONTRADICCIONES Y LEYES DE CÁLCULO PROPOSICIONAL

Consideremos la implicación:

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

cuya tabla de verdad es:

p	q	$p \Rightarrow q$	$(p \Rightarrow q) \wedge p$	$[(p \Rightarrow q) \wedge p] \Rightarrow q$
V	V	V	V	V
V	F	F	F	V
F	V	V	F	V
F	F	V	F	V

Observamos aquí que la proposición compuesta resulta siempre verdadera, independientemente del valor de verdad de las componentes. Se dice entonces que tal proposición es una **tautología** o **ley lógica**

Análogamente lo es, por ejemplo, $p \vee \sim p$.

Sea en cambio la proposición: $p \wedge \sim p$. Su tabla de verdad nos muestra que resulta siempre falsa, y por tal motivo se dice que es una **contradicción.**

En el cálculo proposicional son usuales las siguientes leyes o tautologías:

I) Involución $\sim(\sim p) \Leftrightarrow p$

II) Asociatividad

a) **de la disyunción:** $(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$

b) **de la conjunción:** $(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$

III) Distributividad

a) **de la conjunción respecto de la disyunción:**

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

b) **de la disyunción respecto de la conjunción:**

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

IV) Idempotencia

$$p \vee p \Leftrightarrow p$$
$$p \wedge p \Leftrightarrow p$$

V) Leyes de De Morgan

a) **La negación de una disyunción es equivalente a la conjunción de las negaciones:**

$$\sim(p \vee q) \Leftrightarrow \sim p \wedge \sim q$$

b) **La negación de una conjunción es equivalente a la disyunción de las negaciones:**

$$\sim(p \wedge q) \Leftrightarrow \sim p \vee \sim q$$

La demostración de cualquiera de las leyes enunciadas es muy simple, y se reduce a la construcción de la tabla de verdad correspondiente. Como ejemplo, probaremos esta última:

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

En lógica bivalente, dados n proposiciones, se presentan tantas posibilidades para la construcción de una tabla de verdad como variaciones con repetición de dos elementos de orden n, es decir: 2^n. Tal es el número de filas que contiene la tabla de verdad asociada a n proposiciones componentes. De este modo, el lector podrá comprobar que las tablas de verdad de las leyes asociativas y distributivas constan de $2^3 = 8$ filas.

10. IMPLICACIONES ASOCIADAS A UNA DADA

Sea el condicional $p \Rightarrow q$, que llamamos **directo;** en conexión con él se presentan otros tres:

$q \Rightarrow p$ **recíproco**
$\sim p \Rightarrow \sim q$ **contrario**
$\sim q \Rightarrow \sim p$ **contrarrecíproco,** obtenidos por las permu-

taciones o negaciones posibles del antecedente y consecuente de la implicación dada. Los cuatro condicionales propuestos reciben el nombre de **implicaciones conjugadas,** y eventualmente cualquiera de ellas puede tomarse como directa. El siguiente esquema nos proporciona la relación que las vincula:

Verificamos, mediante tablas de verdad, que los condicionales contrarrecíprocos son equivalentes:

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

Es decir, son tautologías los bicondicionales:

$$(p \Rightarrow q) \Leftrightarrow (\sim q \Rightarrow \sim p)$$

$$(q \Rightarrow p) \Leftrightarrow (\sim p \Rightarrow \sim q)$$

Si la implicación directa es verdadera, nada podemos asegurar respecto de la V o F de la implicación recíproca y contraria. Por otra parte, cuando un condicional se verifica junto con su recíproco o contrario, entonces son válidos los cuatro, y las proposiciones antecedente y consecuente resultan equivalentes.

En matemática los teoremas se enuncian mediante una implicación cuyo antecedente es la hipótesis y el consecuente la tesis. De acuerdo con lo establecido al analizar los condicionales conjugados, podemos afirmar que establecida la validez del teorema directo, el contrarrecíproco también se cumple, aunque nada podemos asegurar acerca de la validez de los teoremas recíproco y contrario.

Sea el teorema cuyo enunciado es $H \Rightarrow T$ (directo); cuando al negar la tesis se llega a la negación de la hipótesis, esto es, se demuestra el teorema $\sim T \Rightarrow \sim H$ (contrarrecíproco), entonces aquél queda demostrado a causa de la equivalencia de las implicaciones contrarrecíprocas, y se ha utilizado el método de demostración por **reducción al absurdo.**

11. RAZONAMIENTO DEDUCTIVO VÁLIDO

En matemática interesa el tipo de razonamiento deductivo. Llamamos razonamiento al par ordenado $(\{p_i\}; q)$, siendo $\{p_i\}$ un conjunto de proposiciones llamadas **premisas**, y q una proposición llamada **conclusión**, respecto de la cual se afirma que deriva de las premisas.

Un razonamiento es deductivo si y sólo si las premisas son evidencias de la verdad de su conclusión, es decir, si $p_1, p_2, \ldots, p_l$ son todas V, entonces q es V. No tiene sentido decir que un razonamiento es V o F, sino que es válido o no. Un razonamiento deductivo es válido cuando no es posible que las premisas sean V y la conclusión F.

Llamamos regla de inferencia a todo esquema válido de razonamiento independientemente de la interpretación de las proposiciones componentes, es decir: toda regla de inferencia es tautológica. Entonces, un razonamiento deductivo es válido cuando el condicional, cuyo antecedente es la conjunción de las premisas y el consecuente es la conclusión, se convierte en tautológico.

Ejemplos de reglas de inferencia:

a) **Modus ponens**

$$\begin{array}{c} p \\ p \Rightarrow q \\ \hline q \end{array}$$

El esquema anterior es la notación clásica del condicional $[(p \Rightarrow q) \wedge p] \Rightarrow q$, el cual es una tautología, como puede probarse mediante tablas de verdad.

b) **Modus tolens**

$$\begin{array}{c} p \Rightarrow q \\ \sim q \\ \hline \sim p \end{array}$$

Es decir, el condicional $[(p \Rightarrow q) \wedge \sim q] \Rightarrow \sim p$ es una tautología.

c) **Ley del silogismo hipotético**

$$\begin{array}{c} p \Rightarrow q \\ q \Rightarrow r \\ \hline p \Rightarrow r \end{array}$$

Esto significa que $[(p \Rightarrow q) \wedge (q \Rightarrow r)] \Rightarrow (p \Rightarrow r)$ es tautológica.

En cambio el condicional:

$[(p \Rightarrow q) \wedge q] \Rightarrow p$ no es forma válida de razonamiento, ya que la tabla de verdad asociada nos muestra que no es tautológico.

p	q	$p \Rightarrow q$	$(p \Rightarrow q) \wedge q$	$[(p \Rightarrow q) \wedge q] \Rightarrow p$
V	V	V	V	V
V	F	F	F	V
F	V	V	V	F
F	F	V	F	V

12. FUNCIONES PROPOSICIONALES Y CUANTIFICADORES

Toda proposición singular asigna a un sujeto particular una propiedad determinada. Ahora bien: una misma propiedad puede predicarse de todos los individuos o sujetos, y en cada uno de estos casos se obtendrá una proposición. Para esquematizar una situación de este tipo, si P es la propiedad, denotaremos con el símbolo $P(x)$ al conjunto de todas las proposiciones singulares obtenidas al sustituir el sujeto variable x por un individuo, en cuyo caso queda definida una **función proposicional con una variable.** $P(x)$ no es una proposición; en consecuencia carece de sentido decir de una función proposicional que es V o F; pero para cada x particular se convierte en proposición.

A partir de funciones proposicionales es posible obtener proposiciones generales mediante el proceso llamado de **cuantificación.**

a) Sea la función proposicional:

$$P(x) : x \text{ es mortal}$$

consideramos como conjunto de posibles sujetos, el formado por los seres humanos; ocurre entonces que todas las proposiciones particulares que pueden obtenerse, son verdaderas. En tal caso, podemos decir:

Cualquiera que sea x, x es mortal.

O bien:

para todo x, x es mortal.

O si no:

Para todo x, se verifica $P(x)$

Se trata de tres versiones distintas de una misma proposición general, siempre verdadera. En este caso suele utilizarse la notación abreviada:

$$\forall x : P(x) \qquad (1)$$

b) Consideremos ahora la función proposicional:

$P(x)$: algunas personas son virtuosas

el campo existencial es el mismo del ejemplo anterior. P(x) se convierte en proposición V para algunos sujetos y F para los restantes. Podemos decir entonces:

Existe algún x, tal que se verifica $P(x)$

Se tiene así una proposición que simbolizaremos con:

$$\exists x / P(x) \qquad (2)$$

Los símbolos $\forall x$ y $\exists x$, se llaman **cuantificadores universal y existencial afirmativos**, respectivamente, los cuales, al preceder a una función proposicional, engendran proposiciones generales.

Definición

Una función proposicional cuantificada universalmente es V si y sólo si son V todas las proposiciones particulares obtenidas al sustituir la variable por sujetos singulares del campo existencial.

Definición

La cuantificación existencial de una función proposicional es V, si y sólo si alguna proposición particular es V.

Los cuantificadores universal y existencial pueden ser negados. Así, la negación de la proposición universal afirmativa:

"Todos los hombres son mortales"

es la proposición existencial:

"Algún hombre no es mortal".

Es decir, la negación de (1) es:

$$\exists x \,/ \sim P(x) \qquad (3)$$

Análogamente, la negación de un cuantificador existencial se convierte en un cuantificador universal respecto de la función proposicional negada.

Simbólicamente se tiene:

$$\sim[\forall x : P(x)] \iff \exists x \,/ \sim P(x)$$

$$\sim[\exists x \,/\, P(x)] \iff \forall x : \sim P(x)$$

Los cuantificadores simples se generalizan y se aplican a funciones proposicionales con dos o más variables, en cuyo caso se tienen cuantificadores dobles, triples, etc., muy usuales en toda teoría matemática. En este caso se presenta la posibilidad de considerar cuantificadores mixtos. Por ejemplo:

I) La conmutatividad de la adición en todo conjunto numérico se expresa mediante un cuantificador universal doble afirmativo:

$$\forall x\, \forall y \text{ se verifica } x + y = y + x$$

II) La existencia de elemento neutro para una operación de grupo, se establece a través de un cuantificador doble existencial universal:

$$\exists e \,/\, \forall x \text{ se verifica: } x * e = e * x = x$$

siendo $*$ la operación que confiere al conjunto estructura de grupo.

III) En el mismo ejemplo anterior de grupo, la existencia de elemento inverso queda establecida en función de un cuantificador doble universal existencial:

$$\forall x\, \exists x' \,/\, x * x' = x' * x = e$$

con x' denotamos el inverso de x respecto de la ley del grupo.

IV) Como es muy simple verificar, las leyes asociativas y distributivas se simbolizan mediante cuantificadores triples. Así:

$$\forall x\, \forall y\, \forall z \text{ se verifica } (x * y) * z = x * (y * z)$$

EJERCICIOS

1. — *Mediante conectivos lógicos, expresar simbólicamente las siguientes proposiciones compuestas:*

   a) *Leonardo pasa de grado o sale de vacaciones.*
   b) *Leonardo pasa de grado y sale de vacaciones.*
   c) *Si Leonardo pasa de grado, entonces sale de vacaciones.*
   d) *Si Leonardo no pasa de grado, entonces sale de vacaciones.*

2. — *Sea el condicional:*

   $$\text{Si } +1 = -1 \text{ entonces } (+1)^2 = (-1)^2$$

   Enunciar las implicaciones conjugadas y analizar sus valores de V.

3. — *Dadas las proposiciones simples:*

   p: Luis lee
   q: Silvina escucha

   se pide el enunciado y expresión simbólica de las siguientes proposiciones:

   a) *disyunción de la primera con la negación de la segunda.*
   b) *conjunción de sus negaciones.*
   c) *negación de su disyunción.*
   d) *conjunción de sus negaciones.*
   e) *¿Cómo son las proposiciones obtenidas en c) y d)? Tener en cuenta las leyes de De Morgan.*

4. — *Sea el condicional:*

   SI Luis lee, ENTONCES Silvina escucha.

   En los casos en que es V, indicar qué proposición es condición necesaria para la otra; análogamente cuál es condición suficiente.

5. — *Construir la tabla de verdad de la proposición*

   $$(p \Rightarrow q) \Rightarrow (\sim q \Rightarrow \sim p)$$

6. — *Demostrar la ley del silogismo hipotético.*

7. — *Investigar si la proposición*

   $$[(p \wedge q) \Rightarrow p] \Rightarrow \sim q$$

   es una regla de inferencia.

8. — *Demostrar que la negación de un cuantificador doble se obtiene aplicando la ley de la negación de los cuantificadores simples en forma sucesiva.*

9. — *Proponer en forma estrictamente simbólica la definición de límite de una función $f(P)$ cuando $P \rightarrow P_0$*

10. — *Idem, la definición de continuidad de la función $f(P)$ en el punto P_0*

CAPITULO II

Teoría de conjuntos

1. CONJUNTOS: SU DETERMINACIÓN

De la posibilidad intelectual de discernir entre uno o varios objetos, surgen intuitivamente las ideas de unidad y conjunto. Estas nociones, que el hombre adquiere y diferencia desde la primera etapa de su evolución mental, son, sin embargo, imposibles de definir explícitamente, pues todo intento sólo conduce al empleo del mismo concepto, generalmente presentado bajo otro nombre. Así, la palabra conjunto sugiere de inmediato la idea de colección, agregado, agrupamiento, grupo, clase, asociación, etc., lo cual, si bien permite apreciar la vastedad y riqueza del idioma al proporcionar una sinonimia tan extensa, no aclara el alcance y contenido del término.

Se conviene entonces en asignar al concepto **conjunto** el carácter de concepto inicial o primitivo.

Cada objeto, unidad o individuo que forma parte de un conjunto se llama **elemento**.

La vida corriente ofrece numerosos ejemplos de conjuntos y a través de ellos surge que los elementos no tienen que ser necesariamente de la misma naturaleza y que su número puede ser finito o no. Sirvan como ejemplos el conjunto formado por los alumnos de una división, el conjunto de los números divisibles por dos, el conjunto de los puntos de un plano, el conjunto formado por una mesa, un banco y un florero, etc.

Se designan los conjuntos por letras mayúsculas A, B, C, etc., y sus elementos por minúsculas.

Para indicar que un objeto es un elemento de un conjunto C, se utiliza el símbolo $\in$, llamado símbolo de pertenencia y se escribe $a \in C$ (a pertenece a C).

Si un objeto b no forma parte del conjunto se escribe: $b \notin C$ (b no pertenece a C).

Es conveniente destacar que unidad o elemento y conjunto son conceptos relativos, por cuanto todo conjunto puede a su vez considerarse como elemento de otro, y un elemento de un conjunto puede concebirse como conjunto de otros entes que lo compongan.

Así, una palabra es un conjunto de letras, pero a su vez es un elemento del conjunto de palabras de una frase, y ésta, por su parte, es un elemento del conjunto de frases de un discurso.

Los conjuntos que pueden formarse sucesivamente de esta manera constituyen distintos **tipos** u **órdenes** de conjuntos y se dice que a través del proceso indicado se asciende en la **escala de tipos**. Cada conjunto creado a expensas de otros como elementos es de orden superior a éstos.

La relación de pertenencia, al vincular un elemento con un conjunto, permite este ascenso en la escala.

Si un objeto a pertenece a un conjunto C y éste es un elemento de otro conjunto D, a no pertenece necesariamente a D. Por ejemplo: si una biblioteca es un conjunto de libros y un libro es un conjunto de hojas de papel, una de estas hojas no es un elemento del conjunto biblioteca.

Es importante, pues, saber discernir sin ambigüedad si un objeto es o no un elemento del conjunto dado. Esto se consigue una vez fijado un criterio que permita decidir, sin lugar a dudas, si un elemento cualquiera pertenece o no a un conjunto.

Se dice entonces que el conjunto está determinado o definido, debiendo entenderse esta última palabra en el sentido de caracterización o individualización de "un" conjunto y no como fijación del alcance y contenido del concepto genérico de conjunto.

A tal efecto hay dos métodos lógicos que permiten definir o determinar un conjunto: por extensión y por comprensión.

Definición

Un conjunto se define por extensión, cuando se nombran todos los elementos que lo constituyen.

La notación es entonces:

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

Indica que el conjunto C está formado por los elementos encerrados entre las llaves.

Ejemplos

$$A = \{\textit{Pedro}, \textit{Juan}\} \quad ; \quad B = \{1, 3, 5, 7, 9\}$$

Este método es el más usual en la vida corriente, pero sólo es aplicable a conjuntos simples, de un número finito y reducido de elementos. En el dominio de las ciencias y en particular de la matemática, no es apto, no sólo por la imposibilidad de definir de tal manera los conjuntos infinitos, sino también por la necesidad de extender los conceptos a entes abstractos que sólo pueden caracterizarse por medio de propiedades que los distinguen de los demás.

Recordemos que dar una propiedad significa dar un enunciado con una variable que se indica con el símbolo $P(x)$, en el cual x representa la variable, de modo que si dicha variable se sustituye por un objeto a, $P(x)$ se transforma en una proposición $P(a)$, es decir, tiene sentido decir si $P(a)$ es verdadera o falsa.

Ejemplos

$P(x)$ es el enunciado "x es un número par".
Si se reemplaza x por el objeto 4, se tiene la proposición:
"4 es un número par", que es verdadera y que expresa que ser un número par es una propiedad del número 4. Si se reemplazara x por el número 5, la proposición que resulta es falsa y por lo tanto expresa que dicho número no cumple o no posee la propiedad.

Dados entonces una propiedad $P(x)$ y un objeto cualquiera a, sólo caben dos posibilidades: $P(a)$ es verdadera o $P(a)$ es falsa.

Se dice que $P(x)$ define un conjunto C cuando se verifica:

$$a \in C \iff P(a) \text{ es verdadera}$$

o bien

$$a \notin C \iff P(a) \text{ es falsa}$$

Esta manera de definir un conjunto se llama por comprensión.

Definición

Un conjunto se define por comprensión cuando se establece una propiedad relativa a los elementos que lo constituyen, de modo que todo objeto que cumpla dicha propiedad pertenezca al conjunto y recíprocamente.

Se indica el conjunto así definido con la notación:

$$C = \{x \,/\, P(x)\}$$

C es el conjunto cuyos elementos son x, tales que $P(x)$.

Ejemplos

a) *Si $P(x)$ es la propiedad de ser número par, se tiene:*
$A = \{x \,/\, x \text{ es un número par}\}$
b) $B = \{x \,/\, x \text{ es un triángulo equilátero}\}$
c) $C = \{x \,/\, x \text{ es un número racional} \wedge 4 < x < 5\}$

Cualquier propiedad define, pues, un conjunto: el conjunto de los elementos que tienen esa propiedad.

Observación

Cabe destacar, sin embargo, que existen algunas excepciones que escapan al sentido intuitivo del concepto conjunto y de la afirmación anterior y que por esa causa condujeron a comienzos del siglo actual al descubrimiento de las famosas contradicciones o paradojas de la teoría de conjuntos. Sea por ejemplo la propiedad $X \notin X$, es decir, un conjunto que no es elemento de sí mismo y formemos el conjunto A cuyos elementos poseen esa propiedad.

$$A = \{X / X \notin X\}$$

La pregunta que surge de inmediato es: ¿A es o no es elemento de sí mismo? Caben dos respuestas:

Si $A \in A$: A no cumple la propiedad que define a A y por lo tanto

$$A \notin A$$

Si $A \notin A$: A cumple la propiedad y por lo tanto

$$A \in A$$

Es decir, ambas hipótesis conducen a la conclusión inversa o sea a una contradicción.

Hay otra propiedad no menos contradictoria y es la de considerar el conjunto formado por todos los conjuntos existentes. Tal conjunto, por lo tanto, debe contenerse a sí mismo como elemento: esto lleva a considerar el conjunto de todos los conjuntos que no forman parte de sí mismos como el A del ejemplo anterior, lo cual lleva a una contradicción, como se ha visto.

Este descubrimiento condujo a Bertrand Russell a una revisión de las hipótesis de la teoría de conjuntos y a formular su teoría de tipos. Las paradojas citadas provienen justamente de una confusión de tipos y de la concepción de clases impuras, es decir, clases de la naturaleza $A \in A$, en las que la relación de pertenencia no señala una ascensión en la escala de tipos.

2. CONJUNTOS ESPECIALES

I) Conjunto vacío

Si se da una proposición contradictoria, es decir, que sea siempre falsa, se dice que define un conjunto vacío.

$$V = \{x / P(x)\} \text{ es vacío} \Leftrightarrow \forall x,\ P(x) \text{ es falsa.}$$

Ejemplos:

$V = \{x / x \in C \wedge x \notin C\}$

$V = \{x / x \text{ número natural par } \wedge 2 < x < 4\}$

$V = \{x / x \text{ es un polígono convexo de tres lados y cuatro ángulos}\}$

Corolario

Un conjunto vacío carece de elementos.

Es inmediato, pues si la proposición que lo define es contradictoria no existe ningún elemento que la satisfaga.

$$V \text{ es un conjunto vacío} \Leftrightarrow \forall x,\ x \notin V.$$

II) Conjunto unitario

Es el conjunto formado por un solo elemento.

$$U = \{a\}$$

Se lo indica también con la notación

$$\{a\} = \{x \,/\, x = a\}$$

O sea:

$$x \in \{a\} \Leftrightarrow x = a$$

teniendo en cuenta que la expresión $x = a$ significa que x y a son "idénticos" y por lo tanto x y a son dos símbolos que representan un mismo objeto.

Observación

El conjunto $\{a\}$ y el elemento a son conceptos distintos y no deben confundirse. Es claro que

$$a \in \{a\}; \quad \text{pero} \quad a \neq \{a\},$$

pues en caso contrario se llega a que $\{a\} \in \{a\}$, lo cual según se ha visto en la observación de la página anterior, es imposible.

Además, el conjunto $A = \{a, a\}$ sólo tiene un elemento, pues se cumple que $a = a$ y por lo tanto $A = \{x \,/\, x = a\}$. Luego

$$A = \{a, a\} = \{a\}$$

Lo mismo ocurre con el conjunto $A = \{a, a, a\}$, etc.

III) Referencial o conjunto universal

Es el conjunto constituido por todos los elementos que estudia una teoría determinada.

Ejemplos

Para el botánico, el referencial está constituido por todos los seres vegetales existentes.

En la teoría de los números reales, el referencial está formado por todos los números reales.

Suele darse al referencial el nombre de conjunto universal, entendiéndose este concepto como relativo a los elementos que se considere en la teoría y sólo a ellos.

3. RELACIONES ENTRE CONJUNTOS

I) Inclusión

Definición

Se dice que un conjunto A **está incluido en otro conjunto** B**, o que** A **es un subconjunto o parte de** B**, si y sólo si todos los elementos de** A **pertenecen también a** B.

$$A \text{ incluido en } B \Leftrightarrow x \in A \Rightarrow x \in B$$

De acuerdo con esta definición todo conjunto A puede ser considerado como una parte de sí mismo. En efecto:

$$A \text{ incluido en } A, \text{ pues } x \in A \Rightarrow x \in A$$

Cuando la inclusión contempla la posibilidad anterior se dice que es **amplia** y se indica con el símbolo: $\subseteq$

$$A \subseteq B \Leftrightarrow x \in A \Rightarrow X \in B$$

Si existen elementos de B que no pertenecen al conjunto A, se dice que la inclusión es **estricta o propia,** o que A es un subconjunto propio o una parte propia de B. Se indica con el símbolo $\subset$.

$$A \subset B \Leftrightarrow [x \in A \Rightarrow x \in B] \wedge \exists y \,/\, y \in B \wedge y \notin A$$

Ejemplos

$$A = \{x \,/\, x \text{ es número natural par}\} \text{ y } N = \{x \,/\, x \text{ es número natural}\}$$

$$A \subset N$$

$$A = \{x \,/\, x \text{ es un cuadrado}\} \text{ y } B = \{x \,/\, x \text{ es un rectángulo}\}$$

$$A \subset B$$

$$C = \{a, b, c, d, e\} \text{ y } D = \{b, c\}$$

$$D \subset C$$

Las relaciones anteriores pueden expresarse de la siguiente manera: $B \supseteq A$ o $B \supset A$ que se leen: B contiene A o B contiene propiamente A, respectivamente.

Corolario

Si un conjunto es vacío está incluido en cualquier otro conjunto.

V es vacío $\wedge$ A es un conjunto $\Rightarrow V \subseteq A$, puesto que $x \in V \Rightarrow x \in A$ es verdadero, pues $x \in V$ es falso.

II) Igualdad de conjuntos

Definición

Dos conjuntos son iguales cuando contienen los mismos elementos.

Es decir, todo elemento del primero pertenece al segundo y recíprocamente. Se indica:

$$A = B \Leftrightarrow (x \in A \Rightarrow x \in B) \wedge (y \in B \Rightarrow y \in A)$$

O sea

$$A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$$

Observación

La igualdad entre conjuntos debe entenderse, de acuerdo con la definición, como identidad. Es decir $A = B$ significa que A y B son conjuntos "idénticos" y por lo tanto con A y B se representa a un mismo conjunto.

Cuando se cambia la propiedad que define a un conjunto por otra lógicamente equivalente, se obtiene el mismo conjunto; es decir, los dos conjuntos así definidos son iguales.

Si $P(x) \Leftrightarrow Q(x)$

$$A = \{x \,/\, P(x)\} \;\; y \;\; B = \{x \,/\, Q(x)\}$$

Resulta:

$$A = B$$

Ejemplos

$$\left.\begin{array}{l} A = \{x \,/\, x \text{ es un triángulo equiángulo}\} \\ B = \{x \,/\, x \text{ es un triángulo equilátero}\} \end{array}\right\} \Rightarrow A = B$$

Corolario

El conjunto vacío es único.

En efecto, si V y V' son conjuntos vacíos, se verifica:

$V \subseteq V'$ pues $x \in V \Rightarrow x \in V'$ es verdadero, por ser falsos ambos términos de la implicación

Análogamente $V' \subseteq V$. Por lo tanto por definición de conjuntos iguales

$$V = V'$$

Se indica entonces el conjunto vacío por medio de un único símbolo: $\varnothing$ (letra escandinava)

III) Propiedades de la inclusión

a) **Reflexividad:**

Todo conjunto está incluido en sí mismo.

$$\forall A, A \subseteq A$$

b) **Antisimetría:**

$$(A \subseteq B \wedge B \subseteq A) \Rightarrow A = B$$

Se cumple por la definición de igualdad de conjuntos.

c) **Transitividad:**

$$(A \subseteq B \wedge B \subseteq C) \Rightarrow A \subseteq C$$

En efecto: $A \subseteq B \Rightarrow (x \in A \Rightarrow x \in B)$ (1)

$B \subseteq C \Rightarrow (x \in B \Rightarrow x \in C)$ (2)

De (1) y (2): $(x \in A \Rightarrow x \in C) \Rightarrow A \subseteq C$

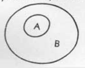
Como se verá más adelante, estas tres propiedades caracterizan a la inclusión entre conjuntos como una relación de orden.

IV) Diagramas de Venn

Como recurso didáctico para facilitar la comprensión de algunos conceptos relativos a la teoría de conjuntos es útil y cómodo el uso de los diagramas de Venn. Consisten en representar los conjuntos por medio de recintos planos cerrados en cuyo interior se ubican los elementos necesarios para la exposición, simbolizados por puntos. Se aclara que este recurso puede usarse para ayudar a la intuición, pero nunca constituye un método de demostración.

La inclusión de conjuntos se representa de la siguiente manera:

$A \subseteq B$



V) Conjunto de las partes o familias de las partes

Definición

Se llama conjunto de las partes de un conjunto E o familia de las partes de E, al conjunto cuyos elementos son todos los subconjuntos de E.

Se indica con la notación: $\mathcal{P}(E)$.

$$\mathcal{P}(E) = \{X / X \subseteq E\} \quad \text{o sea} \quad X \in \mathcal{P}(E) \Leftrightarrow X \subseteq E$$

Si E no es vacío, tiene por lo menos dos subconjuntos distintos, el vacío y E.

$$\varnothing \in \mathcal{P}(E) \quad \text{y} \quad E \in \mathcal{P}(E)$$

Si E es el conjunto unitario U, sólo tiene dos subconjuntos distintos: $\varnothing$ y U.

Luego $\mathcal{P}(U) = \{\varnothing , U\}$ o bien $\mathcal{P}(U) = \{\varnothing , \{u\}\}$

Si E no es vacío ni unitario, además de $\varnothing$ y E, son subconjuntos todos los que se pueden formar a expensas de sus elementos.

Sea $\qquad E = \{a, b, c\}$

$\mathcal{P}(E) = \{\varnothing , \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$

Si E tiene n elementos el número de elementos de $\mathcal{P}(E)$ es igual a 2^n, como puede verificarse a través de los ejemplos. Esta propiedad se demuestra rigurosamente por medio del principio de inducción completa.

De aquí deriva el nombre de **potencial** con que se designa generalmente al conjunto $\mathcal{P}(E)$.

4. OPERACIONES ENTRE CONJUNTOS

Dado un referencial E, sus subconjuntos pueden asociarse o combinarse de distintas maneras, dando lugar a otros subconjuntos de E. Las leyes o criterios fijados a tal efecto constituyen las llamadas operaciones entre conjuntos. En lo que sigue se tendrá en cuenta que los conjuntos que intervienen en cada operación son partes de un mismo referencial.

I) Complementación

Definición

Se llama complemento de un conjunto A **con respecto a un**

referencial E al conjunto $\complement_E A$ formado por los elementos de E que no pertenecen a A.

$$\text{Si} \quad A \subseteq E \text{ es } \complement_E A = \{x \,/\, x \in E \wedge x \notin A\}$$

$$\text{O sea:} \quad x \in \complement_E A \Rightarrow x \in E \wedge x \notin A$$

Cuando no hay ambigüedad respecto al referencial de que se trata puede escribirse abreviadamente:

$$\complement A = \{x \,/\, x \notin A\} \quad \text{o sea:} \quad x \in \complement A \Leftrightarrow x \notin A$$

En lugar de $\complement A$ también son usuales los símbolos A', $\sim A$, $-A$.
La complementación en la teoría conjuntista corresponde a la negación en el cálculo proposicional.

Ejemplos

a) $E = \{a, b, c, d, e\}$ $\quad A = \{a, d, e\}$

$$A' = \{b, c\}$$

b) E = *Conjunto de los números naturales.*
A = *Conjunto de los números naturales que son múltiplos de 2.*
A' = *Conjunto de los números naturales impares.*

Corolario

El complemento del complemento de un conjunto es este conjunto.

$$(A')' = A$$

Es inmediato de acuerdo con la definición anterior.

II) Intersección

Definición

Dados dos conjuntos A y B, se llama intersección de ambos al conjunto cuyos elementos pertenecen simultáneamente a A y a B.

Se indica con la notación $A \cap B$.

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

O sea

$$x \in A \cap B \Leftrightarrow x \in A \wedge x \in B$$

Ejemplos

a) $A = \{a, b, c, d, e\}$ y $B = \{a, c, f, g\}$

$$A \cap B = \{a, c\}$$

b) $A = \{x \,/\, x \text{ es rectángulo}\}$ y $B = \{x \,/\, x \text{ es rombo}\}$

$$A \cap B = \{x \,/\, x \text{ es cuadrado}\}$$

La intersección entre conjuntos corresponde a la conjunción en el cálculo proposicional.

La definición se extiende al caso de más de dos conjuntos.

Definición

Se dice que dos conjuntos A y B son disjuntos si y sólo si su intersección es el conjunto vacío.

$$A \text{ y } B \text{ son disjuntos} \Leftrightarrow A \cap B = \emptyset$$

Ejemplo

Si A es el conjunto de números pares y B el de los impares, entonces

$$A \cap B = \emptyset$$

III) Reunión o unión

Definición

Dados dos conjuntos A y B, se llama reunión o unión de los mismos al conjunto de todos los elementos que pertenecen a A o a B.

Se indica con la notación $A \cup B$.

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

O sea:

$$x \in A \cup B \Leftrightarrow x \in A \vee x \in B$$

Ejemplo

$A = \{a, b, c, d, e\}$ y $B = \{c, d, e, f\}$

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

La unión entre conjuntos corresponde a la disyunción en el cálculo proposicional.

Se extiende la definición al caso de más de dos conjuntos.

IV) Diferencia

Definición

Dados dos conjuntos A y B se llama diferencia entre A y B al conjunto formado por los elementos de A que no pertenecen a B.

Se indica con la notación: $A - B$

$$A - B = \{x \,/\, x \in A \wedge x \notin B\}$$

Ejemplo

$A = \{x \,/ x \textit{ número natural par}\}$ *y* $B = \{x \,/\, x \textit{ es un número primo}\}$

$$A - B = \{x \,/\, x \textit{ número natural par distinto de } 2\}$$

V) Diferencia simétrica

Definición

Dados dos conjuntos A y B se llama diferencia simétrica entre A y B al conjunto formado por los elementos de A que no pertenecen a B o por los elementos de B que no pertenecen a A.

Se indica $A \triangle B$

$$A \triangle B = \{x \,/\, (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\}$$

O sea:

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

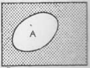
Se observa de inmediato que $A \triangle B = (A - B) \cup (B - A)$

Ejemplo

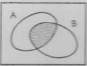
$$E = \{1, 2, 3, 4, 5, 6\} \ , \ A = \{1, 3, 5\} \ y \ B = \{1, 2, 4\}$$

$$A \triangle B = \{2, 3, 4, 5\}$$

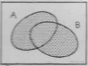
Utilizando los diagramas de Venn, si se representa el referencial E por un rectángulo y los subconjuntos por recintos interiores al mismo, las operaciones anteriores se indican de la siguiente manera:



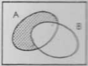
E A'



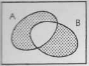
E $A \cap B$



E $A \cup B$



E $A - B$



E $A \triangle B$

5. PROPIEDADES DE LAS OPERACIONES ENTRE CONJUNTOS

Las operaciones entre conjuntos poseen las siguientes propiedades, que guardan estrecha relación con las operaciones análogas del cálculo proposicional, las que intervienen precisamente en las demostraciones de aquéllas.

a) **Conmutatividad de la intersección**

$$A \cap B = B \cap A$$

Corresponde a la conmutatividad de la conjunción lógica:

$$p \wedge q \Leftrightarrow q \wedge p$$

b) **Conmutatividad de la unión**

$$A \cup B = B \cup A$$

Corresponde a la conmutatividad de la disyunción lógica

$$p \vee q \Leftrightarrow q \vee p$$

c) **Asociatividad de la intersección**

$$(A \cap B) \cap C = A \cap (B \cap C)$$

Corresponde a la asociatividad de la conjunción lógica

$$(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$$

d) **Asociatividad de la unión**

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

Corresponde a la asociatividad de la disyunción lógica

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

e) **Distributividad de la unión con respecto a la intersección y viceversa.**

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

Corresponden respectivamente a la distributividad de la disyunción con respecto a la conjunción y de ésta con respecto a la primera.

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

f) **Leyes de De Morgan**

$$(A \cup B)' = A' \cap B'$$
$$(A \cap B)' = A' \cup B'$$

Corresponden a las respectivas leyes de De Morgan relativas a la disyunción y a la conjunción.

$$\sim(p \vee q) \iff \sim p \wedge \sim q$$
$$\sim(p \wedge q) \iff \sim p \vee \sim q$$

Como puede advertirse, la unión y la intersección de conjuntos poseen propiedades análogas. Este paralelismo deja de subsistir si en la composición de unión o de intersección aparecen $\varnothing$, E o el complemento del conjunto dado. En efecto se verifica:

$A \cap \varnothing = \varnothing$	$p \wedge$ contradictoria es contradictoria
$A \cup \varnothing = A$	$p \vee$ contradictoria es p
$A \cap E = A$	$p \wedge$ tautología es p
$A \cup E = E$	$p \vee$ tautología es tautología
$A \cap A' = \varnothing$	$p \wedge \sim p$ es contradictoria
$A \cup A' = E$	$p \vee \sim p$ es tautología

Además

$\varnothing' = E$	la negación de una contradicción es una tautología
$E' = \varnothing$	la negación de una tautología es una contradición

La demostración de las propiedades anteriores es simple y sólo requiere la aplicación de las definiciones relativas a las operaciones de que se trata y de las propiedades del cálculo proposicional.

Además, por tratarse de relaciones de igualdad entre conjuntos, el razonamiento debe hacerse en dos sentidos, es decir, demostrar la implicación a la derecha y a la izquierda.

A título de ejemplo se da la demostración de una de dichas propiedades y se recomiendan las restantes como ejercicio para el lector.

Teorema

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

Se demuestra primero la implicación a la derecha, o sea

$T_1)\quad x \in [A \cup (B \cap C)] \Rightarrow x \in [(A \cup B) \cap (A \cup C)]$

En efecto: $x \in [A \cup (B \cap C)] \Rightarrow x \in A \vee x \in (B \cap C) \Rightarrow$
$\Rightarrow x \in A \vee (x \in B \wedge x \in C) \Rightarrow (x \in A \vee x \in B) \wedge (x \in A \vee x \in C) \Rightarrow$
$\Rightarrow x \in (A \cup B) \wedge x \in (A \cup C) \Rightarrow x \in [(A \cup B) \cap (A \cup C)]$

Implicación a la izquierda, o sea

$T_2)\quad x \in [(A \cup B) \cap (A \cup C)] \Rightarrow x \in [A \cup (B \cap C)]$

Pues $x \in [(A \cup B) \cap (A \cup C)] \Rightarrow x \in (A \cup B) \wedge x \in (A \cup C) \Rightarrow$

$$\Rightarrow (x \in A \vee x \in B) \wedge (x \in A \vee x \in C) \Rightarrow$$
$$\Rightarrow (x \in A \wedge x \in A) \vee (x \in A \wedge x \in C) \vee$$
$$(x \in B \wedge x \in A) \vee (x \in B \wedge x \in C) \Rightarrow$$
$$\Rightarrow x \in A \vee x \in (A \cap C) \vee x \in (A \cap B) \vee x \in (B \cap C) \Rightarrow$$
$$\Rightarrow x \in A \vee x \in (B \cap C) \Rightarrow x \in [A \cup (B \cap C)]$$

o. CUPLA O PAR ORDENADO

Definición

> **Dados dos subconjuntos A y B de un referencial, se llama cupla o par ordenado al ente (a ; b) formado por un elemento de A y un elemento de B, en ese orden.**

O sea a expensas de dos objetos a y b pertenecientes respectivamente a los conjuntos A y B se obtiene un tercer objeto c que se indica (a ; b), conceptualmente distinto de los elementos a y b considerados individualmente, que se toman para definirlo. En particular, puede ser A = B.

Ejemplo

Si A y B son dos subconjuntos del conjunto de los números reales y se considera el plano referido a un sistema de ejes cartesianos, cada punto del plano de abscisa $x \in A$ y ordenada $y \in B$ es una cupla $(x ; y)$. Aquí se advierte la importancia del orden en que se enuncian los elementos, pues $P = (x ; y)$ es en general distinto de $P' = (y ; x)$.

Axioma de igualdad

Si el ente c **es el par ordenado** (a ; b) **y el** c' **el par ordenado** (a' ; b'), **entonces** $c = c' \Leftrightarrow a = a' \wedge b = b'$

O sea $(a ; b) = (a' ; b') \Leftrightarrow a = a' \wedge b' = b'$

El axioma precedente permite introducir el concepto de componentes de un par ordenado. En efecto: dado el par ordenado z, existen por lo menos dos objetos x e y tales que $z = (x ; y)$. Dichos objetos satisfacen la propiedad de constituir una cupla; es decir, se tiene una propiedad con dos variables x e y. En virtud del axioma de igualdad, todos los objetos tales que al reemplazar la variable x por uno de ellos satisfacen la propiedad constituyen un conjunto unitario, o sea existe un solo objeto x que la verifica.

Análogamente, dado $z = (x ; y)$ existe un único objeto y que satisface la propiedad de pertenecer al par ordenado. Luego, tiene sentido la siguiente:

Definición

Dado el par ordenado $z = (x ; y)$, **se llama primera proyección o primera componente de** z **al elemento** x **y se llama segunda proyección o segunda componente de** z **al elemento** y.

$$x = pr_1(z) \quad ; \quad y = pr_2(z)$$

Los conceptos precedentes se extienden permitiendo la creación de nuevos entes a expensas de tres o más objetos.

Definición

Dados tres subconjuntos A, B y C **de un mismo referencial, se llama tripla, triplete o terna ordenada al objeto** u **formado por un elemento de** A, **uno de** B **y uno de** C **en ese orden.**

$$u = (a; b; c) \;/\; (a; b; c) = [(a; b); c]$$

Corolario

La condición necesaria y suficiente para que dos ternas sean iguales es que lo sean sus respectivas componentes.

Si $u = [(a; b); c]$ y $u' = [(a'; b'); c']$ y $u = u'$

debe ser por el axioma de igualdad:

$$(a ; b) = (a' ; b') \quad \text{y} \quad c = c', \text{ o sea:}$$

$$a = a' \ , \ b = b' \ \text{y} \ c = c'$$

Definición

Dados n **subconjuntos** A, B, . . . , N **de un referencial, se llama n-upla al objeto** u **formado por un elemento de** A, **uno de** B, **etc., uno de** N, **en ese orden.**

$u = (a; b; c; \ldots ; n)$ o $u = \{[(a; b); c]; d ; \ldots ; n\}$

7. PRODUCTO CARTESIANO

Definición

Dados dos conjuntos A **y** B, **se llama producto cartesiano al conjunto cuyos elementos son todas las cuplas cuya primera componente pertenece a** A **y la segunda a** B.

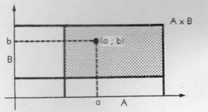
$$A \times B = \{(a ; b) \, / \, a \in A \wedge b \in B\}$$

Ejemplos

a) $A = \{a, a', a''\}$ y $B = \{b, b'\}$

$A \times B = \{(a ; b), (a ; b'), (a' ; b), (a' , b'), (a'' ; b), (a'' ; b')\}$

b)



Si $A = B$, el producto cartesiano $A \times A$ se suele indicar A^2. Este conjunto contiene en particular los elementos $(x; x)$ siendo $x \in A$.

Definición

Se llama diagonal del producto cartesiano $A \times A$ al subconjunto formado por las cuplas del tipo $(x; x)$.

Observación

El producto cartesiano no es, en general, conmutativo. Es decir, $A \times B$ es distinto de $B \times A$, pues según se ha visto, la cupla $(a ; b)$ no es igual a la $(b; a)$.

La definición de producto cartesiano se extiende al caso de varios conjuntos.

Definición

Dados n conjuntos $A, B, \ldots, N$, se llama producto cartesiano de dichos conjuntos al conjunto P, cuyos elementos son las n-uplas formadas con elementos respectivamente pertenecientes a cada uno de los conjuntos dados.

$$P = A \times B \times C \times \ldots\ldots \times N \Leftrightarrow$$

$$\Leftrightarrow P = \{(a ; b ; c ; \ldots\ldots ; n) / a \in A \wedge b \in B \wedge \ldots\ldots \wedge n \in N\}.$$

EJERCICIOS

1. — *Sean dos conjuntos X e Y. Demostrar que* $X \subset Y \Leftrightarrow P(X) \subset P(Y)$.

2. — *Demostrar las siguientes propiedades enunciadas en el texto:*
   a) *Conmutatividad y asociatividad de la intersección de conjuntos.*
   b) *Conmutatividad y asociatividad de la unión de conjuntos.*
   c) *Distributividad de la intersección con respecto a la unión.*
   d) *Leyes de De Morgan.*

3. — *Si* Z^{+} *es el conjunto de los enteros positivos y se consideran los subconjuntos* $A = \{x \,/\, x \text{ múltiplo de } 2\}$
   y $B = \{x \,/\, x \text{ múltiplo de } 3\}$
   Caracterizar los conjuntos siguientes:

   a) $A \cap B$ b) $\complement A$ c) $\complement (A \cup B)$ d) $\complement A \cap \complement B$

4. — *Demostrar que:*
   a) $A \subset B \wedge A \subset C \Leftrightarrow A \subset (B \cap C)$
   b) $A \subset B \Leftrightarrow A \cap B = A$
   c) $A \subset B \wedge C \subset B \Leftrightarrow (A \cup C) \subset B$
   d) $A \subset B \Leftrightarrow A \cup B = B$

5. — *Demostrar las siguientes identidades entre conjuntos:*
   a) $(A - B) \cap B = \varnothing$
   b) $A \cup (B - A) = A \cup B$
   c) $A - B = A - (A \cap B) = (A \cup B) - B$
   d) $A \triangle B = (A \cup B) - (A \cap B)$

6. — *Hallar el resultado de:*
   a) $(A \cup B) \cup [\complement A \cap \complement B]$
   b) $(A \cup B) \cap [\complement A \cap \complement B]$
   c) $[(A \cap B) - A] \cup [B - (A \cap B)]$
   d) $[(A - B) \cup A] \cap [(\varnothing \cup A) \cup B]$

7. — *Si A y B son dos conjuntos, demostrar que:*

$$A \times B = \varnothing \Leftrightarrow A = \varnothing \vee B = \varnothing$$

8. — *Si A, B, X e Y son conjuntos demostrar que:*

$$(A \subseteq X \wedge B \subseteq Y) \Rightarrow A \times B \subset X \times Y$$

La recíproca, ¿es siempre cierta? Utilizar en la discusión la conclusión del ejercicio anterior.

CAPITULO III

Relaciones

La idea de establecer una relación entre dos o más objetos es utilizada frecuentemente en matemática y en la vida cotidiana. Es común determinar relaciones mediante frases como "es padre de", "admira a", "está por encima de", "es más fino que", "es del mismo color que". En geometría elemental se emplean continuamente las expresiones "es semejante a", "es congruente con", "es paralela a", "es perpendicular a", y en aritmética "es mayor que", "es igual a", "es múltiplo de", etc.

Las relaciones, como las operaciones, se clasifican de acuerdo con el número de elementos que intervienen. Si una relación vincula dos elementos se llama "binaria", si vincula tres "ternaria", etc.

En general, las relaciones más comunes son las binarias, como lo indican los ejemplos anteriores. Sin embargo, expresiones como "A está entre B y C", "R es colineal con M y N", "s es la suma de a y b" pertenecen a relaciones ternarias, también usuales en matemática.

1. RELACIÓN BINARIA

Sea A el conjunto de escritores y B el conjunto de sus obras teatrales.

Si se considera la propiedad "es autor de" y se vincula, a través de ella, un ser humano a, con una obra de teatro b, entonces la proposición "a es autor de b" puede ser falsa o verdadera.

Es decir, la propiedad $p(x\,;\,y)$ = "x es autor de y" es una función proposicional de dos variables.

En particular

$$p(\textit{Cané}\,;\,\textit{Juvenilia}) = \textit{Cané es autor de Juvenilia}$$
$$y\ p(\textit{Sáenz}\,;\,\textit{Romeo y Julieta}) = \textit{Sáenz es autor de Romeo y Julieta}$$

son dos proposiciones que vinculan elementos de los conjuntos dados, la primera verdadera y la segunda falsa.

El par (Cané; Juvenilia) está **relacionado** por la propiedad exigida, o bien, Cané está en la **relación p** con Juvenilia.

Se seleccionan así, entre todos los pares ordenados posibles, aquellos pares que verifican la relación indicada. Es decir, ha quedado definido, por comprensión, el conjunto de cuplas de autores y sus respectivas obras teatrales.

Ahora bien, esta selección de pares ordenados entre elementos de dos conjuntos puede ser totalmente arbitraria.

Por ejemplo, si se desea vincular cada vocal con un color, puede definirse, simplemente por extensión, el siguiente conjunto:

$$\{(a\,;\,blanco)\,,\,(e\,;\,rojo)\,,\,(i\,;\,verde)\,,\,(o\,;\,azul)\,,\,(u\,;\,rojo)\}$$

y la relación establecida entre vocales y colores no corresponde a ninguna propiedad característica.

Resulta lógico entonces, definir una relación binaria como un conjunto de cuplas o pares ordenados.

Definición

$\mathcal{R}$ es una relación binaria entre elementos de los conjuntos A y B si y sólo si es un subconjunto del producto cartesiano $A \times B$.

Esto es, $\mathcal{R} \subseteq A \times B$

Es usual designar al conjunto A conjunto de partida y al B conjunto de llegada.

Dada la relación $\mathcal{R}$, si el par ordenado $(a\,;\,b) \in \mathcal{R}$, se dice que "a está en la relación $\mathcal{R}$ respecto de b" y se indica $a\,\mathcal{R}\,b$.

Si A es un conjunto de m elementos y B un conjunto de n elementos, el conjunto $A \times B$ tiene $m \cdot n$ elementos. Existen, por lo tanto, 2^{mn} subconjuntos de $A \times B$, o sea, 2^{mn} posibles relaciones entre los elementos de ambos conjuntos.

Si los conjuntos A y B son iguales, entonces $\mathcal{R}$ es una relación entre los elementos del conjunto A o simplemente $\mathcal{R}$ es una relación en A.

Como ya se ha visto, una relación entre conjuntos puede determinarse mediante una propiedad o regla de correspondencia, o indicando el conjunto de pares que le pertenecen.

Ejemplos

a) *Sea* $A = \{0, 1, 2\}$ *Se define* $(a\,;\,b) \in \mathcal{R} \Leftrightarrow b > a - 1$

Entonces se tiene

$\mathcal{R} = \{(0\,;0)\,,\,(0\,;1)\,,\,(0\,;2)\,,\,(1\,;1)\,,\,(1\,;2)\,,\,(2\,;2)\}$

b) Si $N = \{1, 2, 3, 4, 5\}$ y $(a;b) \in \varrho \iff a + b = 4$ resulta
$\varrho = \{(1;3), (3;1), (2;2)\}$

c) Si $H = \{x / x$ número par$\}$ entonces
$\mathcal{G} = \{(4;10), (2;-6), (4;4)\}$ es una relación definida en H pues $\mathcal{G} \subseteq H^2$

d) Sea $T = \{x / x$ triángulo en el plano euclídeo$\}$.
Se define $(a;b) \in \mathcal{R} \iff a \cong b$ en cuyo caso se tiene una relación en T.

e) Con $S = \{n / n$ ser humano$\}$ y definiendo $(a;b) \in \varrho \iff a$ "es hermano de" b
resulta $\varrho \subseteq S^2$ y por consiguiente ϱ es una relación en S.

Dominio o primera proyección

Definición

Dados dos conjuntos A y B y una relación $\mathcal{R}$ entre sus elementos, el conjunto $D(\mathcal{R})$ es el dominio de la relación si y sólo si está formado por todos los elementos de A que son primeras componentes de las cuplas de $\mathcal{R}$.

Es decir, $x \in D(\mathcal{R}) \iff x \in A \wedge \exists y \in B / (x;y) \in \mathcal{R}$

Recorrido o segunda proyección

Definición

Dados dos conjuntos A y B y una relación $\mathcal{R}$ entre sus elementos, el conjunto $R(\mathcal{R})$ es el recorrido de la relación si y sólo si está formado por todos los elementos de B que son segundas componentes de las cuplas de $\mathcal{R}$.

$$y \in R(\mathcal{R}) \iff y \in B \wedge \exists x \in A / (x;y) \in \mathcal{R}$$

Si $(x;y) \in \mathcal{R}$ se dice que y es imagen de x a través de $\mathcal{R}$.
El recorrido de una función suele denominarse también rango o contradominio.

Ejemplos

a) $A = \{x / x$ número real$\}$
$\mathcal{R} = \{(x;y) / y = \sqrt{x^2}\}$ Aclaración: $\sqrt{x^2} = |x|$

El dominio de la relación es el conjunto de los números reales, mientras que su recorrido es el conjunto de los números reales no negativos.

b) $N = \{a \,/\, a \text{ número natural} \wedge a > 1\}$

$$(a;b) \in \varrho \Leftrightarrow \exists c \in N \,/\, b = a \cdot c$$

El dominio de la relación es el mismo conjunto N, mientras que su recorrido es el conjunto de los números no primos.

En este ejemplo, la relación $a \varrho b$ se lee "a divide a b" o "a es divisor de b" o "b es múltiplo de a" o "b es divisible por a" y se indica $a \mid b$.

Relación inversa

Definición

Si $\mathcal{R}$ es una relación definida en un conjunto A, se llama relación inversa de $\mathcal{R}$ al conjunto $\mathcal{R}^{-1} = \{(y;x) \,/\, (x;y) \in \mathcal{R}\}$

Ejemplos

a) Si $A = \{0, 1, 2\}$ y $\mathcal{R} = \{(0;2), (1;0), (2;1)\}$,
entonces $\mathcal{R}^{-1} = \{(2;0), (0;1), (1;2)\}$

b) Si $A = \{1, 2, 3, 4\}$ y $\mathcal{R} = \{(1;3), (3;1), (2;2)\}$,
entonces $\mathcal{R}^{-1} = \mathcal{R}$

Representación gráfica

Una idea fundamental en geometría analítica es la correspondencia que se establece entre cuplas de números reales y puntos de un plano. Es decir, a cada punto del plano le corresponde un único elemento del producto cartesiano $R \times R$ y a cada elemento de $R \times R$ le corresponde un único punto del plano.

Esta idea se puede extender a cualquier conjunto de cuplas, haciéndole corresponder biunívocamente a cada cupla un punto del plano cartesiano.

Por lo tanto, dada una relación $\mathcal{R}$, si sobre el eje de abscisas se consideran los elementos del conjunto de partida y sobre el eje de ordenadas los del conjunto de llegada, queda formada una cuadrícula donde se pueden señalar los vértices que corresponden a pares ordenados de $\mathcal{R}$.

Ejemplo

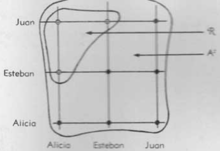
Sea $A = \{$*Juan, Alicia, Esteban*$\}$

Se define $x \mathcal{R} y \Leftrightarrow$ *inicial de* x *"es anterior a" inicial de* y

Resulta

$\mathcal{R} = \{$(*Alicia* ; *Esteban*), (*Alicia* ; *Juan*), (*Esteban* ; *Juan*)$\}$

Gráficamente:



2. RELACIÓN N-ARIA

Se puede generalizar la definición de relación binaria considerando, en lugar de pares ordenados, ternas ordenadas, cuaternas ordenadas, etc.

Definición

> $\mathcal{R}$ **es una relación n-aria entre n conjuntos** A, B, C, D, ... , N **(para** $n \geqslant 2$) **si y sólo si** $\mathcal{R}$ **es un subconjunto cualquiera del producto** $A \times B \times C \times \ldots\ldots \times N$.

Ejemplo

$A = \{0, 1, 2, 3, 4\}$

$\mathcal{R} = \{(0 ; 1 ; 2), (1 ; 3 ; 4), (0 ; 2 ; 1)\}$

$\mathcal{R}$ es una relación ternaria definida en A.

3. PROPIEDADES DE LAS RELACIONES BINARIAS

Una relación binaria $\mathcal{R}$ entre elementos de un conjunto A puede ser

1) **reflexiva:** $\forall x\colon\ x \in A \Rightarrow (x ; x) \in \mathcal{R}$
2) **no-reflexiva:** $\exists x \,/\, x \in A \wedge (x ; x) \notin \mathcal{R}$
3) **a-reflexiva:** $\forall x\colon\ x \in A \Rightarrow (x ; x) \notin \mathcal{R}$

La propiedad 2 es la negación de la propiedad reflexiva.

En el caso 3 ninguna cupla con elementos iguales pertenece a la relación.

4) **simétrica:** $(a\,;b) \in \mathcal{R} \Rightarrow (b\,;a) \in \mathcal{R}$

5) **no-simétrica:** $\exists (a\,;b) \in \mathcal{R} \,/\, (b\,;a) \notin \mathcal{R}$

6) **a-simétrica:** $(a\,;b) \in \mathcal{R} \Rightarrow (b\,;a) \notin \mathcal{R}$

7) **anti-simétrica:** $[(a\,;b) \in \mathcal{R} \wedge (b\,;a) \in \mathcal{R}] \Rightarrow a = b$

8) **transitiva:** $[(a\,;b) \in \mathcal{R} \wedge (b\,;c) \in \mathcal{R}] \Rightarrow (a\,;c) \in \mathcal{R}$

9) **no-transitiva:** $\exists (a\,;b) \in \mathcal{R} \wedge \exists (b\,;c) \in \mathcal{R} \,/\, (a\,;c) \notin \mathcal{R}$

10) **a-transitiva:** $[(a\,;b) \in \mathcal{R} \wedge (b\,;c) \in \mathcal{R}] \Rightarrow (a\,;c) \notin \mathcal{R}$

11) **lineal o conexa:** $[a \in A \wedge b \in A \wedge a \neq b] \Rightarrow [(a\,;b) \in \mathcal{R} \veebar (b\,;a) \in \mathcal{R}]$

Ley de tricotomía: $\forall a \in A,\ \forall b \in A:\ a\,\mathcal{R}\,b \veebar b\,\mathcal{R}\,a \veebar a = b$

Ejemplos

a) Sea $A = \{a, b, c, d, e\}$ *y* $\mathcal{R} = \{(a\,;b), (c\,;c), (d\,;e)\}$

$\mathcal{R}$ *es* no-reflexiva *pues* $(c\,;c) \in \mathcal{R}$, *pero* $(a\,;a) \notin \mathcal{R}, (b\,;b) \notin \mathcal{R}$, *etc.*

$\mathcal{R}$ *es* no-simétrica *pues* $(c\,;c) \in \mathcal{R} \Rightarrow (c\,;c) \in \mathcal{R}$, *pero* $(a\,;b) \in \mathcal{R} \wedge (b\,;a) \notin \mathcal{R}$ *y* $(d\,;e) \in \mathcal{R} \wedge (e\,;d) \notin \mathcal{R}$.

$\mathcal{R}$ *es* transitiva *pues no hay pares de elementos que verifiquen el antecedente de la implicación de transitividad; por lo tanto, al ser falso el antecedente, la implicación es verdadera. En estos casos se dice que la propiedad se satisface* trivialmente.

$\mathcal{R}$ no es lineal *pues* $a \neq c \wedge (a\,;c) \notin \mathcal{R} \wedge (c\,;a) \notin \mathcal{R}$, etc.

b) Si $N = \{0, 1, 2\}$ *y* $\mathcal{R} = \{(0\,;0), (1\,;1), (2\,;2)\}$

$\mathcal{R}$ *es* reflexiva *pues* $(0\,;0) \in \mathcal{R}, (1\,;1) \in \mathcal{R}$ *y* $(2\,;2) \in \mathcal{R}$

$\mathcal{R}$ *es* simétrica *pues*
$$(0\,;0) \in \mathcal{R} \Rightarrow (0\,;0) \in \mathcal{R}$$
$$(1\,;1) \in \mathcal{R} \Rightarrow (1\,;1) \in \mathcal{R}$$
$$(2\,;2) \in \mathcal{R} \Rightarrow (2\,;2) \in \mathcal{R}$$

$\mathcal{R}$ *es* transitiva trivialmente.

TIPOS DE RELACIONES

Las relaciones binarias definidas en un conjunto pueden cumplir o no las propiedades anteriores. Las relaciones más usuales en matemática son:

a) relaciones de equivalencia

b) relaciones de orden

c) relaciones funcionales o aplicaciones

4. RELACIONES DE EQUIVALENCIA

Definición

Una relación binaria $\mathcal{R}$ en un conjunto A es de equivalencia si y sólo si es reflexiva, simétrica y transitiva.

O sea, una relación binaria $\mathcal{R}$ (simbolizada ~) en un conjunto A es una relación de equivalencia si y sólo si posee los siguientes propiedades:

$$E_1 : a \in A \Rightarrow a \sim a$$
$$E_2 : a \sim b \Rightarrow b \sim a$$
$$E_3 : [a \sim b \wedge b \sim c] \Rightarrow a \sim c$$

Ejemplos

a) *La relación de "congruencia módulo n" para n número natural, definida en el conjunto de los números enteros, es una relación de equivalencia.*

Sea Z el conjunto de los enteros y $a \equiv b_{(3)} \Leftrightarrow a - b = 3q$ *con* $q \in Z$

$E_1 : \forall a \in Z,\ a - a = 0 \Rightarrow a \equiv a_{(3)}$

$E_2 : \forall a \in Z, \forall b \in Z,\ a - b = 3q \Rightarrow b - a = 3(-q)$

o sea $a \equiv b_{(3)} \Rightarrow b \equiv a_{(3)}$

$E_3 : \forall a \in Z,\ \forall b \in Z, \forall c \in Z,\ [a - b = 3q \wedge b - c = 3q'] \Rightarrow$

$\Rightarrow a - c = 3(q + q') = 3k$

o sea $[a \equiv b_{(3)} \wedge b \equiv c_{(3)}] \Rightarrow a \equiv c_{(3)}$

b) *Otras relaciones de equivalencia:*

$A = \{a \,/\, a$ *número natural*$\}$ *y* $\mathcal{R}$: *"idéntico a"*
$B = \{b \,/\, b$ *círculo en el plano euclídeo*$\}$ *y* $\mathcal{R}$: *"tiene igual radio que"*
$C = \{c \,/\, c$ *triángulo en el plano euclídeo*$\}$ *y* $\mathcal{R}$: *"tiene igual área que"*
$D = \{p \,/\, p$ *es una proposición*$\}$ *y* $\mathcal{R}$: *"si y sólo si"*

Clases de equivalencia y conjunto cociente

Ya se ha probado que la relación de congruencia módulo n, definida sobre el conjunto Z de los enteros, es una relación de equivalencia.

Si se considera en especial la congruencia módulo 3, esta relación separa a los números enteros en tres clases no vacíos y disjuntas:

$$Z_0 = \{\ldots, -9, -6, -3, 0, 3, 6, \ldots\}$$
$$Z_1 = \{\ldots, -8, -5, -2, 1, 4, 7, \ldots\}$$
$$Z_2 = \{\ldots, -7, -4, -1, 2, 5, 8, \ldots\}$$

Se observa que cada número entero pertenece a uno y sólo uno de estos subconjuntos de Z y que la unión de Z_0, Z_1 y Z_2 es el conjunto Z.

Más aún, Z_0 puede ser caracterizado como el conjunto de todos los números enteros equivalentes a 0 (o a cualquier otro elemento de Z_0) y similarmente Z_1 y Z_2.

Los conjuntos Z_0, Z_1 y Z_2 se llaman clases de equivalencia determinadas por la congruencia módulo 3 sobre Z.

El conjunto formado por estas tres clases de equivalencia es el conjunto cociente de Z sobre la congruencia módulo 3, y se indica $Z/\equiv$.

O sea,

$$Z/\equiv \; = \{Z_0 \, , \; Z_1 \, , \; Z_2\}$$

Por lo tanto, toda relación de equivalencia $\mathcal{R}$, definida en un conjunto A, separa a los elementos de A en subconjuntos no vacíos y disjuntos dos a dos, llamados clases de equivalencia, según la siguiente:

Definición

Si A es un conjunto, $\sim$ una relación de equivalencia definida en A y a un elemento cualquiera de A, entonces C_a es una clase de equivalencia en A, respecto de la relación $\sim$, si y sólo si C_a es el subconjunto de A formado por todos los elementos de A equivalentes al elemento a.

$$C_a = \{x \, / \, x \in A \wedge x \sim a\}$$

El conjunto de todas las clases de equivalencia correspondientes a una relación $\sim$ es el conjunto cociente, de acuerdo con la siguiente:

Definición

$A/\sim$ es el conjunto cociente del conjunto A sobre la relación de equivalencia definida en A, si y sólo si es el conjunto de todas las clases de equivalencia determinadas sobre A por dicha relación.

Pueden considerarse ahora algunas propiedades de las clases de equivalencia definidas en un conjunto A.

Lema 1

Si un elemento b pertenece a una clase de equivalencia C_a, entonces $C_a = C_b$. O sea, $b \in C_a \Rightarrow C_a = C_b$

Demostración:

para probar la igualdad de conjuntos indicada en la tesis, deberá probarse 1º) $C_b \subseteq C_a$ y 2º) $C_a \subseteq C_b$

1º) $\quad x \in C_b \Rightarrow x \sim b$ por definición de clase de equivalencia

$b \in C_a \Rightarrow b \sim a$ por hipótesis y definición de C_a

$(x \sim b \wedge b \sim a) \Rightarrow x \sim a$ por transitividad

$x \sim a \Rightarrow x \in C_a$ por definición de C_a

luego, $(x \in C_b \Rightarrow x \in C_a) \Leftrightarrow C_b \subseteq C_a$ (1) por definición de inclusión

2º) $\quad x \in C_a \Rightarrow x \sim a$ por definición de C_a

$b \in C_a \Rightarrow b \sim a$ por hipótesis y definición de C_a

$b \sim a \Rightarrow a \sim b$ por simetría

$(x \sim a \wedge a \sim b) \Rightarrow x \sim b$ por transitividad

luego, $(x \in C_a \Rightarrow x \in C_b) \Leftrightarrow C_a \subseteq C_b$ (2) por def. de inclusión

De (1) y (2) : $C_a = C_b$

Lema 2

Dos elementos son equivalentes si y sólo si pertenecen a la misma clase de equivalencia. O sea, $a \sim b \Leftrightarrow C_a = C_b$

1º parte: $\quad a \sim b \Rightarrow C_a = C_b$

Demostración:

1º) $\quad x \in C_a \Rightarrow x \sim a$ por definición de C_a

$[(x \sim a) \wedge (a \sim b)] \Rightarrow x \sim b$ por transitividad

$x \sim b \Rightarrow x \in C_b$ por definición de C_b

o sea, $C_a \subseteq C_b$ (1)

2º) $\quad x \in C_b \Rightarrow x \sim b$ por definición de C_b

por hip. $a \sim b \Rightarrow b \sim a$ por simetría

$[(x \sim b) \wedge (b \sim a)] \Rightarrow x \sim a$ por transitividad

$x \sim a \Rightarrow x \in C_a$ por definición de C_a

o sea, $C_b \subseteq C_a$ (2)

De (1) y (2) : $C_a = C_b$

2º parte: $\quad C_a = C_b \Rightarrow a \sim b$

Demostración:

$C_a = C_b \Leftrightarrow (x \in C_a \Leftrightarrow x \in C_b)$

luego, $a \in C_a \Rightarrow a \in C_b$

$a \in C_b \Rightarrow a \sim b$

Lema 3

Si dos clases de equivalencia tienen un elemento común, entonces dichas clases son idénticas. O sea,

$C_a \cap C_b \neq \varnothing \Rightarrow C_a = C_b$

Demostración:

$C_a \cap C_b \neq \varnothing \Rightarrow [\exists x / x \in C_a \wedge x \in C_b]$ por definición de intersección y de $\varnothing$

$x \in C_a \Rightarrow x \sim a$ por definición de C_a

$x \in C_b \Rightarrow x \sim b$ por definición de C_b

$[(x \sim a) \wedge (x \sim b)] \Rightarrow a \sim b$ por simetría y transitividad

$a \sim b \Rightarrow C_a = C_b$ por lema 2.

Lema 4

Si dos clases de equivalencia C_a y C_b son disjuntas, entonces el elemento a no es equivalente al elemento b. Esto es

$C_a \cap C_b = \varnothing \Rightarrow a \nsim b$

Lema 5

Si dos elementos pertenecen a clases diferentes, entonces dichos elementos no son equivalentes. Esto es,

$(x \in C_a \wedge y \in C_b \wedge C_a \neq C_b) \Rightarrow x \nsim y$

PARTICIÓN DE UN CONJUNTO

La serie de lemas anteriores permite demostrar, según ya se ha indicado, que toda relación de equivalencia definida en un conjunto separa a sus elementos, de manera única, en clases no vacías y disjuntas dos a dos, es decir, establece una partición del conjunto dado.

Definición

Un conjunto $\{A_1, A_2, A_3, A_4, \ldots\ldots\}$ de subconjuntos no vacíos de un conjunto A es una partición de A si y sólo si:

1) A es la unión de $A_1, A_2, A_3 \ldots\ldots$ Es decir, $A = \bigcup A_i$

2) la intersección de dos subconjuntos distintos es el conjunto vacío.

Además, toda partición de un conjunto define sobre el mismo una relación de equivalencia.

Se llega así, al siguiente enunciado, básico en el estudio de relaciones de equivalencia:

Teorema fundamental

$\mathcal{R}$ es una relación de equivalencia en el conjunto A si y sólo si determina una partición de A.

1) Si $\sim$ es una relación de equivalencia en A, entonces determina una partición de A.

De acuerdo con la definición de partición de un conjunto, se debe probar 1º) que cada clase de equivalencia es no vacía y la unión de todas es el conjunto A y 2º) que la intersección de dos clases distintas cualesquiera es vacía.

Demostración:

1º) $x \in A \Rightarrow x \sim x$ por reflexividad

$x \sim x \Rightarrow \exists C_x / x \in C_x$ por definición de C_x

$x \in C_x \Rightarrow C_x \neq \varnothing$ por definición de $\varnothing$

Además, como $\forall x : \exists C_x$, la unión es el conjunto A.

2º) contrarrecíproco del lema 3.

2) Si existe una partición de A, entonces queda definida una relación de equivalencia en A.

Demostración:

Se define en A la siguiente relación: dos elementos de A están en la relación "$\sim$" si y sólo si pertenecen a un mismo subconjunto de la partición.

O sea, $a \sim b \Leftrightarrow [\exists C_x / a \in C_x \wedge b \in C_x]$

Se puede probar que "$\sim$" es una relación de equivalencia.

En efecto, es

1) **reflexiva**

$C_a \neq \varnothing$ por def. de partición

$C_a \neq \varnothing \Rightarrow \exists a \in C_a$ por definición de $\varnothing$

$a \in C_a \Rightarrow a \sim a$ definición de $\sim$

2) **simétrica**

$a \sim b \Rightarrow (a \in C_x \wedge b \in C_x)$ por definición de $\sim$

$\Rightarrow (b \in C_x \wedge a \in C_x)$ por conmutatividad de la conjunción

$\Rightarrow b \sim a$ por definición de $\sim$

3) **transitiva**

si $a \sim b$ y $b \sim c$, por definición de $\sim$ en A existen subconjuntos C_x y C_y de A, no necesariamente distintos, tales que:

$$(a \in C_x \wedge b \in C_x) \wedge (b \in C_y \wedge c \in C_y)$$

pero $(b \in C_x \wedge b \in C_y) \Rightarrow b \in (C_x \cap C_y)$ por definición de $\cap$

$\Rightarrow C_x \cap C_y \neq \varnothing$ por definición de $\varnothing$

$\Rightarrow C_x = C_y$ por definición de partición

Por lo tanto $(a \in C_x \wedge c \in C_x) \Rightarrow a \sim c$

Definición por abstracción

Cada relación de equivalencia en un conjunto permite definir por abstracción un nuevo concepto.

Ejemplos

a) Si se considera el conjunto formado por todos los pares ordenados de números naturales, se puede definir una relación de la siguiente manera:

$$(a ; b) \sim (c ; d) \Leftrightarrow a + d = b + c \quad (*)$$

y se prueba fácilmente que es una relación de equivalencia.

Esta relación establece una partición en el conjunto de cuplas de números naturales. Cada clase de equivalencia está formada por todos los pares equivalentes entre sí, según la relación establecida. Cada una de estas clases se llama número entero y cualquiera de sus elementos puede representarla.

O sea, definición por abstracción:

Si $N \times N$ es el conjunto de cuplas de números naturales y $\sim$ la relación de equivalencia definida en (*), número entero $(a ; b)$ es la clase de equivalencia

$$(a ; b) = C_{(a;b)} = \{(x ; y) \,/\, (x ; y) \in (N \times N) \vee (x ; y) \sim (a ; b)\}$$

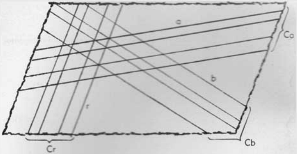
Por ejemplo,

$$(5 ; 3) = C_{(5;3)} = \{(x ; y) \,/\, (x ; y) \in (N \times N) \vee (x ; y) \sim (5 ; 3)\}$$

o sea $(5 ; 3) = \{(5 ; 3), (8 ; 6), (9 ; 7), \ldots\ldots\}$

b) Sea C el conjunto formado por todas las rectas de un plano y "paralelismo" una relación de equivalencia definida en el mismo (toda recta se considera paralela a sí misma.)

Queda establecida una partición de C donde cada recta r representa la clase de equivalencia formada por todas las rectas que le son paralelas. Dicha clase se llama "dirección de la recta r" o "punto impropio de r".



O sea:

Dirección de una recta r es el conjunto de todas las rectas del plano *paralelas a* r.

5. RELACIONES DE ORDEN

Las colecciones ordenadas abundan en matemática: puntos de una recta, números naturales, etc. La noción es tan fundamental e intuitiva que aparece en la vida cotidiana: se ordenan libros, sillas, alumnos, etc.

¿Cuál es el significado intuitivo de un "orden"? Simplemente, dados dos objetos x e y, x "precede a" y, o y "precede a" x.

Usualmente en el caso de puntos de una recta horizontal "precede" significa "a la izquierda de"; en el caso de números naturales, significa "menor que"; en el caso de calles que corren de norte a sur, "precede" significa "al este de", etc.

En matemática, el concepto de orden admite distintas variantes. Se habla de orden amplio, estricto, parcial, total, de buena ordenación, etc.

Orden amplio

Definición

Una relación binaria $\mathcal{R}$ definida en un conjunto A es de orden amplio si y sólo si es reflexiva, antisimétrica y transitiva.

Es decir,

$$A_1: \quad x \in A \Rightarrow x \mathcal{R} x$$

$$A_2: \quad (x \mathcal{R} y \wedge y \mathcal{R} x) \Rightarrow x = y$$

$$A_3: \quad (x \mathcal{R} y \wedge y \mathcal{R} z) \Rightarrow x \mathcal{R} z$$

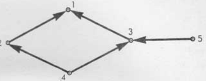
La relación $\mathcal{R}$ de orden amplio o no estricto se indica " $\preccurlyeq$ ".

Ejemplos

a) *En* $Z = \{x / x$ *número entero*$\}$ *se define*
$a \preccurlyeq b \Leftrightarrow \exists c$ *número natural o cero tal que* $a + c = b$

b) *En* $Z = \{x / x$ *número entero*$\}$ *se define* $a \preccurlyeq b \Leftrightarrow \exists c \in Z / b = a \cdot c$

c) *Sea* $A = \{1, 2, 3, 4, 5\}$ *y la relación caracterizada por*
$x \preccurlyeq y \Leftrightarrow x = y$ *o el camino de* x *a* y *tiene el sentido indicado en el diagrama:*



Orden estricto

Definición

Una relación binaria $\mathcal{R}$ definida en un conjunto A es de orden estricto si y sólo si es a-reflexiva, a-simétrica y transitiva.

Es decir,

$$S_1: \quad x \mathcal{R} y \Rightarrow x \neq y$$

$$S_2: \quad x \mathcal{R} y \Rightarrow y \not\mathcal{R} x$$

$$S_3: \quad (x \mathcal{R} y \wedge y \mathcal{R} z) \Rightarrow x \mathcal{R} z$$

La relación $\mathcal{R}$ de orden estricto se indica " $\prec$ ".

Ejemplos

a) $Z = \{x / x$ *número entero*$\}$ *y* $a \prec b \Leftrightarrow \exists c \in N / a + c = b$

b) $A = \{a, b, c, d\}$
y $\mathcal{R} = \{(a; b), (a; c), (a; d), (b; c), (b; d), (c; d)\}$

Orden parcial y total

Si un conjunto A está ordenado en forma amplia o estricta según las condiciones anteriores, pueden existir elementos del conjunto para los cuales $a \mathcal{R} b \wedge b \mathcal{R} a$, es decir, elementos **no comparables** según la relación dada. En esta situación el orden definido es **parcial.**

Es decir, el conjunto de propiedades A_1, A_2 y A_4 es de **orden parcial amplio** y el conjunto S_1, S_2 y S_3 es de **orden parcial estricto.**

Si a las propiedades de orden amplio se agrega la propiedad **lineal** se obtiene un **orden total amplio.** Si a las de orden estricto se añade la ley de **tricotomía,** el orden es **total y estricto.**

En ambos casos no existen elementos incomparables.

Ejemplos

a) *La relación* $\mathcal{R}$, *definida en el ejemplo anterior, es de orden estricto total.*

b) *La relación definida en el tercer ejemplo de orden amplio es parcial, pues existen elementos incomparables. Por ejemplo,*

$$4 \not\mathcal{R} 5 \wedge 5 \not\mathcal{R} 4 \wedge 4 \neq 5 .$$

Es conveniente aclarar que las denominaciones de orden varían según los autores. Algunos prefieren considerar simplemente la siguiente clasificación:

1) **orden parcial :** relación reflexiva, antisimétrica y transitiva.

2) **orden lineal :** relación a-reflexiva, lineal y transitiva.

Buena ordenación

Interesan especialmente los conjuntos ordenados donde cada subconjunto no vacío tiene primer elemento o elemento mínimo.

Un elemento a, perteneciente a un conjunto totalmente ordenado A, es **primer elemento** de A si y sólo si $(x \in A \wedge x \neq a) \Rightarrow a \mathcal{R} x$.

Definición

Una relación binaria $\mathcal{R}$ definida en A es de buena ordenación si y sólo si es de orden total y todo subconjunto no vacío de A tiene primer elemento.

Ejemplos

a) *El conjunto de los números naturales está bien ordenado respecto de la relación de menor.*

b) *El conjunto de los números racionales positivos no está bien ordenado respecto de la relación de menor. En efecto, el conjunto de todos los racionales positivos no tiene primer elemento, pues si r es un racional cualquiera positivo, $\frac{r}{2}$ también es positivo y menor que r.*

6. RELACIONES FUNCIONALES O APLICACIONES

El concepto de **función** es uno de los más importantes en matemática. El término "función" admite varios sinónimos: aplicación, transformación, proyección, correspondencia.

Toda función es una relación, pero el recíproco no es cierto, pues una relación donde existan dos pares ordenados que tengan el mismo primer elemento no es una función.

Es decir, una función está determinada por una regla o conjunto de reglas que asigna a cada elemento de un conjunto A (dominio) un **único** elemento de un conjunto B. La idea fundamental del concepto de función es que cada elemento del dominio tiene una y sólo una imagen en el conjunto B. El conjunto de imágenes se denomina recorrido y es un subconjunto de B.

En general, un elemento del recorrido puede ser imagen de más de un elemento del dominio.

Definición

Una relación f entre elementos de un conjunto A y elementos de un conjunto B es una función o aplicación de A en B si y sólo si

1º) $\forall x \in A \, , \, \exists y \in B \, / \, (x \, ; y) \in f$

2º) $[(x \, ; y) \in f \wedge (x \, ; z) \in f] \Rightarrow y = z$

Notación:

función $f : A \rightarrow B$

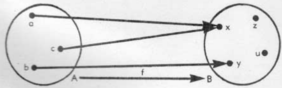
dominio $D_f = A$

recorrido $R_f = \{y \, / \, y \in B \wedge \exists x \in A \wedge f(x) = y\}$

Para dar una función es necesario indicar no solamente las reglas de correspondencia sino también su dominio.

Ejemplos

a) *Sea $f: A \rightarrow B$ definida por*

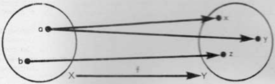


Entonces es: $f = \{(a;x), (b;y), (c;z)\}$

y suele escribirse:

$$x = f(a)$$
$$y = f(b)$$
$$z = f(c)$$

b) *La correspondencia*



no es una función, pues

$$[(a;x) \in f \wedge (a;y) \in f] \wedge x \neq y,$$

en contradicción con la segunda condición de la definición.

c) *Si* $f: x \to \begin{cases} x^2 + 1 \text{ para } x \geqslant 0 \\ 1 + x \text{ para } x \leqslant 0 \end{cases}$, *entonces f es una función.*

En efecto, aunque para $x = 0$ *hay dos reglas diferentes de correspondencia, la imagen* $f(0) = 1$ *es única.*

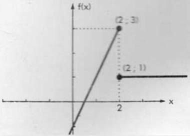
d) *Si* $g: x \to \begin{cases} x + 3 \text{ para } x \geqslant 1 \\ 2 + x^2 \text{ para } x \leqslant 1 \end{cases}$, *entonces g no es una función, pues*

$g(1) = 4 \wedge g(1) = 3$, *o sea la imagen de 1 no es única.*

Interpretación gráfica

La definición de función asegura que para toda representación en coordenadas cartesianas ortogonales, si f es una función, entonces una vertical corta su gráfico **a lo sumo** en un punto.

Si $f: x \to \begin{cases} 2x - 1 \text{ para } x \leqslant 2 \\ 1 \quad \text{ para } x \geqslant 2 \end{cases}$

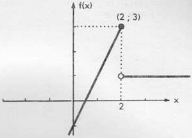


entonces f no es una función, pues la vertical $x = 2$ corta al gráfico en dos puntos.

Si eliminamos la segunda imagen de 2, es decir:

$$g: x \to \begin{cases} 2x - 1 & \text{para } x \leqslant 2 \\ 1 & \text{para } x > 2 \end{cases}, \text{ entonces } g \text{ es una función.}$$

En efecto, la vertical $x = 2$ corta al gráfico solamente en el punto $(2 ; 3)$.



Clasificación de aplicaciones

I — Hasta ahora se han considerado aplicaciones de un conjunto **en** otro. En general, en estos casos el recorrido es un subconjunto del segundo conjunto.

Si $f: A \to B$ **donde** $R_f \subseteq B$, **entonces** f **es una aplicación de** A **en** B.

Ejemplos

a) Si $f: x \to 2x + 1$, entonces f es una aplicación del conjunto de los números naturales en sí mismo, o sea una aplicación de N en N, donde el recorrido es el conjunto de los números impares, incluído propiamente en N.

$$f: N \to N \text{ y } R_f \subset N$$

b) Sea $A = \{a, b, c\}$ y $B = \{x, y, z, k\}$
$g = \{(a ; x), (b ; x), (c ; y)\}$ es una aplicación de A en B.
$R_g = \{x, y\}$ y $R_g \subset B$

II — Aplicaciones sobre o suryectivas

Si cada elemento del conjunto B es imagen, por lo menos, de un elemento del conjunto A, entonces la aplicación es de A **sobre** B.

Definición

f es una aplicación de A sobre B si y sólo si $R_f = B$

Ejemplos

a) $h: x \rightarrow x + 3$ *es una aplicación de N sobre N*

b) *Si* $A = \{a, b, c\}$ *y* $B = \{x, y\}$

$f = \{(a; x), (b; y), (c; y)\}$ *es una aplicación de A sobre B.*

c) *Si* $A = \{a, b, c\}$ *y* $B = \{x, y, z\}$

$g = \{(a; x), (b; y), (c; y)\}$ *no es una aplicación sobre B, pues* $z \in B$ *y no es imagen de ningún elemento de A.*

III — Aplicaciones "uno a uno" o inyectivas

Definición

f es una aplicación inyectiva de A en B o simplemente "uno a uno" de A en B si y sólo si
$\forall a \in A, \forall b \in A: f(a) = f(b) \Rightarrow a = b.$

Es decir, una función "uno a uno" asigna a elementos diferentes del dominio elementos diferentes en el recorrido.

Ejemplos

a) *Si* $A = \{1, 2, 3, 4\}$ *y* $B = \{0, 5, 6, 7, 8\}$

f: $1 \rightarrow 0$
$2 \rightarrow 5$
$3 \rightarrow 6$
$4 \rightarrow 7$ *es una aplicación inyectiva de A en B.*

b) *Si* $g: x \rightarrow x^2$, *g no es una aplicación "uno a uno" del conjunto de los números reales en sí mismo, pues si* $a \neq 0$, $a \neq -a$ *pero* $f(a) = f(-a)$, *ya que elementos distintos del dominio tienen la misma imagen.*

Gráficamente, si la aplicación es "uno a uno", entonces una recta horizontal intersecta a su representación en coordenadas cartesianas **a lo sumo** en un punto.

IV — Aplicaciones biyectivas o "uno a uno sobre"

Definición

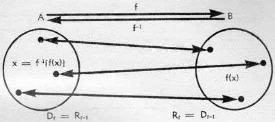
f es una aplicación biyectiva si y sólo si es inyectiva y suryectiva.

En este caso queda establecida una correspondencia biunívoca entre A y B.

Las aplicaciones biyectivas tienen extraordinaria importancia en el estudio de funciones, pues sus relaciones inversas son también aplicaciones biyectivas.

En efecto, puede demostrarse que si f es una aplicación biyectiva de A sobre B, entonces la relación inversa f^{-1} es una función biyectiva de B sobre A y

$$f^{-1}[f(x)] = x \quad \forall x \in D_f$$



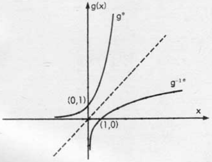
Ejemplos

a) *f: $x \to x^3$ es una función biyectiva definida sobre el conjunto de los números reales.*

f^{-1}: $x \to \sqrt[3]{x}$ es también una función biyectiva sobre R.

c) *g: $x \to e^x$ es una aplicación biyectiva del conjunto de los números reales sobre el conjunto de los reales positivos.*

g^{-1}: $x \to \ln x$ es una aplicación biyectiva del conjunto de los reales positivos sobre el conjunto de los reales.

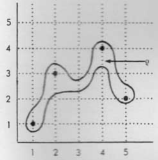


g se lee "gráfico de la función g".*

El gráfico de la función inversa puede obtenerse por simetría respecto de la recta a que pertenece la bisectriz del primer cuadrante.

EJERCICIOS

1. — *Siendo el siguiente el gráfico de la relación ϱ en $\{1, 2, 3, 4, 5\}$ indicar D_ϱ, R_ϱ y la imagen de cada elemento del dominio. Dar la relación inversa.*



2. — *Sean f y v dos proposiciones, la primera falsa y la segunda verdadera. Hacer el gráfico en $\{f, v\} \times \{f, v\}$ de las relaciones determinadas por:*
   a) $\wedge$ b) $\vee$ c) $\Longrightarrow$ d) $\Longleftrightarrow$

3. — *¿Qué otras relaciones son posibles en el conjunto del ejemplo anterior? ¿Tienen sentido lógico?*

4. — *Siendo $A = \{-4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$ y R el conjunto de los números reales, hacer el gráfico de la relación φ:*

   $(x; y) \in \varphi \Longleftrightarrow x \in A,\ y \in R \wedge x + y = 8$. *Dar la relación inversa.*

5. — *Indicar todas las relaciones posibles en $G = \{0, 1, 2\}$*

6. — *Siendo $A = \{0, 1, 2, 3\}$ y $B = \{x, y, z\}$, hacer el gráfico, indicar dominio, recorrido y relación inversa de:*

   $\mathcal{R}_1 = \{(0; x), (0; y), (3; z)\}$
   $\mathcal{R}_2 = \{(0; 0), (0; 2), (0; 3), (0; 1), (3; 2)\}$
   $\mathcal{R}_3 = \{(y; z), (z; y)\}$
   $\mathcal{R}_4 = \{(x; 0), (y; 0), (z; 3)\}$

7. — *Dar ejemplos de relaciones reflexivas, a-reflexivas y no-reflexivas.*

8. — *Dar ejemplos de relaciones simétricas, a-simétricas, no-simétricas y anti-simétricas.*

9. — *Dar ejemplos de relaciones transitivas, a-transitivas y no-transitivas.*

10. — *Clasificar las siguientes relaciones de acuerdo con su tipo de reflexividad, simetría y transitividad:*
    a) *"es esposa de" aplicada a gente*

b) "está al este de" aplicada a lugares de Europa.
c) "está al este de" aplicada a lugares de la Tierra.
d) "es múltiplo de" aplicada a enteros positivos.
e) "es tangente a" aplicada a circunferencias en E_2.
f) "es suplemento de" aplicada a ángulos en E_2.

11. — *Dar ejemplos de una relación:*
a) a-reflexiva, a-simétrica y transitiva.
b) a-reflexiva, a-simétrica y a-transitiva.
c) no-reflexiva, no-simétrica y no-transitiva.

12. — *¿Qué propiedades tiene la relación* $\mathcal{R} = \{(0;1), (2;3)\}$ *definida en el conjunto* $\{0, 1, 2, 3, 4\}$?

13. — *Sea C el conjunto de todos los pares ordenados de enteros. Se define la siguiente relación:* $(a;b) \sim (c;d) \Leftrightarrow a \cdot d = b \cdot c$. *Probar que es una relación de equivalencia, si se excluye el par* $(0;0)$.

14. — *Definir el número racional por abstracción (considerar el conjunto C del ejercicio anterior excluyendo los pares de segunda componente 0).*

15. — *Indicar cuáles de las siguientes relaciones son de equivalencia:*
a) "congruencia" definida en el conjunto de triángulos en E_2.
b) "primos entre sí" definida en el conjunto de enteros positivos.
c) "perpendicularidad" definida en el conjunto de rectas de E_2.

16. — *Definir "forma" de polígonos por abstracción.*

17. — *Definir "superficie" de polígonos por abstracción.*

18. — *Sea* $\mathcal{R}$ *una relación simétrica y transitiva definida en A. Probar que si* $\forall a \in A$, $\exists b \in A / a \,\mathcal{R}\, b$, *entonces* $\mathcal{R}$ *es una relación de equivalencia.*

19. — *Sea* $A = \{1, 2, 3, 4, 5, 6, 7\}$. *Indicar cuáles de las siguientes familias de conjuntos constituyen una partición de A.*
a) $\{A_1, A_2, A_3\}$ *siendo* $A_1 = \{1, 3, 5\}, A_2 = \{2\}, A_3 = \{4, 7\}$
b) $\{B_1, B_2, B_3\}$ *siendo* $B_1 = \{1, 5, 7\}, B_2 = \{3, 4\}, B_3 = \{2, 5, 6\}$
c) $\{C_1\}$ *siendo* $C_1 = \{1, 2, 3, 4, 5, 6, 7\}$
d) $\{D_1, D_2, D_3\}$ *siendo* $D_1 = \{1, 2, 5, 7\}, D_2 = \{3\}, D_3 = \{4, 6\}$

20. — *Probar los lemas 4 y 5.*

21. — *Dar ejemplos de relaciones de orden parcial estricto, parcial amplio, total estricto y total amplio.*

22. — *Probar que en una familia de conjuntos la relación de inclusión* $\subseteq$ *establece un orden amplio.*

23. — *Sean U y V dos conjuntos ordenados en forma estricta y total. Definir un orden total en U × V.*

24. — *Sean* $A = \{1, 2, 3, 4\}$, $B = \{a, b, c\}$ *y* $\alpha = \{(1;a), (2;b), (3;b), (4;c)\}$ *¿Es* α *una aplicación de A sobre B? ¿Es inyectiva? ¿Admite aplicación inversa?*

25. — *Sea* $A = \{a, b, c, d\}$ *y* $B = \{x, y, z, w\}$. *Definir una aplicación f de A sobre B que admita inversa y hallar* f^{-1}.

26. — *Siendo* $f: x \to \operatorname{sen} x$ *para x número real, restringir el dominio de f para que exista* f^{-1}. *Hacer lo mismo para cos x y tg x.*

27. — *Indicar cuáles de las siguientes relaciones son funciones:*
a) $f: x \to |x|$ *para x número real.*

b) $g: x \to \operatorname{sen}^{-1} x$ para x número real

c) $h: x \to \begin{cases} 3x + 5 & \text{para } x \geqslant 0 \\ 5 - x & \text{para } x \leqslant 0 \end{cases}$

d) $s: x \to 4$ para x número complejo.

28. — *Indicar los dominios de las siguientes funciones para que su recorrido esté incluido en el conjunto de los números reales:*

a) $f: x \to \sqrt{x - 1}$

b) $g: x \to \dfrac{1 + |x|}{1 - |x|}$

29. — *Hacer el gráfico de las siguientes funciones bijectivas y construir por simetría el gráfico de sus funciones inversas:*

a) $f: x \to 2x - 3$

b) $g: x \to \operatorname{sen} x$ para $\dfrac{\pi}{2} \leqslant x \leqslant \dfrac{3\pi}{2}$

c) $z: x \to x^2$ para $x \geqslant 0$

CAPITULO IV

Leyes algebraicas

1. LEYES DE COMPOSICIÓN INTERNA

Cuando se intenta definir una operación entre elementos de un conjunto se piensa de inmediato en establecer una ley o un criterio según el cual se pueda asociar a cada par de elementos del conjunto otro elemento del mismo, que será el resultado de tal operación aplicada a los primeros. Es decir, la operación aplicada a cuplas del conjunto determina otro elemento de él. Entonces puede introducirse el concepto de operación o más propiamente de ley de composición interna, mediante la siguiente:

Definición

Se llama ley de composición interna sobre un conjunto E **a toda aplicación de** $E \times E$ **en** E.

Es decir, ley interna: $E \times E \xrightarrow{f} E$

Si la imagen de una cupla $(x\,;y) \in E \times E$ por la aplicación f es un elemento $z \in E$, z recibe el nombre de compuesto de $(x\,;y)$ por esa ley.

O sea:

$$f(x\,;y) = z$$

En lugar de designar el compuesto z por $f(x\,;y)$ es frecuente utilizar diversas notaciones para una ley de composición interna, tales como:

1	$x + y = z$	Se lee x más y
2	$x \quad y = z$	,, ,, x multiplicado por y
3	$x * y = z$	,, ,, x estrella y
4	$x \circ y = z$	,, ,, x círculo y
5	$x \top y = z$	,, ,, x truco y
6	$x \perp y = z$	,, ,, x antitruco y

Tal nómina de símbolos representativos de leyes de composición no pretende ser completa, por cuanto podrá utilizarse cualquier otra notación convencional. Sin embargo, esa lista incluye las expresiones más frecuentes.

Una ley de composición interna queda determinada cuando se conoce el compuesto de cualquier cupla perteneciente a $E \times E$. Una formal usual y cómoda de establecer una ley es construir un cuadro de composición (tabla de operación) según el siguiente criterio:

a) En la primera columna se disponen los elementos de E (primera proyección de las cuplas de $E \times E$).

b) En la primera fila los mismos elementos de E (segunda proyección de las cuplas de $E \times E$).

c) El compuesto $z = a * b$ se ubica en la intersección de la fila que determina a y la columna que define b.

Ley de composición interna $*$

E \ E	a	b	c	e	.	.	.	y
a	b	c	d	a	.	.	.	.
b	c	a	d	b	.	.	.	.
c	d	b	a	c	.	.	.	.
e	a	b	c	e	.	.	.	.
.	.	.	.	.	.	.	.	.
x	.	.	.	.	.	.	.	$x * y$

Es obvio que el primer cuadro de composición ha sido la tabla pitagórica para la suma.

Observación

Dado que las cuplas son pares ordenados, los compuestos de las cuplas $(x ; y)$ e $(y ; x)$ no tienen por qué ser "a priori" iguales; en consecuencia la primera columna del cuadro contiene "exclusivamente" elementos a la izquierda de $*$ y la primera fila elementos a la derecha de $*$.

Definición

Un subconjunto A de E se dice cerrado para una ley definida

en E si y sólo si el compuesto de cualquier par de elementos de A pertenece a A.

A cerrado para $*$ definido en E $\Leftrightarrow$

$$[A \subset E \wedge \forall x \, \forall y \, / \, x \in A \wedge y \in A \Rightarrow x * y \in A]$$

Ejemplo

Si

$$E = N \; ; \; * = + \quad y \quad A = \{x \, / \, x \in N \wedge x \, \text{par}\} \, ,$$

entonces A es cerrado para esa operación suma, puesto que la suma de dos números pares cualesquiera es siempre un número par.

2. PROPIEDADES DE LAS LEYES DE COMPOSICIÓN INTERNA

Estabilidad

Es frecuente e importante el caso en que se han definido simultáneamente una ley de composición interna y una relación de equivalencia entre los elementos de un mismo conjunto. En esa situación sólo existe interés si la relación de equivalencia se conserva para la operación, esto es si el compuesto de dos elementos cualesquiera es equivalente al compuesto de los respectivamente equivalentes a aquéllos; puede introducirse así una primera propiedad característica de una operación, según lo siguiente:

Definición

Una ley de composición interna $(*)$ definida en un conjunto E se dice estable respecto de una relación de equivalencia $(\sim)$ definida entre los elementos del mismo conjunto si y sólo si los compuestos de elementos equivalentes, son también equivalentes.

Esto es:

$$(*) \text{ estable respecto de } (\sim) \Leftrightarrow$$

$$[\forall a \, \forall b \in E \wedge \forall a' \, \forall b' \in E \, / \, a \sim a' \wedge b \sim b'] \Rightarrow$$

$$a * b \sim a' * b'$$

Algunos autores suelen expresar también esta propiedad diciendo que la relación de equivalencia es compatible con la operación "estrella" o que la operación está "bien definida" para esa relación de equivalencia.

Según sabemos, toda relación de equivalencia definida entre los elementos de un conjunto E, introduce en el mismo una partición en clases disjuntas no vacías y cuya unión es el conjunto E tal que dos elementos de E pertenecen a una de esas clases si y sólo si son equivalentes. Tales clases de equivalencia permiten definir, por abstracción, nuevos entes matemáticos, los que constituyen el cociente del conjunto E sobre $\sim$.

Sea

$$E = \{a, a_1, a_2, \ldots, b, b_1, b_2, \ldots, m, m_1, m_2, \ldots\}$$

y $\sim$ la relación en E.

Resulta

$$E = C_a \cup C_b \cup C_c \cup \ldots \cup C_m$$

Donde $C_a, C_b, C_c, \ldots, C_m$ son las clases de equivalencia, o sea:

$$a \sim a_1 \sim a_2 \sim \ldots \in C_a$$

$$b \sim b_1 \sim b_2 \sim \ldots \in C_b$$

. . . .

$$m \sim m_1 \sim m_2 \sim \ldots \in C_m$$

Entonces la clase C_a define un nuevo ente α, la C_b un β, ... la C_m un μ, tal que:

$$\frac{E}{\sim} = \{\alpha, \beta, \ldots, \mu\}$$

Cada ente $\alpha, \beta, \ldots, \mu$ es la respectiva clase; pero cuando deban utilizarse los mismos, cualquier a_i representará al α, cualquier b_j al β, etcétera.

Sea $*$ una ley de composición interna en E:

$$\forall a \ \forall b \in E \ ; \ a * b = c \in E$$

Si la ley es estable para la relación $\sim$:

$$a \sim a' \wedge b \sim b' \Rightarrow a * b \sim a' * b'$$

Pero $a, a', \ldots, \in C_a$ y $b, b', \ldots \in C_b$ y si $c = a * b$ y $c' = a' * b'$ es $c \sim c'$ y en consecuencia, $c, c', \ldots \in C_n$

En consecuencia, dadas dos clases cualesquiera C_a y C_b existe siempre una aplicación que designaremos $*'$ tal que:

$$(C_a ; C_b) \xrightarrow{*'} C_n$$

O lo que es lo mismo:

$$C_a *' C_b = C_n$$

Esto es, la ley * ha "inducido" u originado, por el solo hecho de ser estable, una nueva ley sobre el conjunto cociente.

Tal ley se llama inducida por * y el razonamiento realizado nos permite enunciar el siguiente:

Teorema

Una ley de composición interna definida sobre un conjunto, y estable respecto de una relación de equivalencia en el mismo, induce en el conjunto cociente una nueva ley de composición (que en algunos casos puede coincidir con la primera).

Ejemplo

Consideremos el conjunto $E = Z \times Z^*$, donde Z es el conjunto de los números enteros y Z^* el de los enteros excluido el cero. Esto es, los elementos de E son cuplas de enteros de segunda proyección no nula.

Si:

$$(a_1 ; b_1) \in E \text{ y } (a_2 ; b_2) \in E \text{, se define la siguiente relación:}$$

$$(a_1 ; b_1) \sim (a_2 ; b_2) \iff a_1 \cdot b_2 = a_2 \cdot b_1$$

para la que puede demostrarse que es una relación de equivalencia.

En E se define la siguiente ley de composición:

$$(a_1 ; b_1) + (a_2 ; b_2) = (a_1 b_2 + a_2 b_1 ; b_1 \cdot b_2),$$

la que resulta estable para la relación anterior de equivalencia.

Las clases de equivalencia en E, definen por abstracción los números

$$\frac{a}{b} = C_a \subset E \,/\, (a_1 ; b_1) \text{ y } (a_2 ; b_2) \in C_a \iff a_1 \cdot b_2 = a_2 \cdot b_1$$

De acuerdo con el teorema anterior esa operación + induce en el conjunto de los racionales:

$$Q = \frac{E \times E^*}{\sim},$$

una ley de composición interna, a la que también llamamos "adición de números racionales".

Pero para sumar los racionales $\frac{a}{b}$ y $\frac{c}{d}$, que son respectivamente las clases de equivalencias C_a y C_c, debemos utilizar representantes de esas clases, que pueden ser cualesquiera.

Luego,

$$\forall (a_1 ; b_1) \in C_a \quad \text{y} \quad \forall (c_1 ; d_1) \in C_c \text{, se tiene:}$$

$\frac{a}{b} + \frac{c}{d} \Rightarrow (a_1 d_1 + b_1 c_1 ; b_1 d_1)$ *y este par pertenecerá a una clase C_m que define a un racional $\frac{m}{n}$.*

Entonces resulta la ley de composición interna:

$$\frac{a}{b} + \frac{c}{d} = \frac{m}{n}$$

Obsérvese que gracias a la estabilidad $\frac{m}{n}$ *es único.*

En efecto, si en vez de elegir $(a_1 ; b_1)$ *y* $(c_1 ; d_1)$ *como representantes de las clases* C_a *y* C_c, *hubiéramos considerado:*

$$(a_2 ; b_2) \in C_a \quad y \quad (c_2 ; d_2) \in C_c, \text{ será:}$$

$$(a_1 ; b_1) \sim (a_2 ; b_2) \text{ y } (c_1 ; d_1) \sim (c_2 ; d_2) \qquad (1)$$

y por la estabilidad:

$$(a_1 ; b_1) + (c_1 ; d_1) \sim (a_2 ; b_2) + (c_2 ; d_2) \qquad (2)$$

$$(a_1d_1 + b_1c_1 ; b_1d_1) \sim (a_2d_2 + b_2c_2 ; b_2d_2).$$

Es decir que ambos pares pertenecen a la clase C_m *y en consecuencia el par:*

$$(a_2d_2 + b_2c_2 ; b_2d_2)$$

representa al mismo racional $\frac{m}{n}$, *o lo que es lo mismo,* $\frac{m}{n}$ *es único, independientemente de los elementos que se utilicen para representar las clases de equivalencia.*

Resulta como síntesis del teorema y de las observaciones realizadas a través del ejemplo, que cuando los entes que se manejan son definidos por abstracción por medio de clases de equivalencia, sólo existe ley de composición inducida entre esos entes si la primera es estable para la relación de equivalencia que los engendró.

Finalmente obsérvese que si $\sim$ se tradujera por $=$, las relaciones (1) y (2) serían:

$$\begin{matrix} (a_1 ; b_1) = (a_2 ; b_2) \\ (c_1 ; d_1) = (c_2 ; d_2) \end{matrix} \Rightarrow (a_1 ; b_1) + (c_1 ; d_1) = (a_2 ; b_2) + (c_2 ; d_2),$$

o sea la estabilidad contiene a la ancestral propiedad uniforme.

Asociatividad

Definida una ley $*$ en E, todo par de elementos x e y de E determina un compuesto z perteneciente a E. En tal caso el par de elementos z, t de E definirá un nuevo compuesto r de E. Es decir:

$$x * y = z \qquad z * t = r$$

Lo que puede expresarse, de acuerdo con la significación de paréntesis,

$$(x * y) * z = r$$

Es decir, que toda ley de composición interna puede extenderse por recurrencia a n-uplas de E, y la expresión:

$$\{[(x * y) * z] \ldots\ldots * t\} = s,$$

tiene siempre un solo significado.

Definición

Una ley de composición interna se llama asociativa si y sólo si dados tres elementos cualesquiera del conjunto en un cierto orden, el compuesto del compuesto de los dos primeros con el tercero es igual al elemento que resulta de componer el primero con el compuesto de los otros dos.

Es decir:

la ley $*$ es asociativa si y sólo si:

$$\forall x, \forall y, \forall z \in E : (x * y) * z = x * (y * z)$$

En tales condiciones, conviniendo en considerar siempre los elementos de izquierda a derecha, si la ley es asociativa (y sólo en ese caso) podrá escribirse:

$$(x * y) * z = x * y * z = x * (y * z)$$

Corolario

Si una ley es asociativa el compuesto de una n-upla de E es independiente de las asociaciones que se realicen entre los elementos de la n-upla.

Es decir:

$$\{[x * (y * z)] * \ldots * t\} = \{[(x * y) * z] * \ldots\ldots * t\}$$

Ejemplo

La adición y la multiplicación en todos los conjuntos de números son operaciones asociativas.

Contraejemplo

La potenciación en N no es asociativa.

En efecto: si $a * b = a^b$, $(2 * 3) * 2 \neq 2 * (3 * 2)$, pues el primer miembro es igual a 64 y el segundo igual a 512.

En consecuencia, la notación a^{5^7}, carece de sentido matemático.

Conmutatividad

Puesto que una ley de composición es una aplicación de E x E en E, siendo los elementos de E x E pares ordenados, la imagen de (x ; y) no coincide, en general, con f(y ; x).

Definición

Una ley de composición interna se llama conmutativa si y sólo si el compuesto de dos elementos cualesquiera es independiente del orden de los mismos.

Es decir:

la ley $*$ es conmutativa si y sólo si:

$$\forall x, \forall y \in E : x * y = y * x$$

Corolario

Para una ley asociativa y conmutativa, el compuesto de n elementos es independiente, también, del orden de los mismos.

Basta demostrar que puede cambiarse el orden de dos elementos consecutivos, ya que, satisfecha esa condición, cualquier elemento podrá llevarse por reiteración a cualquier lugar preestablecido.

Es decir, basta demostrar:

$$a_1 * a_2 * a_3 * \ldots\ldots * a_n * a_{n+1} * \ldots . * q =$$
$$= a_1 * a_2 * a_3 * \ldots\ldots * a_{n+1} * a_n * \ldots . * q$$

Si llamamos A al compuesto total, $B = a_1 * a_2 * \ldots . * a_{n-1}$ y $C = a_{n+2} * \ldots . * q$, entonces:

$A = B * a_n * a_{n+1} * C$ por ley asociativa
$A = B * (a_n * a_{n+1}) * C$ " " "
$A = B * (a_{n+1} * a_n) * C$ por ley conmutativa
$A = B * a_{n+1} * a_n * C$ por ley asociativa, lo que demuestra el corolario.

Ejemplo

La adición y la multiplicación en todos los conjuntos numéricos son conmutativas.

Contraejemplo

La potenciación no lo es.

Distributividad

Si sobre un conjunto E se han definido dos leyes de composición interna que indicamos por $\perp$ y $\perp$ se puede, por ejemplo, componer x e y $\in$ E con $\top$ y el resultado (que $\in$ E) con otro z $\in$ E, por medio de la ley $\perp$. Se tiene:

$$z \perp (x \top y) \quad \text{o} \quad (x \top y) \perp z,$$

según el orden en que se opere.

Definición

Una ley de composición $\perp$ es distributiva a la izquierda o a la derecha respecto de otra ley $\top$ definidas sobre un mismo conjunto si y si sólo si cualesquiera sean los elementos x, y, z del conjunto, se verifica:

$$z \perp (x \top y) = (z \perp x) \top (z \perp y)$$

(Distributiva a la izquierda)

$$\text{o} \quad (x \top y) \perp z = (x \perp z) \top (y \perp z)$$

(Distributiva a la derecha).

Si la ley $\perp$ es simultáneamente distributiva a derecha e izquierda, se dice que es doblemente distributiva o, más simplemente, distributiva.

Ejemplos

La multiplicación, en cualquier conjunto numérico, respecto de la adición.
La potenciación, respecto del producto y del cociente.

Contraejemplos

La adición no es distributiva respecto del producto.
La potenciación, radicación y logaritmación no lo son respecto a la adición o diferencia.

Simplificación o Cancelación

En un conjunto E, la igualdad de dos de sus elementos x e y implica la identidad, esto es que x e y son el mismo elemento. Luego cualquiera sea z $\in$ E,

$$x = y \Rightarrow z * x = z * y \quad \text{y} \quad x * z = y * z$$

La implicación recíproca no siempre es verdadera. Basta en efecto observar que la igualdad:

$$0 \cdot a = 0 \cdot b,$$

no garantiza la identidad de a y b.

Definición

Una ley de composición interna se dice cancelativa a la izquierda o a la derecha, respectivamente, si cualesquiera sean x, y, z del conjunto se verifica:

$$z * x = z * y \Rightarrow x = y \qquad \text{(Cancelativa a la izquierda).}$$

o

$$x * z = y * z \Rightarrow x = y \qquad \text{(Cancelativa a la derecha).}$$

Si la ley es simultáneamente cancelativa a la izquierda y a la derecha, se dice, simplemente, que es cancelativa.

Ejemplo

La adición de números es cancelativa.

Contraejemplo

La multiplicación de números no goza de la propiedad cancelativa (salvo que en el conjunto de tales entes se excluya el cero).

3. ELEMENTOS PARTICULARES

Elemento neutro

Definición

Un elemento de un conjunto E es neutro para una ley de E, si y sólo si su compuesto con cualquier elemento de E, por la izquierda y por la derecha, es ese mismo elemento.

$$e \text{ neutro para } * \Leftrightarrow [(e \in E \wedge \forall x \in E) \Rightarrow e * x = x * e = x]$$

Ejemplo

En el conjunto de los números naturales el cero es neutro para la adición *y el 1 es neutro para la multiplicación, puesto que cualquiera sea a:*

$$a + 0 = 0 + a = a \; ; \; a \cdot 1 = 1 \cdot a = a$$

Corolario

Si existe elemento neutro para una operación, es único.

En efecto, si además de e existiera e′ neutro:

$\forall x \in E$: $e * x = x * e = x$ y si $x = e'$:
$e * e' = e' * e = e'$ (1)

Análogamente si e′ es neutro:

$\forall x \in E$: $e' * x = x * e' = x$ y si $x = e$:
$e' * e = e * e' = e$ (2)

Y de (1) y (2) : $e = e' \Rightarrow e$ es único.

Elementos simétricos o inversos

Definición

Dada una ley con elemento neutro e, se dice que dos elementos a y a′ son simétricos si y sólo si sus compuestos, en cualquier orden, son el elemento neutro.

$$a \text{ y } a' \text{ simétricos} \Leftrightarrow a * a' = a' * a = e$$

Ejemplos

En el conjunto de los números enteros, todo número a, tiene un simétrico respecto de la adición: $-a$. En este caso, cuando la ley es la adición, se dice también que los simétricos a y $-a$, son opuestos.

Entre los números racionales, todo $\frac{a}{b}$ no nulo tiene un simétrico $\frac{b}{a}$. Para la operación multiplicación los simétricos se suelen designar recíprocos.

Notación: De una manera general, si existe a′ simétrico de a, se suele escribir $a' = a^{-1}$.

Corolario

En toda operación asociativa el simétrico del simétrico de un elemento es el mismo elemento.

En efecto, si a y a^{-1} son simétricos, por definición:

$$a^{-1} * a = e$$

Y si $(a^{-1})^{-1}$ es el simétrico de a^{-1}, operando en la relación anterior, a la izquierda:

$$(a^{-1})^{-1} * (a^{-1} * a) = (a^{-1})^{-1} * e$$

Y por ley asociativa:

$$[(a^{-1})^{-1} * a^{-1}] * a = (a^{-1})^{-1} * e$$

Por definición de simétrico y de neutro:

$$e * a = (a^{-1})^{-1}$$

Luego:

$$a = (a^{-1})^{-1}$$

Teorema

Para una ley asociativa, el simétrico de un elemento, si existe, es único.

Sean a' y a^{-1} dos simétricos de un elemento a.

Entonces:

$$a * a^{-1} = a^{-1} * a = e \ (1) \quad \text{y} \quad a * a' = a' * a = e \ (2)$$

Considerando de (2): $a * a' = e$ y componiendo a la izquierda con a^{-1}:

$$a^{-1} * (a * a') = a^{-1} * e$$

Y por ser la ley asociativa:

$$(a^{-1} * a) * a' = a^{-1} * e$$

Por definición de simétrico y neutro:

$$e * a' = a^{-1}$$

$$a' = a^{-1}$$

Elementos regulares

Si una operación posee la propiedad cancelativa, resulta que un elemento a cualquiera es simplificable, puesto que:

$$a * x = a * y \wedge x * a = y * a \Leftrightarrow x = y$$

 donde, en efecto, a se ha reducido o simplificado.

Definición

Todo elemento de un conjunto para el cual es válida la propiedad cancelativa de una ley de composición sobre el conjunto se dice regular para esa ley.

Ejemplo

Todos los números naturales son regulares para la adición definida entre los mismos.

Definición

Si la ley de composición es sólo cancelativa a la izquierda o a la derecha, los elementos a los cuales se aplica la ley se dicen, respectivamente, regulares a la izquierda o a la derecha.

Si se tiene:

$$a * x = a * y \Rightarrow x = y$$

a regular a la izquierda.

$$x * a = y * a \Rightarrow x = y$$

a regular a la derecha.

Corolario

Si un elemento es regular para una ley, es simultáneamente regular a la izquierda y a la derecha.

Propiedades y elementos de leyes inducidas

Según se vio en la pág. 67 una ley de composición interna estable respecto de una relación de equivalencia, induce o genera una nueva ley de composición sobre el conjunto cociente del primer conjunto por la relación de equivalencia.

Puesto que toda relación de igualdad entre compuestos según la primera ley en E, se conserva cuando se pasa a la ley inducida sobre el conjunto cociente, puede de inmediato introducirse el siguiente enunciado:

Teorema

Toda ley inducida sobre el conjunto cociente $\frac{E}{\sim}$ por una ley de composición interna de E, estable respecto de $\sim$, tiene las

mismas propiedades que la operación original y sus mismos elementos especiales.

4. COMPOSICIÓN DE APLICACIONES

Sean los conjuntos A, B, C ; f una aplicación de A en B y g una aplicación de B en C.

Es decir:

$$\forall a \in A\ ,\ \exists b \in B\ /\ a \xrightarrow{f} b$$

y

$$\forall b \in B\ ,\ \exists c \in C\ /\ b \xrightarrow{g} c$$

Entonces existe siempre una aplicación h de A en C, puesto que:

$$\forall a \in A,\ \exists c \in C\ /\ \begin{tikzcd} a \arrow[r, "f"] \arrow[rr, bend right, "h"'] & b \arrow[r, "g"] & c \end{tikzcd}$$

La aplicación h es la aplicación compuesta de f y g, o la aplicación producto de las mismas.

Esta consideración lleva a la siguiente:

Definición

Dadas las aplicaciones f de A en B y g de B en C se llama producto de esas aplicaciones a la aplicación de A en C, en la cual la imagen de un elemento a es la imagen a través de g, de la imagen de a a través de f.

$$h = g \circ f \Leftrightarrow A \xrightarrow{h} C\ /\ \forall a \in A : h(a) = g\,[f(a)]\,.$$

Corolario

La composición de aplicaciones que acaba de definirse es siempre asociativa.

Si se tiene:

$$\begin{aligned} f &: A \to B \\ g &: B \to C \\ h &: C \to D \end{aligned}$$

habrá que demostrar: $\forall a \in A$

$$[h \circ (g \circ f)](a) = [(h \circ g) \circ f](a) \qquad (1)$$

Si $a \in A$:

$$(g \circ f)(a) = g\,[f(a)]$$

y entonces:

$$[h \circ (g \circ f)]\,(a) = h\{g[f(a)]\} \qquad (2)$$

Análogamente:

$$(h \circ g)\,(b) = h[g(b)]$$

y entonces:

$$[(h \circ g) \circ f]\,(a) = h\{g[f(a)]\} \qquad (3)$$

De (2) y (3) surge la validez de (1)

Observaciones

I. El producto o composición de aplicaciones corresponde al concepto clásico de función de función para conjuntos numéricos.

II. El producto definido no es propiamente una ley de composición interna por cuanto las aplicaciones h, g, f, no son, obligatoriamente, elementos de un mismo conjunto.

Aplicaciones de un conjunto en sí mismo

Un caso particular muy importante se presenta si los conjuntos dados son iguales entre sí y las aplicaciones que se consideran pertenecen al conjunto de todas las aplicaciones de ese único conjunto en sí mismo.

Sea A un conjunto y $G = \{f, g, h, \ldots\}$ el conjunto de las aplicaciones de A en A.

Entonces:

$$\forall f \in G \text{ y } \forall a \in A : f(a) = b \in A$$

luego:

$$\forall b / b = f(a) : g(b) = c \in A$$

es decir:

$$\forall a \in A : a \xrightarrow{g \circ f} c \in A$$

o sea:

$$g \circ f \text{ es una aplicación de A en A} \Rightarrow g \circ f \in G$$

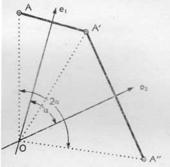
Y, en consecuencia, la ley $\circ$ (composición de aplicaciones) es una ley de composición interna en G.

De acuerdo con la demostración general, esa ley es siempre asociativa, pero puede o no, ser conmutativa.

Ejemplo

El caso analizado se presenta frecuentemente en todos los problemas relativos a las transformaciones puntuales en geometría, llamadas también transformaciones geométricas o más simplemente, puesto que son aplicaciones del conjunto de puntos del espacio sobre el mismo conjunto, operaciones geométricas.

Consideremos el conjunto de todas las transformaciones puntuales de la geometría métrica, es decir, el conjunto de las traslaciones, giros, movimientos, simetrías, homotecias y semejanzas.



Sea: f simetría axial de eje e_1:

$f = S(e_1)$

y g simetría axial de eje e_2:

$g = S(e_2)$, *tal que*

e_1 *y* e_2, *copuntuales.*

La imagen de un punto A del espacio a través de $S(e_1)$ *es* A'.

Se suele escribir:

$$A \cdot S(e_1) = A'.$$

Si A'' *es la imagen de* A' *a través de* $S(e_2)$:

$$A' \cdot S(e_2) = A''.$$

Luego: $A \cdot [S(e_2) \circ S(e_1)] = A''$.

Pero en tal caso la transformación para la cual A'' *(cualquiera sea A) es la imagen directa de A, es el giro de centro en la intersección de los ejes* e_1 *y* e_2 *y cuya amplitud es el ángulo duplo del que forman dichos ejes.*

Es decir:

$$A \cdot G(O, 2\alpha) = A''$$

o sea:

$$S(e_2) \circ S(e_1) \doteq G(O, 2\alpha)$$

De tal modo la aplicación compuesta de dos transformaciones geométricas es otra transformación.

5. LEYES DE COMPOSICIÓN EXTERNA

Según se ha visto, una ley de composición interna en E es una aplicación de E x E en E. Nada impide pensar en que puede establecerse una aplicación del producto cartesiano de dos conjuntos diferentes en uno de ellos. Es decir, a toda cupla de elementos de K y E se le asocia un elemento de E. En este caso se está realizando una operación con cada elemento de E, pero a través de un elemento de K; para operar necesitamos "salir" de E, pero retornamos a E con el resultado. Si se llama operador a cualquier elemento de K, tiene sentido la siguiente:

Definición

> **Dados los conjuntos E y K, se llama ley de composición externa en E, con operadores de K, a toda aplicación de K × E en E.**

Si convenimos en designar los elementos de E con letras latinas y los de K con minúsculas griegas, entonces:

$$\top \text{ es ley de composición externa en } E \iff (K \times E) \xrightarrow{\top} E .$$

O sea todo elemento $(\alpha ; x) \in K \times E$, tiene una imagen $y \in E$ a través de la aplicación $\top$:

$$(\alpha ; x) \xrightarrow{\top} y \in E$$

La notación más frecuente expresa el compuesto y, multiplicativamente entre el operador α y el elemento x, es decir:

$$(\alpha ; x) \xrightarrow{\top} y = \alpha \cdot x$$

o directamente.

$$(\alpha ; x) \xrightarrow{\top} \alpha \cdot x$$

Y es usual también, como se ha hecho, comenzar por escribir el operador.

Ejemplo

Sea E el conjunto de todos los segmentos métricos y K el conjunto de los números naturales. La clásica definición de producto de segmento por un número es una ley de composición externa en E con operadores de K, puesto que cualquier cupla: (número; segmento), tiene por imagen un segmento que pertenece, entonces, a E.

6. PROPIEDADES DE LAS LEYES DE COMPOSICIÓN EXTERNA

Si en los conjuntos E y K se han definido leyes de composición interna, se observa que puede tratar de combinarse esas leyes, respectivamente, con la externa.

Sea $*$ ley de composición interna de E.

$\top$ y $\perp$ leyes de composición interna en K.

$\cdot$ ley de composición externa de E en K.

Entonces pueden plantearse las siguientes combinaciones de operaciones:

1 $\alpha \cdot (x * y)$.
2 $(\alpha \top \beta) \cdot x$
3 $(\alpha \perp \beta) \cdot x$
4 $\alpha \cdot (\beta \cdot x)$

Estas alternativas dan lugar al estudio de las propiedades siguientes:

Distributividad

a) **de la ley externa, respecto de la interna de** E.

Definición

Una ley de composición externa en E**, con operadores de** K **es distributiva respecto de una ley de** E**, si y sólo si se verifica:**

$$\forall \alpha \in K, \forall x \forall y \in E : \alpha \cdot (x * y) = \alpha \cdot x * \alpha \cdot y$$

b) **de la ley externa, respecto de la interna de** K.

Definición

Una ley de composición externa en E**, con operadores de** K **es distributiva respecto de una ley de** K**, si y sólo si se verifica:**

$$\forall \alpha, \forall \beta \in K \wedge \forall x \in E : (\alpha \top \beta) \cdot x = \alpha \cdot x * \beta \cdot x$$

Contra la tentación de escribir:

$$(\alpha \top \beta) \cdot x = \alpha \cdot x \top \beta \cdot x \qquad (1),$$

debe pensarse que $\top$ es una operación de K y los compuestos $\alpha \cdot x$, $\beta \cdot x$, por definición de ley de composición externa, pertenecen a E, donde la ley de composición es $*$. En consecuencia la expresión (1) carece en general de significado.

Observación

Como en K, se han definido dos leyes internas $\top$ y $\perp$, podría plantearse análogamente una distributividad de $\cdot$ respecto de $\perp$.

Esto es:

$$(\alpha \perp \beta) \cdot x = \alpha \cdot x * \beta \cdot x$$

Sin embargo, la simultaneidad de las dos distributividades carece de sentido para el caso más frecuente de leyes externas con elementos regulares.

Probaremos que si se cumple esta condición, las dos distributividades respecto de $\top$ y $\perp$, implican la identidad de esas operaciones:

En efecto:

si: $$(\alpha \top \beta) \cdot x = \alpha \cdot x * \beta \cdot x$$

y $$(\alpha \perp \beta) \cdot x = \alpha \cdot x * \beta \cdot x$$

por propiedad simétrica y transitiva:

$$(\alpha \top \beta) \cdot x = (\alpha \perp \beta) \cdot x$$

Y si todos los elementos de E son regulares para la ley externa, resulta:

$$\alpha \top \beta = \alpha \perp \beta \Rightarrow \top = \perp$$

En consecuencia, para $\top$ y $\perp$ distintas sólo podrá existir distributividad de la ley externa respecto de una de ellas.

Asociatividad

Definición

Una ley de composición externa en E, con operadores de K, es asociativa respecto de una ley interna de K, si y sólo si se verifica:

$$\forall \alpha \, \forall \beta \in K \wedge \forall x \in E : \alpha \cdot (\beta \cdot x) = (\alpha \perp \beta) \cdot x$$

Observación

Con razonamiento análogo al de la observación anterior se prueba que la asociatividad de la ley externa, respecto de $\perp$ y $\top$, para elementos regulares, implica la identidad de $\perp$ y $\top$.

Surge como consecuencia de las dos observaciones formuladas que cuando K posee dos leyes internas, interesa sólo la distributividad de la ley externa respecto de una y la asociatividad respecto de la otra.

Ejemplo

Sea:

$E = \{x \,/\, x$ *segmento métrico*$\}$
$*$ *es la adición de segmentos* $(+)$
$K = \{n \,/\, n$ *número natural*$\}$
$\top$ *es la adición de números* $(+)$
$\perp$ *es la multiplicación de números* $(\cdot)$
$\cdot$ *es la multiplicación de un segmento por un número*

En tales condiciones:

1. $n \cdot (x + y) = n \cdot x + n \cdot y$

O sea que la ley externa es distributiva respecto de la interna de E.

2. $(n + m) \cdot x = n \cdot x + m \cdot x$

De donde resulta que la ley externa es distributiva respecto de la interna de K.

3. $m \cdot (n \cdot x) = (m \cdot n) \cdot x$

Es decir, la ley externa es asociativa respecto de la segunda ley interna de K.

Obsérvese en este ejemplo que el elemento neutro de la segunda operación de K es también neutro para la ley externa. En efecto, el elemento neutro de la multiplicación es el número 1 y $1 \cdot x = x$

7. HOMOMORFISMOS. ISOMORFISMOS

Sean los conjuntos A y A':

$$A = \{a, b, c, \ldots\}$$

$$A' = \{a', b', c', \ldots\}$$

provistos, respectivamente, de leyes de composición internas $\top$ y $\perp$

Consideremos una aplicación f de A en A':

$$a \xrightarrow{f} a'$$

$$b \xrightarrow{f} b'$$

$$\ldots\ldots\ldots$$

Si además:

$$a \top b = c \wedge a' \perp b' = c' \Rightarrow c \xrightarrow{f} c'$$

la aplicación f recibe el nombre de homomorfismo entre A y A'.

Definición

Una aplicación f entre dos conjuntos, provistos cada uno de una ley de composición interna, recibe el nombre de homomorfismo entre los mismos, si y sólo si la imagen del compuesto de cualquier cupla de elementos del primer conjunto es el compuesto de las imágenes de esos elementos.

Es decir, f es un homomorfismo entre A y A' $\Leftrightarrow$

$$\Leftrightarrow A \xrightarrow{f} A' \wedge f(a \top b) = f(a) \perp f(b)$$

Ejemplo

Sea A el conjunto Z de los números enteros, provisto de la multiplicación.
A' el conjunto: $A' = \{-1, 0, +1, +3\}$, también con la multiplicación entre enteros.

y f la siguiente aplicación: de A en A'

$$x > 0 : x \xrightarrow{f} +1$$
$$x = 0 : x \xrightarrow{f} 0$$
$$x < 0 : x \xrightarrow{f} -1$$

Tal aplicación es un homomorfismo entre A y A'.
En efecto, para cualquier cupla de elementos de A se presentan las siguientes alternativas: $\forall x, \forall y \in A$:

1 $\quad x > 0, y > 0 \Rightarrow x \cdot y > 0$:

$$f(x) = +1 \, , f(y) = +1 \, , f(x \cdot y) = +1 \Rightarrow$$
$$\Rightarrow f(x \cdot y) = f(x) \cdot f(y)$$

2 $\quad x > 0, y = 0 \Rightarrow x \cdot y = 0$:

$$f(x) = +1 \, , f(y) = 0 \, , f(x \cdot y) = 0 \Rightarrow$$
$$\Rightarrow f(x \cdot y) = f(x) \cdot (y)$$

3 $\quad x = 0 \, , y = 0 \Rightarrow x \cdot y = 0$:

$$f(x) = 0 \, , f(y) = 0 \, , f(x \cdot y) = 0 \Rightarrow$$
$$\Rightarrow f(x \cdot y) = f(x) \cdot f(y)$$

4 $\quad x > 0 \, , y < 0 \Rightarrow x \cdot y < 0$:

$$f(x) = +1 \, , f(y) = -1 \, , f(x \cdot y) = -1 \Rightarrow$$
$$\Rightarrow f(x \cdot y) = f(x) \cdot f(y)$$

5 $\quad x < 0 \, , y < 0 \Rightarrow x \cdot y > 0$:

$$f(x) = -1 \, , f(y) = -1 \, , f(x \cdot y) = +1 \Rightarrow$$
$$\Rightarrow f(x \cdot y) = f(x) \cdot f(y)$$

Definición

Si la aplicación f es un homomorfismo entre A y A' y f es suryectiva, el conjunto A' se denomina imagen homomorfa de A.

Ejemplo

Si en el ejemplo anterior se considera $A' = \{-1, 0, +1\}$, para la misma aplicación, A' es la imagen homomorfa de A, a través de f.

Observación

Si en A existe elemento neutro e para la ley $\top$:

$$\forall x \in A : x \top e = e \top x = x$$

Y si f es un homomorfismo entre A y A' :

$$\left.\begin{array}{l} x \xrightarrow{f} x' \in A' \\ e \xrightarrow{f} e' \in A' \end{array}\right\}$$

$x' \perp e' = f(x) \perp f(e) = f(x \top e) = f(x) = x'$ análogamente $e' \perp x' = x'$ luego $e' = f(e)$ es neutro para $\perp$

Es decir, **la imagen del elemento neutro de la ley del primer conjunto es elemento neutro para la ley del segundo.**

Definición

Un homomorfismo se denomina endomorfismo si el segundo conjunto está incluido en el primero.

Es decir:

$$A \xrightarrow{f} A'$$

f es endomorfismo $\iff$ f es homomorfismo $\wedge$ $A' \subseteq A$

Desde el punto de vista científico reviste fundamental importancia el caso de los homomorfismos biyectivos, es decir que la aplicación que introduce el homomorfismo es además biyectiva.

Definición

Todo homomorfismo biyectivo entre dos conjuntos recibe el nombre de isomorfismo entre los mismos.

Es decir, la aplicación f entre A y A' es un isomorfismo $\iff$

$$\iff \left\{\begin{array}{l} \text{f es homomorfismo y} \\ \text{f es biyectiva} \end{array}\right.$$

O sea: f es isomorfismo $\iff$

$\iff \exists f \,/\, f(A) = A'$ y $f^{-1}(A') = A$, $\forall a \, \forall b \in A: f(a \top b) = f(a) \perp f(b)$

En otros términos, un isomorfismo implica una correspondencia biunívoca entre los conjuntos en la que siguen siendo homólogos los compuestos de elementos homólogos.

Definición

Se dice que se confiere una estructura a un conjunto, cuando entre sus elementos se definen relaciones y leyes de composición.

Una estructura matemática quedará entonces definida por el sistema de axiomas que caractericen las relaciones y las operaciones que se incorporan al conjunto.

Introducido así el concepto de estructura, puede extenderse el de isomorfismo antes definido, enriqueciéndose el significado de ese término, con la introducción previa de la siguiente:

Definición

Dados los conjuntos A y A′ en los cuales se han definido relaciones binarias R y R′, respectivamente, se dice que una aplicación biyectiva entre A y A′ es un isomorfismo para esas relaciones binarias si y sólo si toda cupla de A^2 perteneciente a R tiene por imagen una cupla de A'^2 perteneciente a R′.

Es decir:

$$A \wedge A' \text{ son isomorfos respecto de } R \wedge R' \Longleftrightarrow$$

$$\exists f \,/\, A \overset{f}{\longleftrightarrow} A' \wedge \forall a \, \forall b \in A \,/\, a\,R\,b \Longrightarrow f(a)\,R'\,f(b)$$

Definición

Dos conjuntos A y A′ a los cuales relaciones binarias R y R′ y leyes de composición $\top$ y $\top'$, $\perp$ y $\perp'$, respectivamente, les confieren determinadas estructuras matemáticas, se dicen isomorfos respecto de esas estructuras si y sólo si existe, al menos, una aplicación que sea un isomorfismo para esas relaciones y para tales leyes de composición.

Consecuencia

Si los conjuntos A y A′ en los cuales se han definido ciertas relaciones binarias y leyes de composición en igual número, son isomorfos para esas relaciones y leyes, resulta:

1. **A toda igualdad entre elementos de A, compuestos por una ley de A, corresponde una igualdad entre las respectivas imágenes en A′, compuestas por la ley correspondiente en A′.**
2. **Toda propiedad de una ley de A, pertenece a la ley correspondiente de A′.**
3. **Las relaciones binarias homólogas gozan de las mismas características.**
4. **Las estructuras que adquieren los conjuntos A y A′ como consecuencia de esas relaciones o leyes son idénticas.**

Finalmente resulta entonces:

> **"Los conjuntos A y A' son dos realizaciones concretas de una misma estructura abstracta cuyas propiedades y características podrán ser investigadas y desarrolladas indistintamente sobre A o sobre A', puesto que el isomorfismo garantiza la conservación de los resultados".**

En la práctica se suele considerar como idénticos los conjuntos isomorfos, pero en realidad, como se ha dicho y en la medida en que se considera el punto de vista de la pura teoría de conjuntos, los mismos gozan, integralmente, de las mismas propiedades.

La importancia matemática de los isomorfismos, aparte de la puntualizada relativa a la elección del modelo conveniente a una estructura, se manifiesta en la consecuencia de su aplicabilidad a los conceptos definidos por abstración. En efecto, si dos conceptos son definidos por ese camino a partir de conjuntos que resultan isomorfos para las relaciones y operaciones que caracterizan esos conceptos, podemos decir que los mismos corresponden esencialmente a **una única idea.**

Ejemplo

Sea $A = \{0, 1, 10, 11, 100, 101, 110, 111, 1000, \ldots\ldots\}$
$A' = \{0, 1, 2, 3, 4, 5, 6, 7, 8, \ldots\ldots\}$
$R = <$

Leyes: adición y multiplicación.

De inmediato se observa que puede establecerse la siguiente biyección:

$$\begin{array}{ccc}
 & f & \\
0 & \longleftrightarrow & 0 \\
1 & \longleftrightarrow & 1 \\
10 & \longleftrightarrow & 2 \\
11 & \longleftrightarrow & 3 \\
\ldots & \ldots & \ldots \\
1000 & \longleftrightarrow & 8 \\
1001 & \longleftrightarrow & 9 \\
1010 & \longleftrightarrow & 10 \\
1011 & \longleftrightarrow & 11 \\
1100 & \longleftrightarrow & 12 \\
1101 & \longleftrightarrow & 13 \\
1110 & \longleftrightarrow & 14 \\
1111 & \longleftrightarrow & 15 \\
\ldots & \ldots & \ldots
\end{array}$$

Que es un isomorfismo para la relación de menor y las operaciones de adición y multiplicación.

Los conjuntos A y A' son dos modelos concretos de una misma estructura abstracta. Y en efecto, no son más que la expresión en los sistemas de numeración binaria y decimal, respectivamente, del conjunto de los números naturales.

EJERCICIOS

1. — *En el conjunto N de los números naturales se considera la ley:*

$$a * b = \frac{a + b}{2}$$

¿Es ésta una ley de composición interna en N?
Estudiar la conmutatividad y la asociatividad.

2. — *En el conjunto de los números naturales se consideran las dos leyes siguientes:*

$$a * b = a + 2b$$
$$a \circ b = 2ab$$

Demostrar:

a) *que la primera ley no es conmutativa ni asociativa.*
b) *que la segunda ley es conmutativa, asociativa y distributiva respecto de la primera.*

3. — *Discutir las mismas propiedades del ejercicio anterior para las siguientes leyes:*

$$a * b = a + b^2$$
$$a \circ b = ab^2$$

4. — *Análogamente para las leyes:*

$$a * b = a^2 + b^2$$
$$a \circ b = a^2b^2$$

5. — *En el conjunto* $A = \{0, 1, 2, \ldots, 9\}$ *se define la siguiente ley:*

$a * b = a + b \quad$ si $a + b < 10$
$a * b = a + b - 10 \quad$ si $a + b \geqslant 10$

Demostrar:

a) *la ley* $*$ *es de composición interna.*
b) *es conmutativa*
c) *es asociativa*
d) *admite elemento neutro*
e) *todo elemento de A, tiene simétrico en A.*

6. — *En el conjunto Z de los números enteros se define la ley:*

$$a * b = a \cdot b + a + b$$

Demostrar:

a) *la ley es conmutativa.*
b) *es asociativa*
c) *0 es el elemento neutro*
d) *para* $a \neq 0$ *no existe elemento simétrico*
e) *Todos los elementos de Z son regulares, salvo* $a = -1$

7. — *En el conjunto de los números racionales Q, se define la ley:*

$$a * b = a + \frac{1}{b}$$

Demostrar que no es asociativa.

8. — *Demostrar que todo elemento de un conjunto que admite simétrico para una ley* $*$ *asociativa es regular.*

9. — *Si a' y b' son los simétricos de a y b, respectivamente, para una ley asociativa, demostrar:*

$$(a * b)' = b' * a'$$

10. — *Sean las simetrías axiales $S(e_1)$ y $S(e_2)$, donde $e_1 \parallel e_2$*
Determinar la aplicación compuesta $S(e_1) \circ S(e_2)$

11. — *Demostrar que el conjunto de lados de un triángulo es isomorfo con el conjunto de ángulos del mismo para la relación de orden menor o igual.*

12. — *Se dan los conjuntos:*

$$A = \{0, 1, 2, 3, \dots n, \dots.\}$$
$$A' = \{0, 1\}$$

Y se define la aplicación $A \xrightarrow{f} A'$ /

$$\forall n \in A \text{ y } n \text{ par: } n \xrightarrow{f} 0$$
$$\forall n \in A \text{ y } n \text{ impar: } n \xrightarrow{f} 1$$

Demostrar que f es un homomorfismo para la multiplicación.

13. — *Demostrar que la aplicación anterior no es un homomorfismo para la adición.*

CAPITULO V

Estructuras algebraicas

En el capítulo anterior se introdujo el concepto de estructura conferida a un conjunto por relaciones y leyes de composición definidas entre los elementos del mismo. De manera fundamental, las estructuras matemáticas dependen de la o de las operaciones que se establezcan "a priori" en los conjuntos que se manejan, y el cumplimiento de determinadas propiedades para los mismos permite caracterizar tales estructuras.

El objetivo de este capítulo es, justamente, analizar, a partir de sistemas axiomáticos, las estructuras algebraicas más importantes y algunas propiedades generales en los mismos, las que facilitan, de manera notable, los estudios especiales que de esas configuraciones encaran las diferentes ramas de la matemática.

1. GRUPOS

Definición

Una ley de composición interna $*$ definida en un conjunto G, confiere al mismo una estructura de grupo si y sólo si dicha ley es asociativa, existe elemento neutro perteneciente al conjunto y todo elemento del mismo posee un simétrico perteneciente a él.

Es decir que dado $G = \{x, y, z, t, \ldots\}$ y una ley $*$, la estructura de grupo queda definida por los cuatro axiomas siguientes:

G_1: $\forall x, \forall y \in G, \exists z \in G / x * y = z$

G_2: $\forall x, \forall y, \forall z \in G : (x * y) * z = x * (y * z)$

G_3: $\exists e \in G / \forall x \in G : e * x = x * e = x$

G_4: $\forall x \in G, \exists x' \in G / x * x' = x' * x = e$

En tales condiciones el grupo que resulta suele designarse por la misma letra G, o decirse que el conjunto G es un grupo, pero con todo rigor debe entenderse que el grupo es una cupla integrada por G y la operación estrella:

$$\text{Grupo} = [(G, *) \,/\, * \text{ satisface } G_1, G_2, G_3 \text{ y } G_4]$$

Definición

Un conjunto G adquiere una estructura de grupo conmutativo o abeliano si y sólo si (G, *) es un grupo y la ley * es conmutativa.

Es decir, para que exista grupo abeliano, además de los axiomas G_1, G_2, G_3 y G_4 debe verificarse el siguiente:

$$G_5\!: \ \forall x, \forall y \in G\!: \ x * y = y * x$$

Ejemplos

a) El conjunto Z de los números enteros y la ley adición forman un grupo abeliano, usualmente llamado grupo aditivo, cuyo elemento neutro es el número cero.

b) El conjunto de todos los vectores de un plano, de origen O y la ley $\vec{x} + \vec{y} = \vec{z}$ *(donde* $\vec{z}$ *se obtiene por la conocida regla del paralelogramo) forman grupo abeliano.*

c) El conjunto $G = \{-1, 1\}$ *y la ley usual de la multiplicación forman grupo abeliano.*

Observación

Todo grupo definido por la ley multiplicación, o cualquiera otra no expresamente anotada, se suele denominar grupo multiplicativo, en tanto que se reserva el nombre de grupo aditivo a los abelianos para leyes de adición.

2. PROPIEDADES DE LOS GRUPOS

I. — **En todo grupo el elemento neutro es único.**

Es simplemente el corolario de la definición del neutro del capítulo anterior (pág. 72).

II. — **El simétrico de un elemento es único.**

Es el teorema del simétrico en una ley asociativa (pág. 74).

III. — **Todos los elementos de un conjunto con estructura de grupo son regulares para la ley que lo define.**

Debe demostrarse:

$$a * b = a * c \Rightarrow b = c \qquad (1)$$

y $$b * a = c * a \Rightarrow b = c \qquad (2)$$

Compongamos por la izquierda el antecedente de la implicación (1), con a', simétrico de a:

$$a' * (a * b) = a' * (a * c) \Rightarrow \text{ ley asociativa}$$
$$\Rightarrow (a' * a) * b = (a' * a) * c \Rightarrow \text{ def. de simétrico}$$
$$\Rightarrow e * b = e * c \Rightarrow \text{ def. de neutro}$$
$$\Rightarrow b = c$$

Y de análoga manera se demuestra la implicación (2)

Corolario

En todo grupo es válida la propiedad cancelativa.

Lo garantiza la propiedad III.

IV. — **En todo grupo, las ecuaciones:**

$$a * x = b \quad ; \quad y * a = b$$

admiten siempre, cada una, una solución única.

Consideremos la primera ecuación y compongamos por la izquierda sus dos miembros con el simétrico de a : a'.

$$a' * (a * x) = a' * b \Rightarrow \text{ ley asociativa}$$
$$\Rightarrow (a' * a) * x = a' * b \Rightarrow \text{ def. de simétrico}$$
$$\Rightarrow e * x = a' * b \Rightarrow \text{ def. de neutro}$$
$$\Rightarrow x = a' * b$$

Y como por definición de grupo,

$$\forall a \in G, \exists a' \in G \text{ y } a' * b = c \in G,$$

resulta que existe siempre $c = a' * b$ que satisface la ecuación, o sea que es solución de la misma.

Es decir:

$$a * x = b \Rightarrow x = a' * b$$

donde la unicidad de la solución está garantizada por la unicidad del simétrico.

Análogamente se procedería con la segunda ecuación.

Observación

Si G es un grupo aditivo, entonces la ecuación:

$$a * x = b, \quad \text{se expresa por} \quad a + x = b$$

y según la solución general, obtenida a través de la propiedad IV:

$$x = b + a'$$

Pero el simétrico de a: a', para la adición es el opuesto $-a$, luego

$$x = b + (-a) \tag{1}$$

Por otra parte, una expresión del tipo:

$$a + x = b$$

permite definir una operación inversa de la adición, la sustracción:

$$x = b - a \Leftrightarrow a + x = b \tag{2}$$

Y de (1) y (2):

$$b - a = b + (-a) \tag{3}$$

O sea, en un grupo aditivo siempre puede definirse la sustracción, dependiente de la adición, puesto que según (3) la sustracción entre dos elementos de un grupo es simplemente la adición del primero (minuendo) y el opuesto del segundo (sustraendo). La sustracción a su vez, resulta una ley de composición interna.

De idéntica manera un grupo multiplicativo permite siempre introducir la operación división como inversa de la que definió el grupo y en tal caso dividir dos elementos de un grupo multiplicativo equivale a multiplicar el primero por el recíproco del segundo.

Ejemplo

El conjunto de los números racionales, excluido el cero: Q^* *y la ley:* $\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$ *forman un grupo abeliano, donde el inverso de un elemento* $\frac{a}{b}$ *resulta ser el racional* $\frac{b}{a}$.

De acuerdo con la observación anterior, en el conjunto Q^* *es posible siempre la división entre dos elementos cualesquiera de* Q^* *y el cociente se obtendrá multiplicando el primer número (dividendo) por el recíproco del segundo (divisor)*

Es decir:

$$\frac{m}{n} : \frac{p}{q} = \frac{m}{n} \cdot \left(\frac{p}{q} \right)' = \frac{m}{n} \cdot \frac{q}{p}$$

$$\frac{m}{n} : \frac{p}{q} = \frac{m \cdot q}{n \cdot p}$$

resultando la conocida regla elemental del cociente obtenido a través de los productos cruzados.

3. GRUPOS FINITOS

Definición

Un grupo es finito si el conjunto G que lo integra tiene un número finito de elementos, número que recibe el nombre de orden del grupo.

Introduciremos uno de los grupos finitos importantes de la matemática, justamente el que dio origen a las teorías de grupo a partir de los trabajos iniciales del gran matemático francés Evaristo Galois, proseguidos por el no menos famoso matemático noruego Niels Abel: el llamado grupo de sustituciones.

Definición

Dado un conjunto finito A, de n elementos, se llama permutación de A a todo ordenamiento estricto de los elementos de A.

Si $A = \{a, b, c, d\}$, una permutación de A es el mismo conjunto A, pero cuyos elementos se han ordenado, por ejemplo, de la siguiente manera:

$$A = \{b, a, c, d\}$$

Resulta que dos permutaciones de un conjunto sólo difieren en el orden en que se consideran los mismos elementos, a los cuales en un ordenamiento de partida podría asignárseles subíndices naturales $1, 2, \ldots, n$. En consecuencia, formar las permutaciones de un conjunto es encontrar todas las aplicaciones biyectivas posibles del conjunto dado sobre el conjunto de números naturales comprendidos entre 1 y n. Y si se desea el número total de las permutaciones de ese conjunto A, habrá que determinar el número total de biyecciones que puedan definirse entre:

$$A = \{a, b, c, d, \overset{n}{\ldots\ldots}, m\} \quad \text{y} \quad B = \{1, 2, 3, \ldots, n\}$$

Existen, en primer lugar, n biyecciones (pues hay n elementos) que aplican los elementos de A sobre el número 1 de B, puesto que:

$$n \left\{ \begin{array}{l} a \xrightarrow{f_1} 1 \\ b \xrightarrow{f_2} 1 \\ c \xrightarrow{f_3} 1 \\ \cdots\cdots \\ m \xrightarrow{f_n} 1 \end{array} \right.$$

Si consideramos la f_1, existen $n-1$ biyecciones que aplican los elementos diferentes de a sobre el número 2:

$$(n-1) \left\{ \begin{array}{l} a\,b \xrightarrow{f'_1} 1\,2 \\ \quad\underbrace{\qquad}_{f_1} \\ a\,c \xrightarrow{f'_2} 1\,2 \\ \quad\underbrace{\qquad}_{f_1} \\ \cdots\cdots\cdots \\ a\,m \xrightarrow{f'(n-1)} 1\,2 \\ \quad\underbrace{\qquad}_{f_1} \end{array} \right.$$

Y recurrentemente, la f'_1 origina $n-2$ biyecciones que aplican los elementos diferentes de a y b sobre el 3, etc. de modo tal que el número total de aplicaciones de A sobre B es:

$$n(n-1)(n-2)\ldots[n-(n-1)] = n(n-1)(n-2)\ldots 2\cdot 1$$

que es la expresión del factorial de n. Y si indicamos por P_n el número de permutaciones de un conjunto A, de n elementos, se tendrá la clásica fórmula de las permutaciones del álgebra combinatoria:

$$P_n = n\,!$$

Definición

Se llama sustitución a toda aplicación biyectiva de un conjunto finito sobre sí mismo.

Si s es la sustitución:

$$A \xrightarrow{s} A$$

Entonces una sustitución transforma una permutación del conjunto A en otra permutación de A.

Definición

Se llama sustitución idéntica a la sustitución que transforma una permutación de A en la misma permutación.

Ejemplo

Sea

$$A = \{1, 2, 3\} \quad \text{el conjunto dado.}$$

Las permutaciones de A, que posee tres elementos, son 6 (3! = 6):

$$\{1, 3, 2\} \; ; \; \{2, 1, 3\} \; ; \; \{2, 3, 1\} \; ; \; \{3, 1, 2\} \; ; \; \{3, 2, 1\} \; ; \; \{1, 2, 3\}$$

Y en consecuencia las sustituciones posibles son:

$$\{1, 2, 3\} \xrightarrow{s_1} \{1, 2, 3\}$$
$$\{1, 2, 3\} \xrightarrow{s_2} \{1, 3, 2\}$$
$$\{1, 2, 3\} \xrightarrow{s_3} \{2, 1, 3\}$$
$$\{1, 2, 3\} \xrightarrow{s_4} \{2, 3, 1\}$$
$$\{1, 2, 3\} \xrightarrow{s_5} \{3, 1, 2\}$$
$$\{1, 2, 3\} \xrightarrow{s_6} \{3, 2, 1\}$$

Donde s_1 es la sustitución idéntica.

Notación

Se suele indicar una sustitución mediante una fracción simbólica, cuyo numerador es la permutación de partida y el denominador la permutación transformada.

Es decir la s_3 del ejemplo anterior se indicaría:

$$s_3 = \begin{pmatrix} 1, 2, 3 \\ 2, 1, 3 \end{pmatrix}$$

Esta notación permite observar claramente que la sustitución s_3 es una biyección que asigna como homólogo del elemento 1 el 2; como imagen del 2 el 1, y como imagen del 3 el mismo 3.

Y en consecuencia, las seis fracciones simbólicas siguientes son expresiones de la misma sustitución s_3, ya que todas ellas conservan las imágenes que origina s_3 como aplicación:

$$s_3 = \begin{pmatrix} 1, 2, 3 \\ 2, 1, 3 \end{pmatrix} = \begin{pmatrix} 1, 3, 2 \\ 2, 3, 1 \end{pmatrix} = \begin{pmatrix} 2, 1, 3 \\ 1, 2, 3 \end{pmatrix} = \begin{pmatrix} 2, 3, 1 \\ 1, 3, 2 \end{pmatrix} = \begin{pmatrix} 3, 1, 2 \\ 3, 2, 1 \end{pmatrix} = \begin{pmatrix} 3, 2, 1 \\ 3, 1, 2 \end{pmatrix}$$

Corolarios

I. — **La aplicación compuesta de dos sustituciones de un mismo conjunto es otra sustitución.**

En efecto, como las sustituciones son aplicaciones biyectivas, la composición de dos sustituciones es otra aplicación biyectiva de A en A, según se ha visto en el capítulo anterior. Por otra parte, si s_i transforma una permutación P_a del conjunto A, en otra P_b, y la sustitución s_j transforma la P_b en P_c, la aplicación compuesta es la aplicación que transforma la P_a en P_c, que es una sustitución s_k.

Es decir:

$$s_i = \begin{pmatrix} P_a \\ P_b \end{pmatrix} \quad ; \quad s_j = \begin{pmatrix} P_b \\ P_c \end{pmatrix}$$

$$s_j \circ s_i = s_k = \begin{pmatrix} P_a \\ P_c \end{pmatrix}$$

II. — **la aplicación inversa de una sustitución es otra sustitución.**

Como s_i es una aplicación biyectiva, existe la aplicación inversa s_i^{-1}. Y si s_i transforma la permutación P_a en P_b, la s_i^{-1} transforma P_b en P_a. Luego s_i^{-1} es una sustitución.

III. — **El número de sustituciones de un conjunto finito de** n **elementos es** n!

Teorema

El conjunto de todas las sustituciones de un conjunto finito y la ley de composición de las mismas como aplicaciones forman un grupo finito.

Sea $A = \{a, b, c, d, \overset{n}{\ldots\ldots}, m\}$ y designemos por $\mathcal{G}$ el conjunto de las sustituciones de A: $\mathcal{G} = \{s_i\}$

Probamos que se satisfacen los cuatro axiomas de grupo:

$$G_1: \forall s_i, \forall s_j \in \mathcal{G}, \exists s_k \in \mathcal{G} \,/\, s_j \circ s_i = s_k$$

Se satisface por corolario I.

$$G_2: \forall s_i, \forall s_j, \forall s_k \in \mathcal{G}: (s_k \circ s_j) \circ s_i = s_k \circ (s_j \circ s_i)$$

Se satisface, pues la composición de aplicaciones es siempre asociativa (capítulo anterior).

$$G_3: \text{ Existe } s_e \in \mathcal{G} \,/\, \forall s_i \in \mathcal{G}: s_e \circ s_i = s_i \circ s_e = s_i$$

Y, en efecto, existe s_e por definición de sustitución idéntica.

$$G_4: \forall s_1 \in \mathcal{G}, \exists s_1' \in \mathcal{G} / s_1' \circ s_1 = s_1 \circ s_1' = s_e$$

Se satisface según el corolario II.

Como además el conjunto $\mathcal{G}$ tiene un número finito de elementos:

$$(\mathcal{G}, \circ) \text{ es un grupo finito}$$

El grupo $\mathcal{G}$, de las sustituciones de un conjunto finito A, que reviste gran importancia en el desarrollo de múltiples teorías matemáticas, recibe también el nombre de **Grupo simétrico a n variables.**

4. SUBGRUPOS

Definición

Un conjunto H incluido en un grupo G, se denomina subgrupo de G si y sólo si no es vacío y es un grupo para la misma ley de composición de G.

Es decir: $(G, *)$ grupo

$$(H, *) \text{ subgrupo de } G \iff H \neq \emptyset \,;\, H \subseteq G \text{ y } (H, *) \text{ es un grupo}$$

Ejemplo

El conjunto Z de los números enteros y la operación adición, forman un subgrupo del grupo de los números racionales para la misma operación.

Corolario

Todo grupo G admite por lo menos dos subgrupos, él mismo y el conjunto unitario constituido por el elemento neutro de G.

5. SEMIGRUPOS

Definición

Se llama semigrupo a la estructura que adquiere un conjunto provisto de una ley de composición interna y asociativa.

Se suele designar también a los semigrupos: **grupoides o monoides.** Es decir que los axiomas de semigrupo son:

$$S_1: \forall x, \forall y \in S: x * y \in S$$

$$S_2: \forall x, \forall y, \forall z, \in S: (x * y) * z = x * (y * z)$$

Ejemplo

El conjunto de todas las aplicaciones de un conjunto A en otro B es un semigrupo para la ley de composición de aplicaciones.

En efecto, según se ha visto, la composición de aplicaciones es otra aplicación y tal composición satisface siempre a la propiedad asociativa.

6. GRUPOS ORDENADOS

Definición

Se llama grupo ordenado a todo grupo abeliano G, provisto de una relación de orden total ($\leqslant$), que satisface la relación siguiente:

$$[\forall z \in G \wedge \forall x,\ \forall y \in G / x \leqslant y] \Rightarrow x * z \leqslant y * z$$

Observación

La condición $x \leqslant y \Rightarrow x * z \leqslant y * z$, suele expresarse diciendo que el orden es invariante para toda traslación.

Ejemplo

La relación de menor o igual asigna estructura de grupo ordenado a los grupos aditivos de los números enteros, racionales y reales, respectivamente.

Definición

Se llaman elementos positivos de un grupo ordenado a aquellos que cumplen la condición:

Si e es el elemento neutro de G, $x \in G$ es positivo $\Leftrightarrow e < x$

Definición

Todo elemento que no es positivo, ni neutro, se llama negativo.

7. ANILLOS

Una ley de composición interna definida entre los elementos de un conjunto ha permitido introducir un primer tipo de estructura algebraica, la de grupo, con sus propiedades características. Nada impide pensar que tal estructura inicial pueda ser sucesivamente ampliada mediante la consideración simultánea de una segunda ley de composición interna introducida en el mismo conjunto.

Definición

Un conjunto A y dos leyes de composición interna definidas en A, constituyen un anillo, si y sólo si la primera operación confiere al conjunto una estructura de grupo abeliano y la segunda es asociativa y doblemente distributiva respecto de la primera.

Es decir que dado $A = \{x, y, z, t, \ldots\ldots\}$ y las operaciones $*$ y $\circ$, una estructura de anillo queda definida por los cuatro axiomas siguientes:

Operación $*$

$$A_1: (A, *) \text{ es un grupo abeliano}$$

Operación $\circ$

$$A_2: \forall x,\ \forall y \in A, \exists t \in A / x \circ y = t$$

$$A_3: \forall x,\ \forall y,\ \forall z \in A: (x \circ y) \circ z = x \circ (y \circ z)$$

Operación $\circ$ respecto de $*$

$$A_4: \forall x,\ \forall y,\ \forall z \in A: x \circ (y * z) = (x \circ y) * (x \circ z)$$

$$(y * z) \circ x = (y \circ x) * (z \circ x)$$

En tales condiciones el anillo que resulta suele designarse con la misma letra A, o decirse que el conjunto A es un anillo, pero, insistimos, desde un punto de vista absolutamente riguroso debe entenderse que el anillo es una terna integrada por A y las operaciones estrella y círculo:

$$\text{Anillo} = [(A, *, \circ) / * \text{ satisface } A_1, \circ \text{ a } A_2 \text{ y } A_3, * \text{ y } \circ \text{ a } A_4]$$

Definición

Un conjunto A adquiere una estructura de anillo conmutativo si y sólo si $(A, *, \circ)$ es un anillo y la ley $\circ$ es conmutativa.

Es decir, debe cumplirse un quinto axioma:

$$A_5: \forall x,\ \forall y \in A: x \circ y = y \circ x$$

Corolario

Si un anillo es conmutativo, la doble distributividad de la segunda operación respecto de la primera es cierta si se verifica simplemente a la izquierda o a la derecha.

Definición

Si la segunda ley posee elemento neutro en A, tal elemento se llama unidad del anillo y el anillo mismo, unitario.

Ejemplos

a) El conjunto Z de los números enteros y las leyes de adición y multiplicación constituyen un anillo.

En efecto, las propiedades conocidas de los enteros nos prueban que se satisfacen los axiomas de anillo, el que es además conmutativo y unitario. (Cero es el neutro para la primera operación —suma— y 1 el neutro de la segunda — producto).

b) El conjunto de los números pares con las leyes usuales de la adición y multiplicación constituyen un anillo no unitario.

La adición y multiplicación son leyes de composición interna en el conjunto dado puesto que

$$\text{par} + \text{par} = \text{par}; \quad \text{par} \times \text{par} = \text{par}$$

Y es entonces inmediato que se satisfacen los axiomas de anillo conmutativo.

En cambio tal anillo no resulta unitario ya que no existe elemento neutro para la multiplicación (el neutro sería el número 1, que no pertenece al conjunto que se maneja, por no ser par).

8. PROPIEDADES DE LOS ANILLOS

Puesto que un anillo es un grupo abeliano para la primera operación, se conservarán en el mismo las propiedades generales analizadas en los grupos, referidas siempre a esa operación. Pero la presencia de una segunda ley introduce algunas otras propiedades de gran interés.

I. — **En todo anillo el compuesto de cualquier elemento, a través de la segunda operación con el neutro de la primera, es este elemento neutro.**

Si es e el neutro de la primera operación, debe demostrarse:

$$\forall a \in A \Rightarrow a \circ e = e \;\; \text{y} \;\; e \circ a = e$$

Por ser e neutro: $\forall b \in A$: $b * e = b$

Componiendo con a a la izquierda por la segunda ley:

$$a \circ (b * e) = a \circ b$$

Por A_4:

$$(a \circ b) * (a \circ e) = a \circ b$$

Y por definición de neutro:

$$(a \circ b) * (a \circ e) = (a \circ b) * e$$

Pero para la primera operación todos los elementos son regu a-res por constituir grupo abeliano:

$$(a \circ e) = e$$

Y de manera análoga se probaría que $e \circ a = e$.

Observación

Esta sencilla propiedad demuestra, de una vez por todas, que el producto por el número cero es siempre cero, en todos los conjuntos de números que forman anillo.

II. — Llamando a' al opuesto de a según $*$, b' al de b y $(a \circ b)'$ al de $(a \circ b)$,

se desea probar:

II_a $a' \circ b = (a \circ b)'$, $\qquad$ II_b $a \circ b' = (a \circ b)'$

Que es equivalente a:

II_a $(a' \circ b) * (a \circ b) = e$ $\qquad$ II_b $(a \circ b') * (a \circ b) = e$

Pero, en II_a

$$(a' \circ b) * (a \circ b) = (a' * a) \circ b \quad \text{por } A_4$$
$$(a' \circ b) * (a \circ b) = e \circ b \quad \text{por } A_1$$

Y por la propiedad I:

$$(a' \circ b) * (a \circ b) = e$$

Análogamente se satisface II_b.

III. — Con los mismos significados se desea probar:

$$a' \circ b' = a \circ b$$

Por la propiedad anterior:

$$a' \circ b' = (a \circ b')' \qquad (1)$$

Por II_b:

$$(a \circ b')' = [(a \circ b)']'$$

Y por propiedad del opuesto de un opuesto:

$$(a \circ b')' = a \circ b \qquad (2)$$

De (1) y (2):

$$a' \circ b' = a \circ b$$

Observación

Si los anillos son numéricos,

$$a' = -a; \; b' = -b \text{ y } (a \cdot b)' = -(a \cdot b)$$

y las propiedades se traducen:

$$(-a) \cdot b = -(a \cdot b) \wedge a \cdot (-b) = -(a \cdot b)$$
$$(-a) \cdot (-b) = a \cdot b$$

Que demuestran también de una vez por todas la famosa regla de los signos, sin necesidad siquiera de hablar de elementos negativos o positivos.

9. SUBANILLOS

Definición

Un conjunto A′ incluido en un anillo A es un subanillo de A si es un subgrupo para la primera ley y es cerrado para la segunda operación.

Es inmediato que en tales condiciones un subanillo es también un anillo.

Ejemplo

Sea Z el conjunto de los números enteros y

$$A' = \{x \,/\, x \in Z \wedge x = \text{múltiplo de } a\}$$

Como la suma de dos múltiplos de un mismo número es también múltiplo de dicho número y el opuesto de un múltiplo es también un múltipo, es inmediato que el conjunto A′ es un subgrupo del grupo aditivo de los números enteros. Y como además el producto de dos múltiplos de un número es otro múltiplo del mismo, la segunda operación es cerrada en A′.

Luego, de acuerdo con la definición.

$$(A', +, \times) \text{ es un subanillo de } (Z, +, \times)$$

10. ANILLOS DE INTEGRIDAD

En un anillo la primera ley de composición goza, según se ha visto, de la propiedad cancelativa, ya que por estructurar un grupo todos los elementos son regulares.

No ocurre lo propio con la segunda ley, que puede o no ser simplificable. La consideración de esos dos casos posibles es de gran importancia, pues la imposibilidad de simplificar no depende solamente de estar operando con el número cero.

Es claro que la igualdad:

$a \cdot 0 = b \cdot 0$, no autoriza a concluir que $a = b$.

Pero aun para elementos no nulos la expresión:

$a \cdot c = b \cdot c$ y $c \neq 0$ puede no implicar $a = b$.

En efecto, tal circunstancia se encuentra por ejemplo en el producto de matrices cuadradas. Recordemos el significado de producto de dos matrices (por comodidad tomamos matrices cuadradas 2×2).

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix} \cdot \begin{bmatrix} m & p \\ n & q \end{bmatrix} = \begin{bmatrix} am + cn & ap + cq \\ bm + dn & bp + dq \end{bmatrix}$$

Aplicando esta definición, efectuemos los siguientes productos:

$$\begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 4 & 4 \\ 4 & 4 \end{bmatrix}$$

y

$$\begin{bmatrix} 5 & -1 \\ 5 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 4 & 4 \\ 4 & 4 \end{bmatrix}$$

De donde resulta:

$$\begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 5 & -1 \\ 5 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

Y es obvio que de esa igualdad no podrá extraerse que el primer factor del primer miembro es igual al primero del segundo miembro puesto que:

$$\begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix} \neq \begin{bmatrix} 5 & -1 \\ 5 & -1 \end{bmatrix}$$

Esta conclusión justifica entonces la diferenciación entre estructuras con segunda ley simplificable o no, aún excluidos los elementos nulos. Y por ello la siguiente:

Definición

Se denomina anillo de integridad a todo anillo cuya segunda ley de composición es simplificable cuando se excluyen los elementos nulos.

Es decir que para definir un anillo de integridad habrá que introducir el siguiente axioma:

A_6: $\forall a, \forall b, \forall c, \in A / c \neq 0 : a \circ c = b \circ c \Leftrightarrow a = b$

Ejemplo

El ya mencionado ejemplo de los números enteros es un anillo de integridad de acuerdo con las conocidas propiedades de la adición y la multiplicación.

Contraejemplo

Para las matrices cuadradas se define la adición:

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix} + \begin{bmatrix} m & p \\ n & q \end{bmatrix} = \begin{bmatrix} a + m & c + p \\ b + n & d + q \end{bmatrix}$$

Puede demostrarse que tal operación confiere estructura de grupo abeliano. Y la operación multiplicación, antes definida, completa una estructura de anillo no conmutativo. Pero, como se ha visto, tal anillo no es de integridad.

11. DOMINIOS DE INTEGRIDAD

Al introducir el concepto de anillo se consideró el caso particular del anillo unitario, es decir, el que contiene el elemento neutro o unidad de la segunda operación. La simultaneidad de los conceptos de integridad y unitario permite introducir lo siguiente:

Definición

Se llama dominio de integridad a todo anillo de integridad que es al mismo tiempo unitario.

Es decir, la definición de un dominio de integridad obliga a la inclusión de un nuevo axioma:

$$A_7: \exists s \in A \,/\, \forall x \in A: s \circ x = x \circ s = x$$

Ejemplo

El conjunto Z es evidentemente un dominio de integridad (por otra parte, es el primero que aparece en las estructuras de números).

Observación

El anillo de matrices cuadradas 2×2 es unitario ya que puede comprobarse de inmediato que la matriz:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

es elemento neutro para la multiplicación.

Pero tal anillo no puede transformarse en dominio, por no ser de integridad.

12. CUERPOS

El recuerdo de las propiedades elementales de la aritmética de los números racionales, reales y complejos nos hace observar que la adición y la multiplicación en cada uno de los conjuntos que ellos determinan configuran una estructura "más avanzada" que la de un dominio, puesto que todo racional, real o complejo no nulo tiene siempre un recíproco, condición no exigida hasta ahora.

El agregado de esa nueva condición a los axiomas anteriores introduce, entonces, una nueva estructura algebraica, caracterizada por la siguiente:

Definición

Se llama cuerpo a la estructura que adquiere un conjunto K en el que se han definido dos leyes de composición internas $*$ y $\circ$, tales que la primera confiere a K estructura de grupo abeliano; la segunda, estructura de grupo para los elementos no nulos de K, siendo la operación $\circ$ doblemente distributiva respecto de la $*$.

Es decir, que dado $K = \{x, y, z, t, \ldots\}$ y dos leyes $*$, $\circ$, la estructura de cuerpo queda definida por los axiomas siguientes:

K_1: $(K, *)$ grupo abeliano (axiomas G_1 al G_5)
K_2: $(K^*, \circ)$ grupo, donde K^* es el conjunto de los elementos no nulos de K (axiomas G_1 al G_4)

$$K_3\text{: } \forall x, \forall y, \forall z \in K: \begin{cases} x \circ (y * z) = (x \circ y) * (x \circ z) \\ (y * z) \circ x = (y \circ x) * (z \circ x) \end{cases}$$

Como se ha observado para grupos y anillos, aun cuando se designe el cuerpo por K, el cuerpo es una terna:

$$\text{Cuerpo} = [(K, *, \circ) \ / \text{ se satisfacen } K_1, K_2 \text{ y } K_3]$$

Definición

Un conjunto K adquiere una estructura de cuerpo conmutativo, si y sólo si $(K, *, \circ)$ es un cuerpo y la operación $\circ$ es conmutativa.

Es decir debe verificarse además:

$$K_4\text{: } \forall x, \forall y \in K\text{: } x \circ y = y \circ x$$

Ejemplo

Los números racionales, reales o complejos, forman cuerpo conmutativo para la adición y la multiplicación.

Contraejemplo

Los enteros no forman cuerpo puesto que un entero a carece de recíproco $\left(\frac{1}{a}\right)$ perteneciente a Z, salvo para los valores particulares de $a = 1$ o $a = -1$.

Corolario

Todo cuerpo es un anillo de integridad.

Si $(K, *, \circ)$ es un cuerpo: $(K^*, \circ)$ es un grupo y por propiedad de grupo, todos los elementos de K^* son regulares es decir que en K^* es válida la ley cancelativa, luego:

$(K, *, \circ)$ es un anillo de integridad.

Corolario

Todo dominio de integridad de un número finito de elementos es un cuerpo.

Para demostrar tal enunciado bastará probar que todo elemento no nulo del dominio tiene un simétrico, para la segunda ley, perteneciente al dominio.

Como el número de elementos es finito, si se suprimen los elementos nulos, los restantes son también finitos y podrán designarse:

$$A = \{a_1, a_2, \ldots a_i, a_j, \ldots a_n\}$$

y entre ellos está incluido el elemento unidad que podemos suponer sea el a_1.

Al componer los elementos de A con un a_i, fijo, arbitrario, como A tiene n elementos, se obtendrán n compuestos que, por la ley de composición, son elementos de A. Dos cualesquiera de esos compuestos son diferentes, pues si existiera:

$a_i \circ a_k = a_i \circ a_p$ como $a_i \neq 0$, resultaría $a_k = a_p$ por A_6 (absurdo)

En consecuencia, teniendo A, n elementos (que incluye el a_1) y siendo los compuestos con a_i también n, diferentes entre sí, existe necesariamente un a_j tal que: $a_i \circ a_j = a_1 \Rightarrow a_j = a_i'$

Y el dominio es un cuerpo.

13. SUBCUERPOS

Definición

Un conjunto $K' \neq \varnothing$ incluido en K, que es un cuerpo para las leyes $*$ y $\circ$, es un subcuerpo de K si es también cuerpo para las mismas leyes.

Ejemplo

El cuerpo de los racionales es un subcuerpo del cuerpo de los reales y éste a su vez es un subcuerpo del cuerpo de los complejos.

14. ESPACIOS VECTORIALES

Las estructuras analizadas hasta ahora han sido engendradas por leyes de composición internas, definidas en un conjunto, que satisfacían determinadas propiedades. Habiéndose definido leyes de composición externa para elementos de un conjunto con operadores de otro, como tales conjuntos pueden poseer algunas de las estructuras discutidas, resulta la posibilidad de introducir nuevas estructuras combinadas. Como se verá, este nuevo planteo permitirá llevar a dar forma abstracta general a fundamentales conceptos de la matemática.

Definición

Un conjunto E, que es un grupo abeliano para una operación interna $*$, adquiere una estructura de espacio vectorial sobre un conjunto K, que es un cuerpo para las leyes $\top$ y $\perp$, si existe una ley de composición externa de E sobre K, tal que dicha ley es distributiva respecto de $*$, distributiva respecto de $\top$, asociativa respecto de $\perp$ y admite como elemento neutro el neutro de la operación $\perp$.

Es decir, E es espacio vectorial sobre K, si se satisfacen los siguientes axiomas:

E_1: $(E = \{x, y, z, \dots\}, *)$ grupo abeliano

E_2: $(K = \{\alpha, \beta, \gamma, \dots\}, \top, \perp)$ cuerpo

E_3: $\exists f \,/\, K \times E \xrightarrow{f} E, \forall x \in E, \forall \alpha \in K$ es $\alpha \cdot x \in E$

E_4: $\alpha \cdot (x * y) = \alpha \cdot x * \alpha \cdot y$

E_5: $(\alpha \top \beta) * x = \alpha \cdot x * \beta \cdot x$

E_6: $\alpha \cdot (\beta \cdot x) = (\alpha \perp \beta) \cdot x$

E_7: Si $\mu \in K \,/\, \forall \alpha \in K$: $\mu \perp \alpha = \alpha \perp \mu = \alpha$

Entonces $\forall x \in E$: $\mu \cdot x = x$

Ejemplo

Sea $E = P = \{A(x), B(x), \dots\dots\}$ *conjunto de todos los polinomios de una variable real.*

$*$ *es la suma de polinomios*
$K = R = \{x \,/\, x$ *número real*$\}$
$\top$ *es la adición de reales*
$\perp$ *es la multiplicación de reales*
$\cdot$ *es la multiplicación usual de un número real por un polinomio, es decir, si* $A(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ *y* $\alpha \in K$:
$\alpha \cdot A(x) = \alpha \cdot a_n x^n + \alpha \cdot a_{n-1} x^{n-1} + \dots + \alpha \cdot a_1 x + \alpha \cdot a_0$

La operación externa $\alpha \cdot A(x)$ se suele llamar también producto escalar del polimonio $A(x)$ por el real α.

Con tales elementos se satisfacen de inmediato los siete axiomas relativos a un espacio vectorial.

E_1: $(P, *)$ es grupo abeliano; ello es cierto, pues la suma de polinomios es interna en P, asociativa, admite como elemento neutro el polinomio nulo, y el opuesto de un polinomio cualquiera se obtiene simplemente considerando los opuestos de los coeficientes del polinomio dado.

E_2: $(K, \top, \perp)$ es un cuerpo, en este caso conmutativo.

E_3: $\exists f$: $\alpha \cdot A(x) = B(x)$, según significado de producto escalar.

E_4: $\alpha \cdot [A(x) + B(x)] = \alpha \cdot A(x) + \alpha \cdot B(x)$

E_5: $(\alpha + \beta) \cdot A(x) = \alpha \cdot A(x) + \beta \cdot A(x)$

E_6: $\alpha \cdot [\beta \cdot A(x)] = (\alpha \cdot \beta) \cdot A(x)$

E_7: El neutro de la segunda ley de K es el real 1. Y en tal caso:

$$\forall A(x) \in P : 1 \cdot A(x) = A(x)$$

En consecuencia el conjunto P de polinomios es un espacio vectorial sobre el cuerpo de los números reales.

Definición

Se llama vector a cualquier elemento de un espacio vectorial.

Definición

Si E es un conjunto no vacío incluido en un espacio vectorial $\mathcal{E}$ sobre un cuerpo K y las leyes interna y externa de $\mathcal{E}$, aplicadas en E, dan a E estructura de espacio vectorial, entonces E se llama subespacio vectorial de $\mathcal{E}$.

15. FAMILIA LIBRE. BASE Y DIMENSIÓN DE UN ESPACIO VECTORIAL

Elementos linealmente independientes

Definición

Un elemento x de un espacio vectorial $\mathcal{E}$, se llama combinación lineal de una familia x_i, de elementos de $\mathcal{E}$, si existe un conjunto de operadores $\alpha_i \in K$ (designados con los mismos subíndices de x_i) tal que:

$$x = \Sigma\, \alpha_i \cdot x_i$$

Observación

Si los elementos α_i son todos nulos, resulta $\Sigma\, \alpha_i \cdot x_i = 0$.
En tal caso se suele decir que el elemento 0 es una combinación lineal **trivial** de los x_i.

Corolario

El conjunto $E = \{x / x = \Sigma\, \alpha_i \cdot x_i\}$ **es un subespacio vectorial de** $\mathcal{E}$.

Ello es inmediato, por cuanto la operación interna y externa de $\mathcal{E}$, dan al conjunto de todos los x posibles (incluida la combinación trivial), estructura de espacio vectorial y $E \subseteq \mathcal{E}$.

Definición

Una familia de elementos x_i **perteneciente a un espacio vectorial** $\mathcal{E}$ **sobre un cuerpo K, se llama familia libre o de elementos linealmente independientes si la condición** $\Sigma\, \alpha_i \cdot x_i = 0$ **se cumple, si y sólo si todos los** α_i **son iguales a cero.**

Es decir:

x_i es familia libre si

$$\Sigma\, \alpha_i \cdot x_i = 0 \Leftrightarrow \alpha_i = 0, \quad \forall_i$$

Base de un espacio vectorial

Definición

Se dice que un conjunto E incluido en otro $\mathcal{E}$, **engendra a** $\mathcal{E}$ **si y sólo si todo elemento de** $\mathcal{E}$ **es una combinación lineal de los elementos de E.**

Definición

Se llama base de un espacio vectorial $\mathcal{E}$ **sobre un cuerpo K a toda familia** x_i **perteneciente a** $\mathcal{E}$, **tal que sea de elementos linealmente independientes y engendre a** $\mathcal{E}$.

Es decir:

x_i es una base de $\mathcal{E} \Leftrightarrow$

$$x_i \in \mathcal{E} \wedge [\Sigma\, \alpha_i \cdot x_i = 0 \Rightarrow \forall_i, \alpha_i = 0] \wedge \forall x \in \mathcal{E}: x = \Sigma\, \alpha_i \cdot x_i$$

Definición

Si $\{x_i\}$ es una base y un vector x es de la forma $x = \Sigma\, \alpha_i \cdot x_i$ los elementos α_i se llaman coordenadas o componentes del vector x, y los elementos $\alpha_i x_i$ proyecciones del mismo vector (obsérvese que tales proyecciones son también vectores)

Corolario

Las coordenadas de todo vector x, en una base x_i son únicas.

Sea

$$x = \Sigma\, \alpha_i x_i$$

Supongamos que x admite también coordenadas α_i'. Entonces

$$x = \Sigma\, \alpha_i' x_i$$

Luego:

$$\Sigma\, \alpha_i x_i - \Sigma\, \alpha_i' x_i = 0$$

O sea:

$$\Sigma\, (\alpha_i - \alpha_i') x_i = 0$$

Y como x_i es una base, resulta

$$(\alpha_i - \alpha_i') = 0 \Rightarrow \alpha_i = \alpha_i'$$

Y el sistema α_i es único.

Definición

Si $\mathcal{E}$ es un espacio vectorial sobre un cuerpo K que posee una base de un número finito de elementos, tal número de elementos se llama dimensión de ese espacio.

Ejemplo

En el siguiente ejemplo se pondrán de manifiesto todos los conceptos introducidos precedentemente.

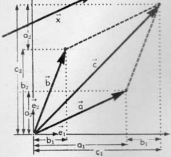
$\mathcal{E} = \{x\,/\,x$ *es vector libre de un plano euclídeo*$\}$
$*$ *es la suma de vectores por regla del paralelogramo.*
$K =$ *cuerpo de los números reales.*
$\top$ *es la adición de números reales*
$\bot$ *es la multiplicación de números reales.*
producto de un número real por un vector.

Con tales elementos probaremos:

1. — $\mathcal{E}$ es un espacio vectorial sobre K.

Ello es inmediato, pues resulta $\mathcal{E}$ un grupo abeliano para la adición de vectores y la ley externa satisface los axiomas de espacio.

2. — Si consideramos un sistema de coordenadas cartesianas en el plano euclídeo de ejes normales x e y, sobre dichos ejes se pueden considerar respectivamente vectores $\vec{e_1}$ y $\vec{e_2}$, a los que suele darse el nombre de versores si sus módulos son iguales a la unidad.



La familia $\{\vec{e_1}, \vec{e_2}\}$ es una familia libre.

En efecto:

$$\Sigma\, \alpha_i \vec{e_i} = \alpha_1 \cdot \vec{e_1} + \alpha_2 \cdot \vec{e_2}$$

y esa expresión será el vector nulo $\vec{x} = \vec{0}$ sólo si son simultáneamente nulos α_1 y α_2.

3. — Todo vector libre del plano es una combinación lineal de $\vec{e_1}$ y $\vec{e_2}$.

En efecto, dado $\vec{x}$ siempre es posible considerar el vector equipolente al dado con origen en O (los vectores equipolentes son vectores libres iguales). Proyectando $\vec{a}$ sobre los ejes, se obtienen proyecciones $\vec{a_1}$ y $\vec{a_2}$, tal que según la ley de adición:

$$\vec{a} = \vec{a_1} + \vec{a_2}$$

Pero, dados $\vec{a_1}$ y $\vec{e_1}$ existe siempre un número real α_1, tales que:

$$\vec{a_1} = \alpha_1 \cdot \vec{e_1}$$

y análogamente:

$$\vec{a_2} = \alpha_2 \cdot \vec{e_2}$$

Luego:

$$\vec{a} = \alpha_1 \cdot \vec{e_1} + \alpha_2 \cdot \vec{e_2}$$

$$\vec{a} = \Sigma\, \alpha_i \vec{e_i}$$

De análoga manera se probaría la relación recíproca.

4. — La familia $E = \{\vec{e_1}, \vec{e_2}\}$ es una base del espacio vectorial que se estudia.

Ya se probó que $\{\vec{e_1}, \vec{e_2}\}$ es una familia libre, que, además, engendra $\mathcal{E}$.

5. — El espacio vectorial de todos los vectores libres del plano euclídeo es de dimensión 2.

En efecto una base es $\{\vec{e}_1, \vec{e}_2\}$, y su número de elementos es 2.

Observación

En el ejemplo concreto anterior, fijada la base $\{\vec{e}_1, \vec{e}_2\}$, todo vector libre del plano es de la forma:

$$\vec{a} = \alpha_1 \vec{e}_1 + \alpha_2 \vec{e}_2$$

Y en consecuencia cada vector $\vec{a}$ queda caracterizado por sus componentes α_i de manera única y recíprocamente. Puede entonces considerarse que las mismas definen al vector $\vec{a}$ y en tal caso:

$$\vec{a} = (\alpha_1; \alpha_2),$$

que permite arribar al concepto abstracto de vector, independiente de significaciones concretas especiales.

EJERCICIOS

1. — *En un grupo abeliano, resolver la ecuación:*

$$x \cdot a \cdot b \cdot x \cdot c = b \cdot x \cdot a$$

2. — *En el conjunto Z de los números enteros, se toma como ley de composición:*

$$x * y = -y$$

Probar que $(Z, *)$ *no es un grupo.*

3. — *En el conjunto de los números reales excluidos 0, —1 y 1 se definen las aplicaciones:*

$$x \xrightarrow{f_1} x \ ; \ x \xrightarrow{f_2} \frac{1}{x} \ ; \ x \xrightarrow{f_3} -x \ ; \ x \xrightarrow{f_4} -\frac{1}{x}$$

Demostrar que el conjunto finito: $A = \{f_1, f_2, f_3, f_4\}$ *es un grupo para la ley de composición de aplicaciones.*

4. — *Sea el conjunto C, cuyos elementos son cuplas de números racionales:*

$$C = \{(a\,;\,b) \,/\, a \wedge b \in Q\}$$

En C se define la ley:

$$(a\,;\,b) * (a'\,;\,b') = (aa'\,;\,ba' + b')$$

¿Qué estructura tiene $(C, *)$*?*

5. — *Demostrar que el conjunto* $C' = \{(1\,;\,b) \,/\, b \text{ racional}\}$ *es un subgrupo de C.*

6. — *Demostrar que la condición necesaria y suficiente para que un conjunto no vacío H incluido en un grupo G sea un subgrupo del mismo, para la misma ley de G, es que*

$$\forall x, \forall y \in H \,:\, x * y' \in H$$

7. — *Demostrar que en todo grupo ordenado:*

a) $x * z \leqslant y * z \Longrightarrow x \leqslant y$
b) $x \leqslant y \Longleftrightarrow x * y' \leqslant e$
c) $x \leqslant y \Longleftrightarrow y' \leqslant x'$
d) $x \leqslant y \wedge z \leqslant t \Longrightarrow x * z \leqslant y * t$

8. — *En un grupo abeliano aditivo, se define una segunda ley:*

$$\forall a, \forall b \,:\, a \cdot b = 0$$

Demostrar que el grupo y esa ley forman un anillo.

9. — *Sea un conjunto C, cuyos elementos son cuplas de enteros.*

$$C = \{(a\,;\,b) \,/\, a \wedge b \in Z\}$$

En C se definen las leyes:

$$(a\,;\,b) + (a'\,;\,b') = (a + a'\,;\,b + b')$$

y

$$(a ; b) \cdot (a ; b') = (aa' + 2bb' ; ab' + ba')$$

Demostrar que C, con tales leyes, es un anillo unitario. ¿Es de integridad? ¿Es dominio?

10. — *Se considera un conjunto S, cuyos elementos son cuplas de números reales*

$$S = \{(a ; b) \,/\, a \wedge b \text{ números reales}\}$$

se definen en S las dos leyes:

$$(x ; y) + (x' ; y') = (x + x' ; y + y')$$
$$(x ; y) \cdot (x' ; y') = (xx' ; xy' + x'y)$$

Demostrar que S con tales leyes es un anillo conmutativo unitario. ¿Cuándo S es un cuerpo?

11. — *Demostrar que el conjunto de los números reales de la forma:* $a + b\sqrt{N}$, *donde a y b son reales y N natural, es un subcuerpo del cuerpo de los reales.*

12. — *Demostrar que la intersección de dos subcuerpos de un cuerpo es también un subcuerpo.*

13. — *Sea* $\mathcal{E}$ *el conjunto de cuplas de números reales.*
En $\mathcal{E}$ *se define:*

$$(a ; b) + (c ; d) = (a + c ; b + d)$$

Y la ley externa:

$$\mu(a ; b) = (\mu a ; 0)$$

¿Es $\mathcal{E}$ *un espacio vectorial sobre el cuerpo de los reales? ¿Qué axioma no se cumple?*

14. — *Demostrar que si los vectores* $a_1, a_2, a_3, \ldots, a_n$ *son linealmente independientes, también lo son los vectores* b_i, *tales que:*

$$b_1 = a_1 ; b_2 = a_1 + a_2 ; \ldots ; b_n = a_1 + a_2 + \ldots + a_n$$

15. — *Demostrar que si dos subespacios E' y E" de un espacio vectorial* $\mathcal{E}$ *tienen la misma dimensión y* $E' \subseteq E''$, *entonces, necesariamente,* $E' = E''$.

CAPITULO VI

Axiomática

Si alguien acepta la idea de que en un diccionario se definen todos los términos de un idioma, evidentemente se equivoca. Basta considerar un ejemplo sencillo. Si se busca el significado de la palabra "dolor" se encuentra "pesar, aflicción, pena". "Pesar" es "dolor, amargura, pesadumbre, aflicción". "Pena" es "dolor, aflicción, pesadumbre, tristeza"; y no hace falta ir demasiado lejos para ver que se está efectuando un recorrido circular. ¿Dónde está el defecto? En pensar que pueden definirse **todos** los términos de un lenguaje. Si se quiere evitar el círculo vicioso, la única solución posible es efectuar algún corte brusco. Es decir, es necesario considerar en un momento de cualquier discurso lógico, términos que no se definen o términos primitivos.

El mismo razonamiento circular no puede tolerarse respecto de las oraciones que se utilizan y debe haber algunas de ellas que no se deducen, las cuales se conoçen como axiomas o postulados.

1. EL MÉTODO MATEMÁTICO

Las ideas anteriores dan la base del método axiomático utilizado en matemática.

Se eligen **términos primitivos técnicos** de tres tipos: conjuntos, leyes algebraicas o relaciones, y también **términos primitivos lógicos.** Además, se indica un conjunto de propiedades básicas que cumplen los términos primitivos, a los cuales se llama **axiomas o postulados** y que definen implícitamente a los primitivos o regulan su comportamiento. El resto de elementos a utilizar, así como las relaciones y operaciones no primitivas, se definen en base a los términos iniciales y los teoremas se deducen de los axiomas utilizando reglas lógicas.

En general, es común no aclarar cuáles son los términos lógicos que se consideran primitivos, tales como: "todo", "alguno", etc. y se utiliza, salvo indicación contraria, la lógica clásica. Esta lógica, también llamada del sentido común o aristotélica, admite solamente dos valores posibles para cualquier proposición: verdad o falsedad. Existen otras lógicas modernas que aceptan, por ejemplo, una tercera posibilidad, y cualquier proposición puede ser, entonces, verdadera o falsa o dudosa, y reciben el nombre de lógicas trivalentes. De la misma forma, las lógicas multivalentes aceptan n valores posibles para sus proposiciones. Si se utiliza cualquiera de estas lógicas no clásicas, debe repensarse todo el edificio matemático.

Vale decir que paralelamente al sistema matemático, se admite la validez de una lógica bivalente con todas sus reglas o tautologías, las cuales permiten establecer rigurosamente las definiciones y deducir teoremas en forma válida. Estas reglas o principios lógicos ya han sido mencionados en el capítulo I y pueden utilizarse libremente. Las más empleadas son, por ejemplo, la del **tercero excluido:** $p \veebar \sim p$; la de **no contradicción:** $\sim(p \wedge \sim p)$; la del **silogismo:**

$$[(p \Rightarrow q) \wedge (q \Rightarrow r)] \Rightarrow (p \Rightarrow r)\text{, etc.}$$

Por lo tanto, aparte de la lógica empleada, que en este libro se considera clásica, un sistema matemático formal se compone de:

1) **términos primitivos** (elementos, operaciones o relaciones sin definir)

2) **axiomas** (propiedades de los términos primitivos que no se demuestran)

3) **definiciones** (todos los términos no primitivos deben ser definidos)

4) **teoremas** (todas las propiedades no primitivas deben deducirse de los axiomas).

De acuerdo con el planteo anterior, los términos primitivos no tienen en sí mismos significado alguno, es decir, son variables a las que puede representarse simplemente con letras: $x, y, z, C, \mathcal{R} \ldots$ Los axiomas que se refieren a dichas variables son, por lo tanto, funciones proposicionales.

Si se sustituyen las variables (términos primitivos) por entes significativos, las funciones proposicionales (axiomas) se convierten en proposiciones. Esto es, se ha dado una **interpretación** al sistema axiomático. Si la interpretación convierte a los axiomas en proposiciones verdaderas, entonces se ha obtenido un **modelo** del sistema.

Por lo tanto, pueden considerarse dos aspectos en el estudio de los sistemas axiomáticos.

El primero, es el estudio del sistema abstracto en sí mismo. Es decir, un sistema abstracto no es un compendio de leyes arbitrarias, sin sentido propio, sino una entidad lógica que debe reunir ciertas propiedades. Expresiones del tipo "el axioma A implica el teorema T" o "el axioma B es independiente en el sistema S" pueden ser verdaderas o falsas y son proposiciones referentes a postulados o teoremas. Su estudio constituye la "matemática pura".

El otro aspecto es el estudio de las interpretaciones y modelos, para el que algunos autores reservan el nombre de "matemática aplicada".

2. EJEMPLO DE UN SISTEMA AXIOMÁTICO

Sistema O:

primitivos : **un conjunto** $C = \{a, b, c, \ldots\}$
una relación binaria $\mathcal{R}$ **definida en** C

axiomas : A_1 : $\mathcal{R}$ **es reflexiva**
A_2 : $\mathcal{R}$ **es antisimétrica**
A_3 : $\mathcal{R}$ **es transitiva**

(La relación $\mathcal{R}$, según se ha visto en el cap. III, establece en el conjunto C un orden parcial amplio.)

De los postulados A_1, A_2 y A_3, puede deducirse lógicamente una serie de teoremas $T_1, T_2, \ldots$ Las definiciones se designarán D_1, $D_2, \ldots$

D_1 : $b \,\mathcal{S}\, a \Leftrightarrow a \,\mathcal{R}\, b$ (es decir, $\mathcal{S}$ es la relación $\mathcal{R}^{-1}$)

T_1 : $\mathcal{S}$ **es una relación reflexiva en** C. Esto es $x \in C \Rightarrow x \,\mathcal{S}\, x$

Demostración:

$$\begin{array}{rll} & x \in C \Rightarrow x \,\mathcal{R}\, x & \text{por } A_1 \\ & x \,\mathcal{R}\, x \Rightarrow x \,\mathcal{S}\, x & \text{por } D_1 \\ \text{luego,} & x \in C \Rightarrow x \,\mathcal{S}\, x & \end{array}$$

T_2 : $\mathcal{S}$ **es una relación antisimétrica en** C.

Esto es, $x \,\mathcal{S}\, a \wedge a \,\mathcal{S}\, x \Rightarrow x = a$

Demostración:

$$\begin{array}{rll} & x \,\mathcal{S}\, a \wedge a \,\mathcal{S}\, x \Rightarrow a \,\mathcal{R}\, x \wedge x \,\mathcal{R}\, a & \text{por } D_1 \\ & a \,\mathcal{R}\, x \wedge x \,\mathcal{R}\, a \Rightarrow a = x & \text{por } A_2 \\ & a = x \Rightarrow x = a & \\ \text{Luego,} & x \,\mathcal{S}\, a \wedge a \,\mathcal{S}\, x \Rightarrow x = a & \end{array}$$

T_3 : $\mathcal{S}$ **es una relación transitiva en** C.

Demostración:

$$\begin{array}{ll} x \,\mathcal{S}\, y \wedge y \,\mathcal{S}\, z \Rightarrow y \,\mathcal{R}\, x \wedge z \,\mathcal{R}\, y & \text{por } D_1 \\ y \,\mathcal{R}\, x \wedge z \,\mathcal{R}\, y \Rightarrow z \,\mathcal{R}\, y \wedge y \,\mathcal{R}\, x & \text{conmut. de } \wedge \\ z \,\mathcal{R}\, y \wedge y \,\mathcal{R}\, x \Rightarrow z \,\mathcal{R}\, x & \text{por } A_3 \end{array}$$

$$z \mathcal{R} x \Rightarrow x \mathcal{S} z \qquad \text{por } D_1$$

Luego, $\quad x \mathcal{S} y \wedge y \mathcal{S} z \Rightarrow x \mathcal{S} z$

El sistema formado por los términos primitivos indicados, los axiomas A_1, A_2 y A_3, la definición D_1 y los teoremas T_1, T_2 y T_3 constituye un ejemplo elemental del comienzo de una teoría matemática pura o abstracta, cuyo desarrollo puede continuarse con otros teoremas y definiciones.

Interpretación 1 **(aritmética).**

C es el conjunto de los números enteros.

$\mathcal{R}$ es la relación de "menor o igual".

Interpretación 2 **(teoría de conjuntos)**

C es el conjunto potencial de un conjunto finito A, o sea, C está formado por todos los subconjuntos de A.

$\mathcal{R}$ es la relación de inclusión (impropia) entre conjuntos.

Puede probarse que cada una de las interpretaciones anteriores convierte a los axiomas A_1, A_2 y A_3 en proposiciones verdaderas. Luego, constituyen modelos del sistema O.

3. OTRO EJEMPLO DE SISTEMA AXIOMÁTICO

Sistema B:

primitivos : **un conjunto** $C = \{a, b, c \ldots\}$
dos operaciones binarias $\cup$ y $\cap$

axiomas :

B_1 : $\cup$ **y** $\cap$ **son operaciones conmutativas.** O sea,

$$\forall a \in C, \ \forall b \in C, \quad \text{es} \quad a \cup b = b \cup a \quad \text{y}$$
$$a \cap b = b \cap a$$

B_2 : **existe elemento neutro para cada operación.** O sea,

$$\exists z \in C, \ \exists u \in C \, / \, \forall a \in C, \quad \text{es} \quad a \cup z = a$$
$$\text{y} \quad a \cap u = a, \quad z \neq u$$

B_3 : **cada operación es distributiva con respecto a la otra.** O sea,

$$\forall a \in C, \ \forall b \in C, \ \forall c \in C, \quad \text{es} \quad a \cup (b \cap c) =$$
$$= (a \cup b) \cap (a \cup c) \ \text{y} \ a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$$

B_4 : **para cada elemento** a **de** C **existe** a' **en** C

$$a \cup a' = u \quad y \quad a \cap a' = z$$

(Este sistema recibe el nombre de álgebra de Boole. Los postulados anteriores fueron establecidos por E. V. Hungtinton)

T_1 : **Las operaciones** $\cup$ **y** $\cap$ **cumplen la ley idempotente**, esto es, $\forall x \in C$, es a) $x \cup x = x$ b) $x \cap x = x$

Demostración:

$$\begin{array}{ll} x = x \cup z & \text{por } B_2 \\ x = x \cup (x \cap x') & \text{por } B_4 \\ x = (x \cup x) \cap (x \cup x') & \text{por } B_3 \\ x = (x \cup x) \cap u & \text{por } B_4 \\ x = x \cup x & \text{por } B_2 \end{array}$$

Intercambiando $\cup$ por $\cap$ y z por u, se obtiene la parte b).

T_2 : **Para todo elemento** x **del conjunto** C **se cumple**

a) $x \cup u = u$ b) $x \cap z = z$

Demostración:

$$\begin{array}{ll} z = x \cap x' & \text{por } B_4 \\ z = x \cap (x' \cup z) & \text{por } B_2 \\ z = (x \cap x') \cup (x \cap z) & \text{por } B_3 \\ z = z \cup (x \cap z) & \text{por } B_4 \\ z = (x \cap z) \cup z & \text{por } B_1 \\ z = x \cap z & \text{por } B_2 \end{array}$$

La parte b) también se obtiene por dualidad, es decir, intercambiando $\cup$ por $\cap$ y z por u.

D_1 : $x \subset y \Leftrightarrow x \cup y = y$

Puede continuarse así el desarrollo de esta rama de matemática pura que ha recibido variadas e importantes aplicaciones.

Interpretación 1 **(teoría de conjuntos)**

C es el conjunto potencial de un conjunto A no vacío.

$\cup$ es la operación "unión" de conjuntos.

$\cap$ es la operación "intersección" de conjuntos.

Es evidente que z es el conjunto vacío, u el conjunto A y a' es el complemento relativo de cada subconjunto respecto de A.

Interpretación 2 (aritmética)

C es el conjunto de divisores naturales del número 30, es decir, $C = \{1, 2, 3, 5, 6, 10, 15, 30\}$.

$x \cup y$ es el mínimo común múltiplo de x e y.

$x \cap y$ es el máximo común divisor de x e y.

En este caso, z es 1 y u es 30.

Interpretación 3 (cálculo proposicional)

C es un conjunto de proposiciones.

$\cup$ es la "disyunción" de proposiciones.

$\cap$ es la "conjunción" de proposiciones.

u es una proposición tautológica, z es la negación de una proposición tautológica y la igualdad significa equivalencia lógica.

Puede probarse, según se ha indicado, que estas tres interpretaciones son modelos del sistema axiomático B.

4. PROPIEDADES DE LOS SISTEMAS AXIOMÁTICOS

De acuerdo con lo establecido anteriormente, podría pensarse que basta dar una colección cualquiera de símbolos como términos primitivos y un conjunto arbitrario de postulados para obtener un sistema axiomático y, por lo tanto, una expresión de matemática pura.

Existe, sin embargo, un conjunto de propiedades que dan interés y valor a los sistemas. Algunas de ellas son indispensables y otras solamente aconsejables.

Conviene considerar en primer lugar un concepto importante en cualquier estudio matemático.

Equivalencia

Definición

Dos sistemas S_1 y S_2 son equivalentes si y sólo si los términos primitivos de cada uno de ellos son definibles o primitivos en el otro y cada axioma es axioma o teorema en el otro.

La noción de sistemas equivalentes corresponde al concepto de proposiciones equivalentes.

Puede demostrarse, por ejemplo, que el siguiente sistema es equivalente al indicado en un punto anterior para el álgebra de Boole.

Sistema B' **:**

primitivos : un conjunto $C = \{a, b, c \ldots\}$

una operación binaria $\cap$

una operación unitaria $\overline{}$

axiomas:

B'_1 : **la operación** $\cap$ **es conmutativa en** C. O sea, $\forall a \in C, \forall b \in C$, es $a \cap b = b \cap a$

B'_2 : **la operación** $\cap$ **es asociativa en** C. O sea, $\forall a \in C, \forall b \in C, \forall c \in C$, es $(a \cap b) \cap c = a \cap (b \cap c)$

B'_3 : $\forall a \in C, \forall b \in C$, si $\exists x \in C / a \cap \overline{b} = x \cap \overline{x}$, entonces $a \cap b = a$

B'_4 : $\forall a \in C, \forall b \in C$, si $a \cap b = a$, entonces $\forall x \in C$ es $a \cap \overline{b} = x \cap \overline{x}$

La demostración de la equivalencia de los sistemas B y B' consiste en probar:

1º) los términos primitivos de la formulación anterior, que no son comunes a ambas formulaciones, deben definirse en base a los nuevos y éstos en base a los anteriores. Es decir, $\cup$ debe definirse mediante $\cap$ y $\overline{}$, y $\overline{}$ debe definirse mediante $\cup$ y $\cap$.

2º) los axiomas B_1, B_2, B_3 y B_4, que no pertenecen a la segunda formulación, deben deducirse de los axiomas B'_1, B'_2, B'_3 y B'_4 y estos últimos de los anteriores.

Se demuestra que la equivalencia de sistemas es una relación de equivalencia, de acuerdo con la definición dada en el cap. III.

Compatibilidad, consistencia o no contradicción

Definición

Un sistema axiomático es compatible si y sólo si sus axiomas no implican contradicción.

Entre todas las propiedades de un sistema de postulados, ésta es la única imprescindible. Es decir, su ausencia indica que el sistema considerado no tiene ningún valor lógico ni matemático.

Probar la compatibilidad de un sistema no es un problema sencillo. Si en una teoría abstracta aparecen dos axiomas o teoremas que se contradicen, entonces queda probada de inmediato su incompatibilidad. En cambio, si la teoría no es contradictoria, es prácticamente imposible enunciar todos los teoremas y probar así que no existe ningún par que se contradiga.

La consistencia de un sistema se prueba entonces de manera indirecta, por el método de los modelos. La prueba es concreta si puede exhibirse una interpretación real que satisfaga los axiomas. Por ejemplo, el sistema formado por los axiomas de equivalencia es consistente concretamente, pues pueden exhibirse modelos con n objetos reales, para n número finito. La compatibilidad queda probada al asumirse que la realidad no es contradictoria.

En cambio, si el conjunto tiene infinitos elementos es imposible exhibir un modelo real y debe recurrirse entonces a otros sistemas axiomáticos.

Por ejemplo, de la interpretación 1 del sistema de orden amplio parcial, se puede concluir que este sistema es consistente si lo es la aritmética de los números enteros. Del mismo modo, por ejemplo, la geometría analítica es un modelo para la geometría de Euclides e indica que la geometría euclídea es compatible si lo es el sistema de los números reales. En estos casos, la consistencia es relativa, es decir, la geometría euclídea es **tan consistente** como el sistema de los reales.

Teniendo en cuenta las consideraciones anteriores, puede darse la siguiente **definición "efectiva"** de sistema compatible:

Un sistema axiomático es compatible si y sólo si tiene modelo.

Los modelos hallados previamente para los axiomas de orden parcial y para el álgebra de Boole prueban entonces su compatibilidad.

Independencia

Un axioma es independiente en un conjunto de axiomas si no puede demostrarse lógicamente a partir de los otros axiomas.

Formalmente, si S es un sistema, A un axioma de S, ~A su negación, S − A el mismo sistema donde se ha excluido el axioma A y S + B es el sistema al cual se ha agregado el axioma B, entonces,

Definición

A es independiente en S si y sólo si S y (S − A) + ~A son ambos compatibles.

Un sistema es independiente si todos sus axiomas lo son.

Ejemplo

Sea el sistema O de orden parcial amplio indicado anteriormente, cuyos axiomas son:

$A_1 : x \in C \Rightarrow x \mathcal{R} x$

$A_2 : (x \mathcal{R} y \wedge y \mathcal{R} x) \Rightarrow x = y$

$A_3 : (x \mathcal{R} y \wedge y \mathcal{R} z) \Rightarrow x \mathcal{R} z$

O es independiente si y sólo si A_1 es independiente y A_2 es independiente y A_3 es independiente.

1) A_1 **es independiente**

Recordando que al negar la implicación $p \Rightarrow q$ se obtiene la conjunción $p \wedge \sim q$, la negación de A_1 tiene la forma siguiente:

$\sim A_1 : \exists x / x \in C \wedge x \not\mathcal{R} x$

Se debe encontrar entonces, un modelo para el sistema $\sim A_1$, A_2 y A_3.

Interpretación:

$C = \{0, 1, 2\}$ $\quad\quad$ $\mathcal{R} = \{(1 ; 1)\}$

La interpretación es modelo, pues verifica:

$\sim A_1$) $0 \in C \wedge 0 \not\mathcal{R} 0$

A_2) $(1 ; 1)$ es el único par de la relación y

$$(1 \mathcal{R} 1 \wedge 1 \mathcal{R} 1) \Rightarrow 1 = 1$$

A_3) $(1 \mathcal{R} 1 \wedge 1 \mathcal{R} 1) \Rightarrow 1 \mathcal{R} 1$

2) A_2 **es independiente**

$\sim A_2 : \exists x \in C, \exists y \in C / (x \mathcal{R} y \wedge y \mathcal{R} x) \wedge x \neq y$

Debe existir un modelo para A_1, $\sim A_2$ y A_3.

Interpretación:

$C = \{x / x \in Z\}$ $\quad$ $x \mathcal{R} y \Leftrightarrow |x| = |y|$

A_1) $x \in C \Rightarrow |x| = |x|$ por definición de valor absoluto.

$\sim A_2$) $(|3| = |-3| \wedge |-3| = |3|) \wedge 3 \neq -3$

A_3) $(|x| = |y| \wedge |y| = |z|) \Rightarrow |x| = |z|$ por propiedad del valor absoluto.

3) A_3 **es independiente**

$\sim A_3 : \exists x \in C, \exists y \in C, \exists z \in C / (x \mathcal{R} y \wedge y \mathcal{R} z) \wedge x \not\mathcal{R} z$

Debe existir modelo para A_1, A_2 y $\sim A_3$.

Interpretación:

$C = \{0, 1, 2\}$ $\quad$ $\mathcal{R} = \{(0 ; 0), (0 ; 1), (1 ; 1), (1 ; 2), (2 ; 2)\}$

A_1) $0 \mathcal{R} 0$, $1 \mathcal{R} 1$, $2 \mathcal{R} 2$

A_2) $(0 \mathcal{R} 0 \wedge 0 \mathcal{R} 0) \Rightarrow 0 = 0$

$(1 \mathcal{R} 1 \wedge 1 \mathcal{R} 1) \Rightarrow 1 = 1$

$(2 \mathcal{R} 2 \wedge 2 \mathcal{R} 2) \Rightarrow 2 = 2$

Para el resto de los pares de la relación, la antisimetría se satisface trivialmente. Ejemplo: $0 \mathcal{R} 1$ pero $1 \not\mathcal{R} 0$, luego al ser falso el antecedente, la implicación del axioma es verdadera.

$\sim A_3)$ $(0 \mathcal{R} 1 \wedge 1 \mathcal{R} 2) \wedge 0 \not\mathcal{R} 2$

La independencia no es una propiedad esencial en un sistema matemático y a veces se sacrifica por razones de conveniencia. Por ejemplo, el sistema indicado para un orden estricto total no es independiente y se han elegido esos axiomas simplemente por razones pedagógicas. En efecto:

E_1 : a-reflexividad
E_2 : a-simetría
E_3 : transitividad
E_4 : tricotomía

E_2 puede deducirse de los otros axiomas.

Sea el teorema correspondiente : $a \mathcal{R} b \Rightarrow b \not\mathcal{R} a$
Por contradicción: $(a \mathcal{R} b \wedge b \mathcal{R} a) \Rightarrow a \mathcal{R} a$ (por E_3) que contradice E_1.

Luego, el teorema queda demostrado.

Completicidad, integridad o saturación

Al establecer un conjunto de axiomas es conveniente, a veces, indicar todos los axiomas independientes posibles, de manera tal que ningún teorema correspondiente a la teoría pueda quedar sin demostración. Es decir:

Definición

Un sistema está completo o saturado si para cualquier propiedad p, relativa a la teoría, los axiomas del sistema implican dicha propiedad o su negación. O sea, no existe ningún enunciado p que pueda ser axioma independiente en el sistema.

Como en el caso de la compatibilidad, es más fácil probar que un sistema no posee la propiedad. Si en el desarrollo lógico de la teoría se llega a un teorema que no puede probarse ni negarse, entonces el sistema elegido no alcanza como soporte de la teoría, es decir, no está completo. Para probar que un sistema está completo se considera también un método indirecto, apelando a los modelos.

Definición

Un sistema S es categórico si y sólo si dos cualesquiera de sus modelos son isomorfos. (Sólo interesa la categoricidad de sistemas compatibles.)

Esto significa que entre dos modelos cualesquiera de S puede establecerse una correspondencia biunívoca que "preserva" relaciones y operaciones de acuerdo con la definición dada en el cap. IV.

Se prueba que si un sistema es **categórico,** entonces está **completo** y, en general, categoricidad y completicidad se consideran conceptos lógicamente equivalentes.

En resumen, para probar que un sistema no está completo basta exhibir dos modelos no isomorfos. En cambio, para probar que lo está, el método consiste en demostrar que cada modelo del sistema es isomorfo con un modelo elegido.

Ejemplo

Los axiomas de orden parcial amplio no constituyen un sistema completo.

Basta considerar los dos modelos siguientes:

$$M_1 : C_1 = \{0, 1, 2\} \quad \mathcal{R} : \leqslant$$
$$M_2 : C_2 = \{0, 1, 2, 3, 4\} \quad \mathcal{R} : \leqslant$$

Es evidente que M_1 y M_2 no son isomorfos, pues no es posible definir entre ellos una aplicación biyectiva.

El sistema se puede transformar en un sistema categórico si se añade un postulado que fije el número de elementos del conjunto:

A_4 : C contiene exactamente 4 elementos.

La propiedad de completicidad puede ser deseable o no, según los casos. La ventaja de muchos sistemas incompletos está en la gran amplitud de sus aplicaciones. Por ejemplo, los axiomas de grupo son comunes a muchas estructuras matemáticas y es conveniente conocer los teoremas deducidos a partir del conocido sistema de axiomas que es incompleto. Lo mismo sucede con los anillos, cuerpos, relaciones de equivalencia, relaciones de orden, etc.

La categoricidad de un sistema es una relación de equivalencia en el conjunto formado por todos sus modelos y dos interpretaciones pertenecen a la misma clase si y sólo si son isomorfos. La categoricidad corresponde entonces, a la existencia de una sola clase de equivalencia en el conjunto de los modelos.

EJERCICIOS

1. — *Considerando el siguiente sistema*

   L : *primitivos* : $C = \{a, b, c, d\}$ $\quad \mathcal{R}$ ***relación binaria***

   axiomas : $A_1 : a \neq b \Longrightarrow (a \mathcal{R} b \vee b \mathcal{R} a)$

   $A_2 : a \mathcal{R} b \Longrightarrow a \neq b$

   $A_3 : (a \mathcal{R} b \wedge b \mathcal{R} c) \Longrightarrow a \mathcal{R} c$

   A_4 : *C tiene exactamente cuatro elementos.*

   Probar los siguientes teoremas:

   $T_1 : a \mathcal{R} b \Longrightarrow b \not\mathcal{R} a$

   $T_2 : (x \neq a \wedge x \neq b \wedge a \mathcal{R} b) \Longrightarrow (a \mathcal{R} x \ \underline{\vee} \ x \mathcal{R} b)$

   $T_3 : \exists x \in C \, / \, \forall a \in C$ *es* $x \not\mathcal{R} a$

2. — *Probar que L es un sistema compatible.*

3. — *Probar que L es un sistema independiente.*

4. — *Probar que L es un sistema categórico.*

5. — *Probar que la equivalencia de sistemas axiomáticos es una relación de equivalencia.*

6. — *Dar ejemplos de definiciones equivalentes.*

7. — *Establecer la compatibilidad del sistema de axiomas para un cuerpo.*

8. — *Probar que los axiomas de la relación de equivalencia son independientes.*

9. — *Probar la compatibilidad del siguiente sistema, donde "flor" y "estrella" son términos primitivos:*

   F_1 : *cada flor es un conjunto de estrellas.*

   F_2 : *dos flores diferentes cualesquiera tienen una y sólo una estrella en común.*

   F_3 : *cada estrella pertenece a dos flores y solamente a dos.*

   F_4 : *existen exactamente cuatro flores.*

   (puede buscarse un modelo geométrico interpretando "flor" como recta y "estrella" como punto.)

10. — *De los axiomas anteriores deducir los siguientes teoremas:*

    T_1 : *existen exactamente seis estrellas.*

    T_2 : *a cada flor pertenecen exactamente tres estrellas.*

11. — *Probar que el isomorfismo entre modelos de un sistema axiomático es una relación de equivalencia.*

CAPITULO VII

El número y sus generalizaciones

1. EVOLUCIÓN DEL CONCEPTO DE NÚMERO

El número, piedra angular de todo el edificio matemático, aparece íntimamente vinculado a los más diversos aspectos de la vida cotidiana. Sin embargo, si a una persona medianamente culta y hábil, inclusive en el cálculo operatorio, se le preguntase ¿qué es el número? probablemente la respuesta sería una mirada de extrañeza ante la aparente trivialidad de la pregunta, o bien la clásica tautología: un número es un número, o tal vez, algún ejemplo concreto.

Para los matemáticos la pregunta no es trivial y durante mucho tiempo se la formularon sin hallar respuesta satisfactoria. La cuestión es, en efecto, profunda y compleja; su análisis va más allá del terreno puramente matemático y preocupa por igual a lógicos y filósofos.

Kroenecker, matemático alemán del siglo XIX, soslayó el problema con su conocida conclusión: el número es obra de Dios, lo demás corresponde a los hombres. Klein, por su parte alude a la sensación de bienestar que se experimenta cuando se deja a un lado dicha cuestión.

La génesis del número se pierde en el origen remoto de los primeros núcleos humanos. Aparece allí el número como noción primaria estrechamente vinculada a los objetos materiales y como resultado de la percepción directa del cambio producido al añadir algún objeto a otro, o al quitar o agregar elementos a un conjunto de varios objetos.

Se advierte este carácter esencialmente concreto de la idea de número a través del estudio de las lenguas primitivas, en las que aparecen términos distintos para designar el número según que los objetos de que se trate sean personas, animales o cosas. Restos de esa distinción subsisten en los idiomas modernos, como ser yunta, pareja, casal, par, etc.

Este sentido precario del número se ensancha cuando el hombre adquiere la técnica de contar, operación que requiere cierto grado de evolución mental. Pero fue necesario que la inteligencia humana alcanzase un nivel superior de desarrollo para que la idea concreta del número diese lugar a su concepción abstracta. Advertir que una yunta de bueyes o un par de personas son ambos ejemplos concretos del número dos, requiere un refinado proceso de abstracción, operación que marca, sin duda, un jalón en el desenvolvimiento de las facultades intelectivas.

A esto sucedió el largo proceso histórico a través del cual el concepto de número se amplió con la creación de las reglas del cálculo y las sucesivas extensiones que lo llevaron a su forma actual.

Pero es recién en el siglo XIX cuando los matemáticos se abocaron al estudio riguroso y sistemático del concepto de número y en particular del número natural.

2. EL NÚMERO NATURAL. SU FUNDAMENTACIÓN

A través de las teorías formuladas para fundamentarlo, el número natural aparece desdoblado en dos aspectos: el cardinal y el ordinal.

El concepto de número cardinal surge como respuesta a la pregunta: ¿cuántos elementos tiene un conjunto? En él se prescinde de la naturaleza de los elementos y del orden en que se presenten. Se basa como veremos más adelante en la idea de correspondencia y nace como atributo característico de los conjuntos finitos entre los que existe una biyección.

El número ordinal nace en cambio de la operación de contar. Al contar se asigna a cada elemento del conjunto un número; esto implica una ordenación entre los elementos del mismo y el número que corresponde al último elemento es el ordinal del conjunto.

La separación de ambos conceptos, cardinal u ordinal, establece dos caminos para la fundamentación del número natural. En su condición de cardinal nace, por abstracción, de la teoría de conjuntos. Como ordinal se introduce axiomáticamente y se considera, por lo tanto, concepto primitivo.

El primer camino fue seguido por Cantor, Fregue, Dedekind, Russell. El segundo fue adoptado por Peano, que formuló su teoría dentro de los sistemas formales creados por Hilbert.

3. FUNDAMENTACIÓN AXIOMÁTICA DEL NÚMERO NATURAL

Sistema de Peano

La teoría de Peano es axiomática y ordinal y parte de tres conceptos primitivos: un objeto llamado 1, un conjunto N cuyos elementos se llaman números naturales y una relación "siguiente de" o sg, definidos implícitamente por medio de cinco axiomas.

N_1: **Uno es un número natural** $(1 \in N)$

N_2: **Todo número natural tiene un único siguiente**

$$\forall x \in N, \exists sg\, x \in N \,/\, [s = sg\, x \wedge z = sg\, x] \Rightarrow s = z$$

N_3: **Si los siguientes de dos elementos son iguales, los elementos también lo son:**

$$sg\, x = sg\, y \Rightarrow x = y$$

N_4: **El uno no es siguiente de ningún número**

$$\forall x \in N, 1 \neq sg\, x$$

N_5: **Si un conjunto C de números naturales es tal que 1 pertenece a él y el siguiente de todo número natural perteneciente a C, pertenece también a C, entonces éste contiene a todos los números naturales.**

$$[\exists C / C \subseteq N \wedge 1 \in C \wedge (x \in C \Rightarrow sg\, x \in C)] \Rightarrow N \subseteq C$$

Observación

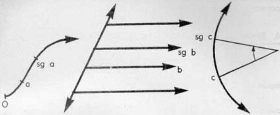
El número de axiomas de este sistema puede reducirse a cuatro, teniendo en cuenta que N_2 y N_3 equivalen al siguiente enunciado: sg es una aplicación inyectiva de N en N.

Estos axiomas, al señalar las propiedades del llamado conjunto natural lo van configurando de tal manera que es posible seleccionar paso a paso los conjuntos que satisfacen el esquema propuesto, y excluir aquellos que no lo cumplen hasta llegar a la caracterización total de una única especie de conjuntos.

Así, el N_1 elimina los conjuntos vacíos. El N_2 permite considerar aquellos conjuntos ordenados por la relación primitiva "siguiente" que no ofrecen bifurcación en la generación del elemento siguiente a uno dado; por ejemplo, si se considera el conjunto formado por todos los hombres y la relación "ser padre de" como "siguiente" se satisfacen las condiciones del N_1, pues el conjunto no es vacío, y del N_2, pues cada elemento tiene un único siguiente. Sin embargo esta relación es polifurcable hacia atrás, pues cada hombre puede ser padre de varios hijos. Este posible desdoblamiento de la relación se elimina con el N_3, que afirma la unicidad del antecedente del par de elementos vinculados por ello.

El N_4 impone la condición de la existencia de un elemento inicial.

Es de observar, que existen numerosos ejemplos de conjuntos que satisfacen a los cuatro primeros axiomas, pero que están lejos de ser modelos del conjunto natural. Así, responden a las cuatro condiciones las reuniones de conjuntos disjuntos linealmente ordenados, sin primero ni último elemento, con la restricción de que uno de ellos tenga origen pero no extremo. Por ejemplo la reunión de los tres conjuntos siguientes:



Esta arbitrariedad desaparece por obra del N_5, que selecciona entre la variedad de sucesiones formadas a expensas de un elemento inicial por la relación generadora "siguiente", las sucesiones naturales que son las sucesiones mínimas que pueden obtenerse de esa manera, es decir, las que están incluidas en cualquier conjunto que contenga al uno y al siguiente de un elemento perteneciente a él.

El N_5 es el llamado principio de inducción completa y es la base del fructífero método de demostración del mismo nombre. En efecto, su enunciado es equivalente a la siguiente proposición: **Si P es una propiedad que se cumple para 1 y cumpliéndose para un número natural cualquiera, se cumple también para el siguiente, entonces P es una propiedad que pertenece a todos los números naturales.**

La equivalencia de ambos enunciados es inmediata si se considera que dar el conjunto C implica dar una propiedad P, la de pertenecer a C; recíprocamente, dar una propiedad P implica dar un conjunto C, el formado por los elementos que cumplen P.

El mismo axioma es el fundamento de las definiciones por recurrencia, que permiten la creación de nuevos conceptos en los que figure un número natural cualquiera, mediante un proceso de construcción escalonado inductivamente.

Con estos procedimientos Peano edifica toda la aritmética sobre el concepto de número ordinal. El desarrollo es estimable por su perfección lógica, pero resulta laborioso y pesado por el uso reiterado del principio de inducción completa y su carácter esencialmente formal, lo cual hace que el método no sea aconsejable al nivel de la enseñanza media.

Se ha objetado, además, al sistema de Peano, que sus postulados no definen en realidad los números naturales ordinales, pues no los caracterizan unívocamente, sino a cualquier sucesión natural de entes arbitrarios. Así lo hizo notar Russell, que observó que toda sucesión o progresión $a_1, a_2, \ldots, a_n, \ldots$ con primer elemento a_1 y en la que cada elemento tenga un siguiente, determinado por ciertas relaciones, satisface los cinco axiomas. La objeción desaparece si se considera que los conceptos de sucesión natural y de sucesión numérica natural son isomorfos y por lo tanto pueden considerarse como modelos de un concepto único. Basta entonces, tomar una cualquiera de ellas como representante de las demás y asignar a cada uno de sus elementos un nombre y un símbolo convencional que lo identifique. Tal podría ser, por ejemplo, la sucesión 1, 2, 3, . . . , n, . . .

4. ADICIÓN Y MULTIPLICACIÓN DE LOS NÚMEROS NATURALES EN EL SISTEMA DE PEANO

Se definen por medio del método de recurrencia que utiliza el siguiente proceso de construcción:

I) Se define explícitamente el compuesto de un número natural cualquiera a con el número natural 1.

II) Se define explícitamente el compuesto de a con el siguiente de un número natural cualquiera h.

III) Por I) y II) y aplicando el principio de inducción completa, se obtiene el compuesto de a y b, números naturales cualesquiera.

Definición

Se llama adición de números naturales a la operación que satisface las siguientes definiciones explícitas:

N_6: $\forall a \in N, a + 1 = sg\ a$
N_7: $\forall a, \forall h \in N, a + sg\ h = sg(a + h)$

Como se advierte, la segunda definición, se refiere a la operación de sumar el siguiente de h a un número natural cualquiera a, admitiendo como definida la operación de sumar h al mismo. En virtud de la definición explícita N_6, la N_7 puede escribirse:

$$a + (h + 1) = (a + h) + 1$$

De esta manera, aplicando reiteradamente N_6 y N_7 se obtiene por recurrencia la suma de $a + b$, cualesquiera que sean a y b.

$$a + 2 = a + sg\ 1 = sg(a + 1)$$
$$a + 3 = a + sg\ 2 = sg(a + 2)$$
. . . .

Es decir, por aplicación del N_5 de Peano, resulta a prima facie **definida** la suma $a + b$ y así es en realidad, pero lo anterior no basta para asegurarlo y es necesario establecer que la suma $a + b$ queda unívocamente determinada.

Si C es el conjunto de los números naturales x tales que $a + x$ está definida unívocamente, resulta por N_6 y por ser $1 \in N$, que $1 \in C$. Si $a + x = y / x \in C$, resulta y unívocamente determinado por hipótesis de recurrencia y por lo tanto también su siguiente, o sea sg y = a + sg x. Es decir, el sg y pertenece a C y por lo tanto por el N_5, $N \subseteq C$, es decir, a + b está unívocamente definido y es también un número natural.

Consecuencia

La adición de números naturales es una ley de composición interna.

En base a la definición y a los axiomas se pueden demostrar las siguientes:

Propiedades de la adición de números naturales

1. — $a + b \neq b$
2. — **Conmutativa:** $a + b = b + a$
3. — **Asociativa:** $(a + b) + c = a + (b + c)$
4. — **Cancelativas:** $b + a = c + a \Rightarrow b = c$
   $a + b = a + c \Rightarrow b = c$
5. — $a \neq b \Rightarrow a + c \neq b + c$

Corolario

La adición de números naturales no posee elemento neutro.

Es inmediato según la propiedad 1.

Definición

Se llama multiplicación de números naturales a la operación que satisface las siguientes definiciones explícitas:

N_8: $\forall a \in N,\ a \cdot 1 = a$

N_9: $\forall a,\ \forall h \in N,\ a \cdot \mathrm{sg}\, h = a \cdot h + a$

Análogamente a lo hecho en el caso de la adición y con procedimiento similar, se demuestra que el producto $a \cdot b$, cualesquiera sean a y b, queda unívocamente determinado.

Son también de demostración inmediata las siguientes:

Propiedades de la multiplicación de números naturales

1. — **Conmutativa:** $a \cdot b = b \cdot a$
2. — **Asociativa:** $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

3. — **Distributiva respecto de la adición:**

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

4. — **Cancelativas:** $a \cdot c = a \cdot b \Rightarrow c = b$

$$c \cdot a = b \cdot a \Rightarrow c = b$$

Consecuencia

Existe elemento neutro de la multiplicación de números naturales

Es inmediato a partir de N_4 y de la propiedad conmutativa. Es el número 1.

Observación

En el sistema de Peano, no se considera el cero como perteneciente al conjunto N de los números naturales. Las teorías más modernas —y así lo hizo el mismo Peano en ediciones posteriores de su obra— se desarrollan de manera que el cero aparece como número natural y esto se consigue sin hacer ninguna modificación de fondo en el sistema de axiomas. Basta, en efecto, introducir un pequeño cambio formal que consiste en sustituir el símbolo 1 por el 0.

En tal caso, las definiciones de adición y multiplicación se cambian por las siguientes:

N_6: $a + 0 = a$

N_7: $a + \text{sg}\, h = \text{sg}(a + h)$

N_8: $a \cdot 0 = 0$

N_9: $a \cdot \text{sg}\, h = a \cdot h + a$

Se define $1 = \text{sg}\, 0$ y con ello resultan de inmediato como teoremas las definiciones dadas anteriormente.

En efecto: $a + 1 = a + \text{sg}\, 0 = \text{sg}\,(a + 0) = \text{sg}\, a$

$$a \cdot 1 = a \cdot \text{sg}\, 0 = a \cdot 0 + a = 0 + a = a$$

5. OTROS SISTEMAS AXIOMÁTICOS PARA EL NÚMERO NATURAL

Siguiendo el camino enunciado por Peano, otros matemáticos como Padoa, Pieri, etc., se ocuparon de definir axiomáticamente el número natural.

Padoa reduce a dos los conceptos primitivos: número natural y siguiente, al observar que de las proposiciones mismas se puede extraer la definición del número que no es siguiente de ningún otro.

Caracteriza dichos conceptos por medio de cuatro axiomas independientes.

I. — El siguiente de un número natural es un número natural.

II. — Si los siguientes de dos números naturales son iguales, dichos números también lo son.

III. — Existe por lo menos un número natural que no es el siguiente de otro.

IV. — Si en un conjunto C de números naturales hay un número que no es siguiente de otro y si el siguiente de un elemento de C, pertenece también a C, entonces C contiene a cualquier número natural.

En base a estos axiomas, se demuestra la unicidad del número que no es siguiente de otro.

Pieri toma los mismos conceptos primitivos: número natural y siguiente y construye un sistema de cuatro axiomas independientes:

I. — Existe, por lo menos, un número natural.

II. — El siguiente de un número natural es un número natural.

III. — Si dos números son siguientes de otro, son iguales.

IV. — En cualquier conjunto no vacío de números naturales existe por lo menos un elemento que no es siguiente de otro elemento del mismo conjunto.

En ambos sistemas, una vez establecidas las proposiciones primitivas, se definen las operaciones de adición y multiplicación por recurrencia, como en la teoría de Peano.

6. FUNDAMENTACIÓN DEL NÚMERO NATURAL POR TEORÍA DE CONJUNTOS

El número natural surge, en su faz cardinal, como atributo característico de los conjuntos finitos y se apoya en la idea de coordinabilidad.

Definición

Se dice que un conjunto es finito cuando se puede introducir en él una ordenación perfecta, es decir, una ordenación total según la cual todo subconjunto no vacío tenga primero y último elementos.

Definición

Se dice que dos conjuntos X e Y son equipotentes o coordinables, cuando existe una biyección de X sobre Y.

$$X \text{ equipotente } Y \iff \exists f : X \xrightarrow{f} Y \text{ biyectiva.}$$

Definición

La relación que vincula dos conjuntos equipotentes se llama coordinabilidad o equipotencia.

Corolario

La equipotencia entre conjuntos es una relación de equivalencia.

En efecto, se cumplen las condiciones exigidas:

a) **reflexividad** X equipotente X.

Basta tomar como biyección f la función idéntica que a cada elemento $x \in X$ hace corresponder el mismo elemento.

b) **simetría** X equipotente Y $\iff$ Y equipotente X.

Si f es una biyección de X sobre Y, f^{-1} es una biyección de Y sobre X.

c) **transitividad** [X equip. Y $\wedge$ Y equip. Z] $\Rightarrow$ X equip. Z.

Si f es una biyección de X sobre Y y g es una biyección de Y sobre Z, $g \cdot f$ es una biyección de X sobre Z.

Como se ha visto en el capítulo III, toda relación de equivalencia definida en un conjunto determina en éste una partición en clases de equivalencia.

Luego, si se considera el conjunto F, formado por todos los conjuntos finitos, la relación de coordinabilidad entre los mismos produce en él una partición y los conjuntos pertenecientes a una misma clase pueden considerarse identificados por una característica que les es común. Nuestra mente crea así, por abstracción, un nuevo objeto o concepto que toma el nombre de número natural cardinal.

Definición

Se llaman números naturales cardinales a los elementos del conjunto cociente del conjunto F (de conjuntos finitos) por la relación de coordinabilidad.

A cada conjunto finito se asigna, pues, un nuevo ente que es su natural cardinal, tal que:

$$\text{Card. } (X) = \text{Card. } (Y) \Leftrightarrow X \text{ equip. } Y$$

O lo que es lo mismo: X e Y pertenecen a la misma clase de equivalencia.

Decimos entonces que dos conjuntos coordinables tienen el mismo número de elementos.

Los dos caminos seguidos hasta ahora para fundamentar el número natural, sea en su aspecto ordinal o en el cardinal, conducen, en el caso de los conjuntos finitos, a un concepto único, el de número natural. Para esto se prueba que el número ordinal de un conjunto finito es único e independiente del orden en que se consideran sus elementos y esta proposición constituye el llamado principio de invariancia del número.

Esta invariancia existe también en el caso del cardinal, pues si un conjunto es equipotente con otro, lo sigue siendo cualquiera sea la forma en que se realiza la correspondencia.

De ahí que ambos aspectos, número cardinal y número ordinal puedan considerarse como representantes de un mismo concepto relativo a los conjuntos finitos, el de número natural.

El número natural caracteriza, pues, los conjuntos finitos y establece cuantos elementos lo componen.

Si los conjuntos son infinitos no rige el mismo principio. Según sea el orden seguido al contar, el ordinal es distinto. La extensión de la operación de contar al caso de los conjuntos infinitos se debe a Cantor que creó los números trasfinitos para distinguir los diferentes tipos de conjuntos infinitos.

7. DEFINICIÓN AXIOMÁTICA DE LAS OPERACIONES ENTRE LOS NÚMEROS NATURALES

En la teoría de Peano sobre los números naturales se definen las operaciones de adición y multiplicación por el método de recurrencia. En la teoría conjuntista, se definen a partir de las operaciones entre conjuntos. Existe otro procedimiento axiomático por el cual se caracterizan simultáneamente los números naturales y ambas operaciones.

Se toman como elementos primitivos un conjunto N cuyos elementos se designan números naturales, y dos operaciones binarias cerradas en N llamadas adición y multiplicación.

Los axiomas que cumplen dichos objetos son los siguientes:

N_1 : **Conmutatividad de la adición:** $a + b = b + a$

N_2 : **Asociatividad de la adición:** $(a + b) + c = a + (b + c)$

N_3 : **Conmutatividad de la multiplicación:** $a \cdot b = b \cdot a$

N_4 : **Asociatividad de la multiplicación:** $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

N_5 : **Distributividad de la multiplicación con respecto a la adición:** $a \cdot (b + c) = a \cdot b + a \cdot c$

N_6 : **Existencia del neutro para la multiplicación:**

$$\exists\, 1 \in N \,/\, \forall a \in N,\ a \cdot 1 = a.$$

N_7 : $a + b \neq a$

N_8 : **Cancelatividad de la adición:**

$$a + b = a + c \Rightarrow b = c$$

N_9 : **Cancelatividad de la multiplicación:**

$$a \cdot b = a \cdot c \Rightarrow b = c$$

N_{10}: $a \neq b \Rightarrow \exists x / a + x = b \veebar \exists y / a = b + y$

N_{11}: Si N' Si $N' \subseteq N$, $1 \in N' \wedge (m \in N' \Rightarrow m + 1 \in N')$ entonces $N = N'$

Se demuestra que todo conjunto así definido es isomorfo a cualquier conjunto caracterizado por el sistema de Peano, estructurados en la forma expuesta en cada caso por las operaciones adición y multiplicación.

8. PROPIEDADES ESTRUCTURALES DEL CONJUNTO DE LOS NÚMEROS NATURALES

De lo tratado resulta que el conjunto de los números naturales es:

a) un semigrupo abeliano, cancelativo, sin elemento neutro, con respecto a la adición.

b) Un semigrupo abeliano, cancelativo, con elemento neutro, con respecto a la multiplicación.

9. EXTENSIÓN DEL CONCEPTO DE NÚMERO

El concepto de número se amplía sucesivamente, a medida que lo requiere la necesidad de hacer posibles algunas operaciones que no pueden realizarse en un campo numérico dado.

Esta generalización puede hacerse de dos maneras: a) definiendo los nuevos conceptos por abstracción, a expensas de números del campo conocido, lo cual constituye el método genético; b) enunciando las leyes algebraicas fundamentales que deben satisfacer los nuevos entes, tomados como conceptos primitivos, es decir, por el método axiomático.

En ambos casos, las sucesivas ampliaciones deben hacerse de tal modo que se respete el llamado principio de permanencia de las leyes formales, de Hankel, según el cual, el nuevo sistema de números creados debe satisfacer las reglas operatorias establecidas en el sistema anterior, y éste, a su vez, debe formar parte del nuevo como caso particular.

De otro modo, si A es un conjunto en el que se han definido una o dos operaciones, se dice que B es una ampliación de A si, definidas en B dos operaciones correspondientes a las de A, existe un subconjunto A' de B, isomorfo a A. Se impone también como condición igualmente esencial que se cumplan en B las propiedades que no se cumplen en A y que motivaron la extensión, o sea, se debe pasar, por ejemplo, de un semigrupo a un grupo o de un dominio de integridad a un cuerpo.

10. EL NÚMERO ENTERO

Nos ocuparemos a continuación de la primera ampliación del concepto de número, es decir, de los números enteros, como ejemplo de los métodos usuales a tal fin, dejando para un volumen posterior las extensiones subsiguientes.

Los números enteros se introducen con el objeto de dar siempre solución a la ecuación $a + x = b$.

Existe solución en el campo de los números naturales sólo si $b > a$, en cuyo caso se representa $x = b - a$ y se dice que x es la diferencia entre b (minuendo) y a (sustraendo). La operación que permite hallar x se llama sustracción.

Si $b \leqslant a$, la ecuación mencionada carece de solución en el campo natural.

El problema consiste entonces en ampliar el conjunto N, algebrizado por una ley de composición interna, conmutativa y asociativa, la adición, que le confiere estructura de semigrupo abeliano, de modo que se obtenga un conjunto más amplio provisto de una ley interna, extensión de la anterior en el sentido de conferirle estructura de grupo. Es decir, que exista neutro y que cada elemento de N tenga su simétrico en el nuevo conjunto.

11. CONSTRUCCIÓN DE LOS ENTEROS POR EL MÉTODO GENÉTICO

Sea N el conjunto de los números naturales y consideremos el producto cartesiano $E = N \times N$, es decir, el conjunto de los pares ordenados $(a\,;\,b)$ formados con elementos de N.

Definición

Dos pares $(a\,;\,b)$ y $(c\,;\,d) \in E$, son equivalentes si y sólo si: $a + d = b + c$.

$$(a\,;\,b) \sim (c\,;\,d) \Leftrightarrow a + d = b + c$$

La relación dada es efectivamente de equivalencia, pues se cumplen las condiciones exigidas:

a) **reflexividad:**

$$(a ; b) \sim (a ; b) \text{ pues } a + b = b + a$$

b) **simetría**

$$(a ; b) \sim (c ; d) \Rightarrow (c ; d) \sim (a ; b)$$

$$\text{Pues } a + d = b + c \Rightarrow c + b = d + a$$

c) **transitividad**

$$[(a ; b) \sim (c ; d) \wedge (c ; d) \sim (e ; f)] \Rightarrow$$
$$\Rightarrow (a ; b) \sim (e ; f)$$

En efecto, si $a + d = b + c$ y $c + f = d + e$, resulta

$$(a + d) + (c + f) = (b + c) + (d + e)$$

Y aplicando las propiedades asociativa y conmutativa en N, se obtiene:

$$(a + f) + (c + d) = (b + e) + (c + d)$$

Y por la propiedad cancelativa de la adición en N

$$a + f = b + e$$

La relación precedente divide, pues, al conjunto E en clases de equivalencia.

Definición

Se llama conjunto de los números enteros al conjunto cociente de E por la relación de equivalencia definida anteriormente.

Se lo designa por la letra Z. Luego

$$Z = \frac{N \times N}{\sim}$$

Definición

Se llama número entero racional o número entero relativo o entero, a cada una de las clases de equivalencia del conjunto Z.

Ejemplo

$M = \{(6 ; 4), (8 ; 6), (5 ; 3), (200 ; 198) \ldots\}$ es una de las clases de equivalencia de Z.

Enteros positivos, negativos y nulo

Cada clase de equivalencia de Z, es decir, cada entero relativo, admite como representante un par cualquiera perteneciente a dicha clase. O sea todo entero se representa por un par $(x ; y)$ donde x e y son números naturales.

De acuerdo con ello y considerando que los números naturales satisfacen la ley de tricotomía, es decir, dados x e y se verifica: $x > y \veebar x = y \veebar x < y$, es posible clasificar los enteros relativos en tres subconjuntos según dichas posibilidades.

$$x > y \Rightarrow x = a + y, \text{ luego el par } (x ; y) = (a + y ; y)$$

Es inmediato que todos los pares de la forma $(a + y ; y)$, donde y es un número natural cualquiera, pertenecen a una misma clase de equivalencia. En efecto $(a + y ; y) \sim (a + z ; z)$ pues $(a + y) + z = y + (a + z)$. De acuerdo con lo enunciado, tiene sentido la siguiente:

Definición

Se llama entero positivo al representado por el par $(a + y ; y)$

Se lo simboliza de la siguiente manera:

$$(a + y ; y) = +a$$

Y al subconjunto de Z formado por todos los enteros positivos se lo simboliza Z^+.

Análogamente: si dado el par $(x ; y)$ se verifica que $x < y$, reresulta $y = x + b$, o sea $(x ; y) = (x ; x + b)$ y los pares de este tipo pertenecen a una misma clase de equivalencia cualquiera sea x.

Definición

Se llama entero negativo al representado por el par $(x ; x + b)$

Se lo simbolize:

$$(x ; x + b) = -b$$

Y al subconjunto de Z formado por ellos Z^-

De igual modo, dado el par $(x ; y)$ tal que $x = y$, resulta $(x ; y) = (x ; x)$ y todos los pares de este tipo pertenecen a una misma clase de equivalencia.

Definición

Se llama número entero cero al representado por el par $(x ; x)$

Se lo simboliza:

$$(x ; x) = 0$$

Corolario

El entero 0 **es único.**

En efecto, es inmediato en virtud de la definición de cero.

Definición

Se llama conjunto de los elementos nulos de Z, **al conjunto unitario:**

$$C(0) = \{0\}$$

Corolario

El conjunto Z es la unión del conjunto de los enteros positivos, el conjunto de los enteros negativos y el conjunto de los elementos nulos.

$$Z = Z^{+} \cup Z^{-} \cup C(0)$$

12. ADICIÓN Y MULTIPLICACION DE NÚMEROS ENTEROS

Definición

En $E = N \times N$ **se define la siguiente ley de composición que se llama adición:**

$$(a ; b) + (c ; d) = (a + c ; b + d)$$

Probaremos la estabilidad de la ley respecto de la relación de equivalencia establecida en E, es decir, si

$$(a ; b) \sim (c ; d) \wedge (a' ; b') \sim (c' ; d')$$

Entonces:

$$(a + a' ; b + b') \sim (c + c' ; d + d') \qquad (T)$$

En efecto:

$$(a ; b) \sim (c ; d) \Rightarrow a + d = b + c$$
$$(a' ; b') \sim (c' ; d') \Rightarrow a' + d' = b' + c'$$

Luego:

$$a + a' + d + d' = b + b' + c + c'$$

O sea:

$$(a + a') + (d + d') = (b + b') + (c + c') \Rightarrow (T)$$

De esto surge, como se ha visto en el capítulo IV, que la operación definida en $E = N \times N$ define o induce una operación en el conjunto cociente Z; a esta operación la llamamos adición de números enteros.

Luego, para sumar dos números enteros, tomamos como representante de cada clase de equivalencia de Z un par cualquiera perteneciente a la misma. Así, si $\alpha =$ clase $(a ; b)$ y $\alpha' =$ clase $(a' ; b')$:

$$\alpha + \alpha' = (a ; b) + (a' ; b')$$
$$\alpha + \alpha' = (a + a' ; b + b')$$

y el par obtenido representa al número entero α''. El resultado es único en virtud de la estabilidad de la operación.

Propiedades de la adición de números enteros

Es fácil probar que la adición de enteros es conmutativa, asociativa y cancelativa, demostraciones que se proponen como ejercicios.

Existencia de elemento neutro. Si existe, el módulo será un entero que representaremos por el par $(m ; n)$ perteneciente a la clase que lo define y tal que:

$$(a ; b) + (m ; n) = (a ; b)$$

Por def. de adición:

$$(a + m ; b + n) = (a ; b)$$
$$a + m + b = b + n + a$$

y por ley cancelativa:

$$m = n$$

Luego el elemento neutro es el entero de la forma:

$$e = (m ; m)$$

Que, según se ha visto, corresponde al número 0.

Existencia del opuesto. Sea el entero α, representado por el par $(a ; b)$; si existe su opuesto α', que podemos representar por $(a' ; b')$, debe verificarse, por definición:

$$(a ; b) + (a' ; b') = (m ; m)$$

O sea:

$$(a + a' ; b + b') = (m ; m)$$

Es decir:

$$a + a' + m = b + b' + m$$

Luego

$$a + a' = b + b'$$

y por def. de igualdad

$$(a' ; b') = (b ; a)$$

Luego el opuesto de un número entero $\alpha = (a ; b)$, queda representado por $(b ; a)$ y se lo indica por $\alpha' = -\alpha$

Consecuencia

El conjunto Z provisto de la ley de adición, es decir $(Z, +)$ constituye un grupo abeliano.

Multiplicación de números enteros

De manera similar a la adición, se define la multiplicación. Para ello se introduce la siguiente ley de composición en $E = N \times N$.

$$(a ; b) \cdot (c ; d) = (ac + bd ; bc + ad)$$

Se demuestra, como en el caso de la adición, que la operación es estable respecto a la relación de equivalencia definida en E y se tiene que: si $\alpha =$ clase $(a ; b)$ y $\beta =$ clase $(c ; d)$, eligiendo un representante de cada clase:

$$\alpha \cdot \beta = (a ; b) \cdot (c ; d)$$
$$\alpha \cdot \beta = (ac + bd ; bc + ad)$$

Donde el segundo miembro es un par de $N \times N$ que pertenece a una cierta clase que define al entero γ.

Propiedades de la multiplicación de enteros

a) **conmutatividad:** $\alpha \cdot \beta = \beta \cdot \alpha$

b) **asociatividad:** $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$

c) **Existencia del neutro:** $\alpha \cdot \varepsilon = \alpha$

d) **Cancelativa para elementos no nulos:**

$$\alpha \neq 0 \wedge \alpha \cdot \beta = \alpha \cdot \gamma \Rightarrow \beta = \gamma$$

e) **distributividad con respecto a la adición:**

$$\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$$

Demostraremos las propiedades c) y e) dejando las demás, dada su sencillez, a cargo del lector, como ejercicio.

c) De existir el elemento neutro, al que representamos por $(p\,;q)$, para todo número entero representado por $(a\,;b)$ debe verificarse.

$$(a\,;b)\cdot(p\,;q) = (a\,;b)$$

O sea:

$$(ap+bq\,;bp+aq) = (a\,;b)$$

Es decir:

$$ap+bq+b = bp+aq+a$$

Y por propiedades de los números naturales:

$$ap+b(q+1) = bp+a(q+1)$$

Ecuación con incógnitas p y q, donde es suficiente que se verifique:

$$p = q+1$$

Luego el par $(p\,;q)$, tiene la forma: $(q+1\,;q)$

Es decir, existe el elemento neutro $u =$ clase $(q+1\,;q)$

e) Siendo $(a\,;b)$, $(c\,;d)$ y $(r\,;s)$ representantes de las clases que definen α, β y γ, respectivamente:

$$\begin{aligned}\alpha\cdot(\beta+\gamma) &= (a\,;b)\,[(c\,;d)+(r\,;s)] = (a\,;b)\,(c+r\,;d+s) = \\ &= (ac+ar+bd+bs\,;ad+as+bc+br) \qquad (1)\end{aligned}$$

$$\begin{aligned}\alpha\cdot\beta+\alpha\cdot\gamma &= (a\,;b)\,(c\,;d)+(a\,;b)\,(r\,;s) = \\ &= (ac+bd\,;bc+ad)+(ar+bs\,;as+br) = \\ &= (ac+bd+ar+bs\,;bc+ad+as+br) \qquad (2)\end{aligned}$$

De (1) y (2):

$$\alpha\cdot(\beta+\gamma) = \alpha\cdot\beta+\alpha\cdot\gamma$$

13. ISOMORFISMO ENTRE LOS NÚMEROS NATURALES Y LOS ENTEROS POSITIVOS

Es inmediato que si establecemos la aplicación:

$$f: N \to Z+ \,/\, \forall a \in N: f(a) = \text{clase } (a+y\,;y),$$

dicha aplicación es biyectiva. Probaremos que es un isomorfismo con respecto a las operaciones de adición y multiplicación. En efecto,

$$f(a+b) = \text{clase } [(a+b)+y\,;y]$$

y

$$f(a) + f(b) = \text{clase } (a + m \,;\, m) + \text{clase } (b + n \,;\, n)$$
$$= \text{clase } [(a + b) + (m + n) \,;\, m + n]$$

Pero clase $[(a + b) + y \,;\, y] = \text{clase } [(a + b) + (m + n) \,;\, m + n]$

Luego:

$$f\,(a + b) = f\,(a) + f\,(b) \Rightarrow$$

$\Rightarrow$ f es un isomorfismo respecto de la adición.

Análogamente se prueba que es un isomorfismo con respecto al producto

$$f\,(a \cdot b) = \text{clase } [(a \cdot b) + y \,;\, y]$$

y

$$f\,(a) \cdot f\,(b) = \text{clase } (a + m \,;\, m) \cdot \text{clase } (b + n \,;\, n)$$

$$= \text{clase } [(a \cdot b) + \underbrace{an + bm + 2\,mn}_{p} \,;\, \underbrace{an + bm + 2\,mn}_{p}]$$

Pero clase $[(a \cdot b) + y \,;\, y] = \text{clase } [(a \cdot b) + p \,;\, p]$

Luego:

$$f\,(a \cdot b) = f\,(a) \cdot f\,(b) \Rightarrow$$

$\Rightarrow$ f es un isomorfismo para la multiplicación.

En consecuencia: el conjunto de los números enteros Z contiene un conjunto Z^+, isomorfo al de los números naturales con respecto a las dos leyes de composición que configuran sus estructuras.

Por lo tanto el número natural a puede representarse por el entero positivo $+a$ y recíprocamente:

$$a = +a$$

14. SUSTRACCIÓN DE NÚMEROS ENTEROS

La ecuación $x + \alpha = \beta$ tiene siempre solución en el campo de los números enteros y esta solución es única, puesto que los números enteros forman grupo para la adición y aquella es propiedad general de todo grupo.

La solución es $x = \beta + \alpha'$

Resulta entonces según se ha visto en el capítulo de estructuras, que a expensas de la adición puede definirse siempre otra operación: la sustracción.

Definición

Dados dos números enteros β y α, se llama sustracción a la

operación interna que asocia a dos enteros dados otro entero x tal que $\alpha + x = \beta$

Se indica

$$\beta - \alpha = x$$

$$\text{Luego } \beta - \alpha = x \Leftrightarrow \alpha + x = \beta$$

El entero x se llama resta o diferencia; el primer número β se llama minuendo y el segundo α sustraendo.

Corolario

La sustracción de dos números enteros equivale a la adición entre el minuendo y el opuesto del sustraendo.

Es decir:

$$\beta - \alpha = \beta + (-\alpha)$$

Observación

Si se considera el caso particular en que α y β son dos enteros positivos, o sea $\alpha = +a$ y $\beta = +b$

$\beta - \alpha = (+b) - (+a) = b - a$ (1) por el isomorfismo entre enteros positivos y naturales. Y teniendo en cuenta el significado de entero positivo:

$$\beta - \alpha = (b + m ; m) - (a + n ; n)$$

Luego

$$\beta - \alpha = (b + m ; m) + (n ; a + n),$$

por el corolario de la definición de sustracción y por el significado de opuesto de un entero.

Es decir:

$\beta - \alpha = (b + m + n ; m + a + n)$, por definición de adición de enteros; o sea

$$\beta - \alpha = (b ; a) \qquad (2)$$

De (1) y (2)

$$b - a = (b ; a)$$

De aquí resulta que el punto y coma que se empleó como signo de separación entre los números naturales que componen el par $(b ; a)$ y que como sabemos representa un entero, significa siempre el signos menos.

Como el razonamiento es válido cualesquiera sean $+b$ y $+a$, resulta el siguiente:

Corolario

Todo número entero es la diferencia de dos números naturales

Observación

Dados los números naturales b y a, el entero γ queda unívocamente determinado por la clase de equivalencia del par (b ; a) y, por lo visto

$$\gamma = b - a$$

Si

$$b > a \Rightarrow \gamma = +c$$
$$b = a \Rightarrow \gamma = 0$$
$$b < a \Rightarrow \gamma = -c$$

La recíproca no se cumple, es decir, γ puede ser considerado como diferencia de infinitos pares de números naturales, todos los que constituyen los pares que pertenecen a la clase de equivalencia γ.

15. PROPIEDADES ESTRUCTURALES DE LOS NÚMEROS ENTEROS

Se ha definido entre los enteros una ley de composición interna, la adición, que como se ha visto le confiere estructura de grupo abeliano. Una segunda ley, la multiplicación, es asociativa, conmutativa, cancelativa, doblemente distributiva con respecto a la primera y con unidad. Así el conjunto Z, con las operaciones de adición y multiplicación adquiere estructura de anillo conmutativo, de integridad y unitario, es decir, es un dominio de integridad.

1. — $(Z, +)$ es grupo abeliano aditivo
2. — $(Z, +, \cdot)$ es anillo conmutativo con unidad
3. — $(Z, +, \cdot)$ es anillo de integridad
4. — $(Z, +, \cdot)$ es dominio de integridad

16. CONSTRUCCIÓN AXIOMÁTICA DE LOS ENTEROS

Se toman como conceptos primitivos:
un conjunto $Z = \{\alpha, \beta, \gamma, \dots\}$, cuyos elementos se llaman números enteros y dos operaciones internas, adición y multiplicación, que se definen implícitamente por las siguientes propiedades primitivas o axiomas que los caracterizan:

$Z_1 : \alpha + \beta = \beta + \alpha$

$Z_2 : (\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$

$Z_3 : \forall \alpha \in Z, \exists 0 \in Z / \alpha + 0 = \alpha$

Z_4 : $\forall \alpha \in Z$, $\exists -\alpha \in Z / \alpha + (-\alpha) = 0$

Z_5 : $\alpha \cdot \beta = \beta \cdot \alpha$

Z_6 : $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$

Z_7 : $\forall \alpha \in Z, \exists\, 1 \in Z / \alpha \cdot 1 = \alpha$

Z_8 : $\alpha \cdot \beta = \alpha \cdot \gamma \wedge \alpha \neq 0 \Rightarrow \beta = \gamma$

Z_9 : $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$

Z_{10}: Existe un subconjunto Z^+ de Z, llamado de enteros positivos, que satisface las siguientes condiciones:

a) $\alpha \in Z \Rightarrow \alpha \in Z^+ \veebar \alpha = 0 \veebar -\alpha \in Z^+$

b) $\forall \alpha, \forall \beta \in Z^+ \Rightarrow \alpha + \beta \in Z^+ \wedge \alpha \cdot \beta \in Z^+$

Z_{11}: Si $\left.\begin{array}{l} P \subseteq Z \wedge \alpha \in P \Rightarrow -\alpha \in P \\ \wedge\, \alpha \in P \wedge \beta \in P \Rightarrow \alpha + \beta \in P \wedge \alpha \cdot \beta \in P \\ \wedge\, 1 \in P \end{array}\right\} \Rightarrow P = Z$

Los axiomas Z_1 al Z_9 dan a Z la estructura de dominio de integridad.

El Z_{10} se expresa diciendo que Z es ordenado.

El Z_{11} indica que no hay ningún subdominio de integridad contenido en Z, distinto de Z.

EJERCICIOS

1. — *Demostrar, aplicando el principio de inducción completa, las propiedades de la adición y de la multiplicación de números naturales enunciadas en el texto.*

2. — *Se define en el conjunto N la relación*

$$a < b \Longleftrightarrow \exists x / a + x = b$$

Demostrar que dicha relación es de orden lineal y estricto en N.

3. — *Demostrar que el orden definido en el ejercicio 2 es un buen orden en N.*

4. — *Demostrar las propiedades conmutativa y asociativa de la adición de números enteros.*

5. — *Demostrar la asociatividad y conmutatividad de la multiplicación de enteros.*

6. — *Demostrar que:*

$$[\alpha \cdot \beta = 0 \wedge \alpha \neq 0] \Longrightarrow \beta = 0$$

7. — *Demostrar*

$$\forall \alpha \in Z^- \wedge \forall \beta \in Z^- : \alpha + \beta \in Z^-$$

8. — *Demostrar*

$$\forall \alpha \in Z^+ \wedge \forall \beta \in Z^- : \alpha \cdot \beta \in Z^-$$

9. — *Demostrar*

$$\forall \alpha \in Z^- \wedge \forall \beta \in Z^- : \alpha \cdot \beta \in Z^+$$

10. — *Demostrar*

$$\forall \alpha \in Z : \alpha \cdot 0 = 0 .$$

CAPITULO VIII

Introducción a la aritmética trasfinita

1. DEFINICIONES Y PROPIEDADES USUALES

Existe una premisa fundamental relativa a la aritmética finita, es decir, la que maneja conjuntos finitos y opera con ellos, y consiste en este enunciado simple y absolutamente intuitivo: "el todo es mayor que cualquiera de sus partes propias". Esta situación no se mantiene al considerar conjuntos infinitos, respecto de los cuales la propiedad anterior se transforma precisamente en su opuesta: "en un conjunto infinito el todo no es mayor que alguna de sus partes propias". La intuición no tiene cabida aquí, y por consiguiente no será posible que acompañe a las seguras e ineludibles razones lógicas y de pensamiento, que son las que cuentan definitivamente y en última instancia. Este hecho fue estudiado e investigado por el genial Georg Cantor, señalado como el padre de la "aritmética trasfinita". El origen de muchos progresos y conquistas suele ser una especie de admiración por las cosas insólitas o sublimes; es allí donde ubicamos la génesis de la tarea de Cantor, que hizo escuela a fines del siglo pasado.

Vamos a iniciar la introducción a la aritmética trasfinita con el enunciado de algunas definiciones y proposiciones, cuyas demostraciones hemos obviado, según corresponde a la naturaleza del presente texto.

Definición

Se llama sección o intervalo natural inicial I_n al conjunto de los n primeros números naturales.

$$I_n = \{1, 2, 3, \ldots\ldots, n\}$$

Definición

Dos conjuntos son equipotentes o coordinables, si y sólo si existe una aplicación biyectiva entre los mismos.

$$X \,\bar{\sim}\, Y \Leftrightarrow \exists f : X \to Y \,/\, f \text{ es biyectiva}$$

Definición

Un conjunto es finito, si y sólo si es vacío, o bien coordinable con un intervalo natural inicial.

$$X \text{ es finito} \Leftrightarrow X = \emptyset \vee \exists n \in N / X \; \pi \; I_n$$

Esta definición es equivalente a la dada en el cap. VII

Definición

Un conjunto es infinito si y sólo si no es finito.

Proposición

Todo subconjunto de un conjunto finito, es finito.

$$X \text{ finito y } X' \subseteq X \Rightarrow X' \text{ es finito}$$

Proposición

Un conjunto es infinito si y sólo si admite un subconjunto coordinable con N.

Proposición

Un conjunto es infinito si y sólo si es coordinable con una parte propia de sí mismo.

$$X \text{ es infinito} \Leftrightarrow \exists X' \subset X / X \; \pi \; X'$$

Consecuencia

Un conjunto es finito si y sólo si no es coordinable con ninguna parte propia de sí mismo.

Ejemplo

En virtud de la propiedad anterior, podemos demostrar que el conjunto Z de los enteros es infinito, por ser coordinable con el conjunto de los números pares P. En efecto, sean:

$$Z = \{\ldots\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\ldots\}$$
$$P = \{\ldots\ldots -4, -2, 0, 2, 4, \ldots\ldots\}$$

Se tiene: $P \subset Z$ *pues* $(x \in P \Rightarrow x \in Z) \wedge \exists y \in Z / y \notin P$.

Es decir, el conjunto de los números pares es una parte propia del conjunto *de los enteros. En estas condiciones, definimos la aplicación:*

$$f: Z \to P \quad \text{del siguiente modo: } f(x) = 2x$$

Tal aplicación es inyectiva y sobre, es decir, biyectiva.

En consecuencia, ambos conjuntos son equipotentes o coordinables, lo cual prueba que Z es infinito.

2. NÚMEROS CARDINALES Y CONJUNTOS NUMERABLES

Definición

Número cardinal del conjunto finito no vacío A es el número n, si y sólo si A es coordinable con I_n. El número cardinal del conjunto vacío es cero.

$$c(A) = n \Leftrightarrow A \ \bar{\times} \ I_n$$
$$c(A) = 0 \Leftrightarrow A = \varnothing$$

El símbolo c(A) se leerá: número cardinal del conjunto A .

El concepto de número cardinal se extiende a los conjuntos infinitos en cuyo caso, los números que se engendran, reciben el nombre de números cardinales **trasfinitos.** El número cardinal asociado a un conjunto revela su potencia o "numerosidad", y jerarquiza al conjunto desde el punto de vista de la cuantía de sus elementos. Los términos número cardinal y potencia son sinónimos. Hemos dicho que las cosas suceden de un modo naturalmente intuitivo cuando se trabaja con conjuntos finitos, es decir, con números cardinales finitos; pero la sorprendente propiedad de que "un conjunto infinito es coordinable con una parte propia de sí mismo", hace que la operatoria con números cardinales trasfinitos no siga las leyes usuales de la aritmética finita.

Definición

Dos conjuntos admiten el mismo número cardinal si y sólo si son coordinables.

$$c(X) = c(Y) \Leftrightarrow X \ \bar{\times} \ Y$$

Esta definición es general y aplicable por lo tanto a conjuntos finitos o infinitos. Consecuencia de la misma, y de lo demostrado antes, es el hecho de que el conjunto de los enteros y de los números pares, están representados por el mismo número cardinal trasfinito. Del mismo modo se puede probar que el conjunto N tiene el mismo número cardinal que el conjunto de los pares positivos. Cantor propuso el símbolo $\aleph_0$ para designar el número cardinal del conjunto N de los naturales, es decir:

$$c(N) = \aleph_0$$

Resulta así que todo conjunto coordinable con N admite el número cardinal $\aleph_0$ de acuerdo con la siguiente:

Definición

Un conjunto tiene potencia $\aleph_0$ si y sólo si es coordinable con N

$$c(X) = \aleph_0 \Leftrightarrow X \sim N$$

Definición

Un conjunto es numerable si y sólo si su número cardinal es $\aleph_0$

3. COMPARACIÓN DE NÚMEROS CARDINALES

Definición

Dados dos conjuntos X e Y, se dice que $c(X) \leqslant c(Y)$ si y sólo si X es coordinable con una parte de Y.

$$c(X) \leqslant c(Y) \Leftrightarrow \exists Z \subseteq Y \,/\, X \sim Z$$

La relación $\leqslant$ así definida, es de orden amplio, ya que verifica los axiomas:

I) **Reflexividad:**

$$\forall X \quad \text{es} \quad c(X) \leqslant c(X)$$

II) **Transitividad:**

$$c(X) \leqslant c(Y) \wedge c(Y) \leqslant c(Z) \Rightarrow c(X) \leqslant c(Z)$$

III) **Antisimetría:**

$$c(X) \leqslant c(Y) \wedge c(Y) \leqslant c(X) \Rightarrow c(X) = c(Y)$$

La demostración de esta importante propiedad no es simple y es objeto del célebre teorema de Cantor-Bernstein, cuyo enunciado es el siguiente:

"**Si un conjunto es coordinable con una parte de otro, y éste**

es coordinable con una parte del primero, entonces ambos conjuntos son coordinables."

Como aplicación, demostramos el siguiente:

Teorema

El conjunto de los números primos positivos tiene potencia $\aleph_0$. (1)

Desdoblamos la demostración en dos partes:

1º) **El conjunto P = {primos positivos} es infinito**

Supongamos que P es finito; en este caso $P \nsim I_n$, es decir, sólo existen n números primos: $p_1, p_2, \ldots, p_n$

Formamos el número natural

$$a = \left(\prod_{i=1}^{n} p_i\right) + 1 \qquad (1)$$

Por el teorema fundamental de la aritmética, este número admite un divisor primo, es decir

$$\exists p_j \in P \,/\, p_j \mid a$$

Caben dos posibilidades:

a) $p_j = a \implies \exists a$ primo y mayor que todo p_i, proposición contradictoria con la suposición de partida.

b) $p_j \neq a$.

Entonces, por definición de divisor, se tiene:

$$a = p_j \cdot m \ (2) \qquad \text{siendo } m \in N$$

De (1) y (2), por transitividad resulta:

$$m \cdot p_j = \left(\prod_{i=1}^{n} p_i\right) + 1$$

y en consecuencia: $m \cdot p_j - \prod_{i=1}^{n} p_i = 1 \qquad (3)$

Siendo por otra parte p_j primo, debe identificarse con algún p_i

---

(1) Recordamos lo siguiente:

Definición: Un entero p es primo, si y sólo si es distinto de 0, de ± 1, y además divisible únicamente por ± 1 y $\pm p$.
Los enteros distintos de 0 y de ± 1 que no son primos, se llaman compuestos.

desde que hemos supuesto la existencia de n números primos solamente; y por lo tanto:

$$\prod_{i=1}^{n} p_i = p_j \cdot q \qquad (4)$$

entendiéndose que q denota el producto de los (n — 1) primos distintos de p_j. Por sustitución de (4) en (3), queda:

$$m \cdot p_j - p_j \cdot q = 1$$

lo que implica:

$$p_j \cdot (m - q) = 1$$

Y por definición de divisor resulta $p_j \mid 1$

Como los únicos divisores de 1 son $+1$ y -1, se tiene: $p_j = \pm 1$

ABSURDO, pues p_j es primo.

2º) P **es coordinable con** N

Siendo P infinito por propiedad anterior admite un subconjunto P' coordinable con N, es decir: $c(N) \leqslant c(P) \qquad (5)$

Además, $P \subset N \Rightarrow c(P) \leqslant c(N) \qquad (6)$

De (5) y (6), por el teorema de Cantor-Bernstein, resulta:

$$c(P) = c(N) = \aleph_0$$

4. PROPIEDADES DE LOS CONJUNTOS NUMERABLES

El método característico que permite demostrar la numerabilidad de un conjunto, consiste en la posibilidad de establecer una correspondencia biunívoca del mismo con el conjunto de los números naturales, es decir, de formar una sucesión con sus elementos. Utilizando este procedimiento sencillo, es posible demostrar las siguientes propiedades:

I) **La unión de un conjunto numerable y de un conjunto finito, es un conjunto numerable.**

II) **La unión de un número finito de conjuntos numerables es un conjunto numerable.**

La demostración, debida a Cantor, consiste en la aplicación del conocido "proceso diagonal", mediante el cual se forma una sucesión con todos los elementos de los conjuntos dados.

Sean m conjuntos numerables:

$$C_i = \{a_{i1}, a_{i2}, a_{i3}, \ldots, a_{in}, \ldots\}$$

 siendo $i = 1, 2, 3, \ldots, m$

Se trata de probar que: $C = \bigcup_{i=1}^{m} C_i \curlywedge N$

Para ello disponemos los elementos de los m conjuntos numerables según lo indica el siguiente cuadro:

$$\begin{array}{l}
a_{11}\ a_{12}\ a_{13}\ a_{14}\ \ldots\ldots\ a_{1n}\ \ldots\\
a_{21}\ a_{22}\ a_{23}\ a_{24}\ \ldots\ldots\ a_{2n}\ \ldots\\
a_{31}\ a_{32}\ a_{33}\ a_{34}\ \ldots\ldots\ a_{3n}\ \ldots\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
a_{m1}\ a_{m2}\ a_{m3}\ a_{m4}\ \ldots\ldots\ a_{mn}\ \ldots
\end{array}$$

Siguiendo el esquema diagonal indicado por las flechas, formamos la sucesión:

$$a_{11}\,,\ a_{21}\,,\ a_{12}\,,\ a_{31}\,,\ a_{22}\,,\ a_{13}\,,\ \ldots\ldots,\ a_{ij}\,,\ \ldots \qquad (1)$$

Los elementos del conjunto unión están ordenados así: de dos elementos, es anterior aquél cuya suma de subíndices es menor, y en caso de igual suma es anterior aquél cuyo segundo subíndice es menor.

Introducimos la aplicación $f: C \to N$ cuyo dominio es el conjunto unión, y que definimos así:

$$f(a_{ij}) = \frac{(i+j-1)(i+j-2)}{2} + j \qquad (2)$$

La imagen de todo elemento de (1) es un elemento de N, puesto que siendo $(i+j-1)$ e $(i+j-2)$ enteros no negativos consecutivos, su producto es par y el cociente por 2 es un entero no negativo (sólo nulo para $i = j = 1$), el cual sumado a j, determina un número natural.

Así:

$$f(a_{11}) = 1$$
$$f(a_{21}) = 2$$
$$f(a_{12}) = 3\,,\ \text{etc.}$$

Se demuestra que la aplicación (2) es inyectiva y sobre; por tanto, es biyectiva, es decir: $C \curlywedge N$

En consecuencia $C = \bigcup_{i=1}^{m} C_i$ es numerable, como queríamos demostrar.

III) **La unión de una familia numerable de conjuntos finitos disjuntos es numerable.**

IV) **La unión de una familia numerable de conjuntos numerables, es numerable.**

5. POTENCIA DEL CONJUNTO DE LOS RACIONALES

Teorema

El conjunto de los números racionales es numerable.

Hipótesis) $Q = \{\text{racionales}\}$

Tesis) $c(Q) = \aleph_0$.

Demostración) Nos restringimos primero a los racionales positivos, con los cuales confeccionamos un cuadro del siguiente modo: en la primera fila figuran los racionales de denominador 1; en la segunda, los de denominador 2, y así sucesivamente:

$$\begin{array}{cccccc}
\frac{1}{1} & \frac{2}{1} & \frac{3}{1} & \frac{4}{1} & \cdots\cdots & \frac{n}{1} \;\cdots\cdot \\
\frac{1}{2} & \frac{2}{2} & \frac{3}{2} & \frac{4}{2} & \cdots\cdots & \frac{n}{2} \;\cdots\cdot \\
\frac{1}{3} & \frac{2}{3} & \frac{3}{3} & \frac{4}{3} & \cdots\cdots & \frac{n}{3} \;\cdots\cdot \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
\frac{1}{n} & \frac{2}{n} & \frac{3}{n} & \frac{4}{n} & \cdots & \frac{n}{n} \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots
\end{array}$$

Aplicamos el proceso diagonal siguiendo la indicación de las flechas y queda formada la sucesión:

$$1/1\,,\,2/1\,,\,1/2\,,\,1/3\,,\,2/2\,,\,3/1\,,\,4/1\,,\,3/2\,,\,2/3\,,\,1/4\,,\ldots\ldots$$

de la cual suprimimos las fracciones cuyos términos no son primos entre sí, para que cada racional figure una sola vez, y se obtiene la sucesión resultante:

$$\begin{array}{ccccccccc}
1, & 2, & 1/2, & 1/3, & 3, & 4, & 3/2, & 2/3, & \ldots\ldots \\
\updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\
1, & 2, & 3, & 4, & 5, & 6, & 7, & 8, & \ldots\ldots
\end{array}$$

La correspondencia biunívoca establecida permite afirmar que $Q^+ \barwedge N$. De modo análogo, los racionales negativos constituyen un conjunto numerable, es decir: $Q^- \barwedge N$.

El conjunto de los racionales está formado por los racionales positivos, los negativos y el cero, esto es:

$$Q = Q^{+} \cup Q^{-} \cup \{0\}$$

Por tratarse de la unión de dos conjuntos numerables y de un conjunto finito, resulta numerable, lo cual implica que $c(Q) = \aleph_0$.

6. POTENCIA DEL CONJUNTO DE LOS NÚMEROS REALES

Hemos visto que todos los conjuntos infinitos estudiados hasta ahora: naturales, enteros, pares, primos y racionales admiten la misma potencia $\aleph_0$, y cabe preguntarse naturalmente si no se trata de una característica común a todo conjunto infinito. El mismo Cantor probó que tal cosa no sucede, al demostrar la no numerabilidad del conjunto de los números reales.

I) **El conjunto de los números reales es coordinable con el conjunto de los reales del intervalo abierto** (0 ; 1).

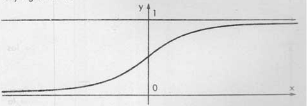
En efecto: consideramos la aplicación de Klein:

$$f : R \rightarrow (0\,;\,1)$$

definida así:

$$f(x) = -\frac{1}{\pi}\,\text{arc cotg}\,x$$

cuyo gráfico es



Tal aplicación estrictamente creciente es biyectiva, lo cual implica que el dominio y el rango son equipotentes, es decir:

$$R \sim (0\,;\,1)$$

II) **El conjunto de los números reales del intervalo** (0 ; 1) **es no numerable.**

La demostración de Cantor consiste en suponer que los reales del intervalo (0 ; 1) forman una sucesión (en cuyo caso se trataría de un conjunto numerable), y en construir posteriormente un número real del mismo intervalo que no figura en la misma, es decir, sin correspondiente en el conjunto N.

Consideramos la supuesta sucesión de todos los reales del intervalo abierto (0 ; 1), con infinitas cifras decimales:

$$R \begin{cases} 0, a_1a_2a_3 \ldots\ldots \\ 0, b_1b_2b_3 \ldots\ldots \\ 0, c_1c_2c_3 \ldots\ldots \\ \ldots\ldots\ldots\ldots \end{cases}$$

Mediante un proceso diagonal, construimos un número real del mismo intervalo que no figura en la sucesión. Para ello elegimos como primera cifra decimal un número natural a distint- de a_1, de 0 y de 9; como segunda cifra un número b distinto de [illegible] 0 y de 9, y así sucesivamente. Queda formado el número [illegible]

$$\alpha = 0, a\,b\,c \ldots\ldots$$

Este número es distinto de todos los que figuran en la sucesión, pues difiere de cada uno de ellos en alguna cifra decimal, por construcción.

Por otra parte, α pertenece al intervalo (0 ; 1), pues la elección de sus cifras, que son distintas de 0 y de 9, elimina la eventual posibilidad de identificarse con los extremos 0 y 1.

En consecuencia, la supuesta sucesión no contiene a todos los reales, y resulta

$$(0 ; 1) \not\sim N$$

Esto implica, por I), que $R \not\sim N$, es decir: $c(R) \neq \aleph_0$. lo que demuestra, precisamente, el teorema.

Para denotar la cardinabilidad del conjunto de los re-les, introducimos la siguiente:

Definición

Se llama potencia del continuo c, al número cardinal del conjunto no numerable de los reales.

Es decir:

$$c(R) = c$$

7. NÚMEROS ALGEBRAICOS Y TRASCENDENTES

Definición

Un número es algebraico si y sólo si es raíz de una ecuación algebraica con coeficientes enteros.

La estructura de una ecuación algebraica con coeficientes enteros, de grado n, es del tipo:

$$\sum_{i=0}^{n} a_i x^i = 0 \ , \text{ con } n \geqslant 1 \wedge a_n \neq 0 \wedge a_i \in Z$$

cuyo desarrollo es:

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0 \qquad (1)$$

entonces, el número α es algebraico si y sólo si es raíz de (1)

Consecuencias inmediatas

a) Los números enteros son algebraicos.

En efecto, sea $p \in Z$. Dicho entero p es raíz de la ecuación algebraica con coeficientes enteros:

$$x - p = 0$$

y esto prueba que p es algebraico.

b) Los racionales son números algebraicos.

Sea $p/q \in Q$; el mismo es raíz de la siguiente ecuación algebraica con coeficientes enteros:

$$qx - p = 0$$

y en consecuencia, cualquier racional es algebraico.

c) Existen irracionales que son algebraicos.

Consideremos el número irracional $\sqrt{2}$. Tal número es raíz de la ecuación

$$x^2 - 2 = 0$$

y por lo tanto, $\sqrt{2}$ es un número algebraico.

Podría pensarse en primera instancia que todos los números reales son algebraicos; pero esta posibilidad no se mantiene desde que el mismo Cantor demostró que el conjunto de los números algebraicos es numerable y como sabemos, el de los reales no lo es. Este teorema es el objeto del parágrafo siguiente y prueba el hecho fundamental de la existencia de números reales no algebraicos, a los cuales se los llama trascendentes, de acuerdo con lo siguiente:

Definición

Un número es trascendente si y sólo si es no algebraico.

Altura de una ecuación algebraica

Definición

Se llama altura de una ecuación algebraica con coeficientes enteros, a la suma de los valores absolutos de sus coeficientes y del grado de la misma.

Sea la ecuación

$$\sum_{i=0}^{n} a_i x^i = 0$$

Su altura es, por definición, el número natural:

$$h = |a_n| + |a_{n-1}| + \ldots\ldots + |a_1| + |a_0| + n$$

es decir:

$$h = \sum_{i=0}^{n} |a_i| + n$$

Surge de la definición dada, que para cada altura h existe un número finito de ecuaciones algebraicas asociadas.

En efecto, siendo la ecuación de grado n, se tiene $a_n \neq 0$, y en consecuencia: $h > |a_n|$ y $h > n$.

Los posibles valores para a_n son:

$$\pm 1, \pm 2, \ldots\ldots, \pm (h-1)$$

y para $a_i \neq a_n$ dichos valores posibles son:

$$0, \pm 1, \pm 2, \ldots\ldots, \pm (h-2)$$

Es decir, el número posible de valores que puede adoptar el primer coeficiente no supera a $2(h-1)$ y, en consecuencia, es menor que $2h$.

Del mismo modo, para todo coeficiente que no sea el primero, dicho número no supera a $2(h-2)+1$, es decir, es menor que $2h$.

De donde resulta que el número de ecuaciones algebraicas de altura h, es finito y seguramente menor que $(2h)^{n+1} \leqslant (2h)^h$ por tratarse de las variaciones con repetición de $2h$ elementos de orden $(n+1)$.

8. POTENCIA DEL CONJUNTO DE LOS NÚMEROS ALGEBRAICOS

Teorema

El conjunto de los números algebraicos es numerable.

Hipótesis) $A = \{\text{algebraicos}\}$

Tesis) $c(A) = \aleph_0$

Demostración) De acuerdo con lo establecido anteriormente, para cada altura h existe un número finito de ecuaciones algebraicas con coeficientes enteros, el cual es

$$N < (2h)^h$$

Como cada ecuación admite a lo sumo n raíces distintas, ocurre que el mayor número posible de números algebraicos asociados a la altura h, es

$$N_a < (2h)^h \cdot n < (2h)^h \cdot h \text{ puesto que } n < h$$

Es decir

$$N_a < 2^h \cdot h^{h+1}$$

Esto significa que para cada altura h, el número de números algebraicos es finito; y podemos obtener, para la sucesión natural de alturas, el conjunto de todos los números algebraicos como la unión de un conjunto numerable de conjuntos finitos, el cual, como sabemos, es numerable.

9. NÚMEROS TRASCENDENTES

Sabemos que el conjunto de los números reales es no numerable, y que el subconjunto de los reales algebraicos es numerable. Por otra parte, hemos definido los números trascendentes, que son irracionales, como los no algebraicos. Ciñéndonos al campo real, se tiene:

$$R = A \cup T$$

siendo T el conjunto de los números trascendentes. Resulta claro que T es **no numerable** pues, en caso contrario, su unión con A, que es numerable, sería también numerable, lo que es absurdo.

Para probar que un número es trascendente se necesita demostrar que no es raíz de ninguna ecuación algebraica con coeficientes enteros.

En 1783 Hermite demostró la trascendencia de e, y en 1882 Lindemann hizo lo propio con π. Siegel y Gelfond demostraron la trascendencia de los números del tipo α^β, siendo α algebraico distinto de 0 y de 1 y β un irracional algebraico. De este modo son trascendentes:

$$2^{\sqrt{2}},\ 3^{\sqrt{2}},\ 5^{\sqrt{3}},\ \text{etc.}$$

La potencia del conjunto de los números trascendentes, lo mismo que la del conjunto de los irracionales, es la del continuo:

$$c(T) = c(I) = c(R) = c$$

10. POTENCIA DEL CONJUNTO DE LAS FUNCIONES REALES

Se demuestra que el número cardinal trasfinito c, es la potencia del conjunto de los puntos del plano, del espacio tridimensional y, en general, del espacio de un número finito de dimensiones. Surge entonces de modo natural la posibilidad de investigar conjuntos infinitos cuya potencia sea mayor que la del continuo de los números reales.

Tal es el caso que se presenta al considerar el conjunto de las funciones reales definidas sobre cualquier intervalo real, cuya potencia es mayor que la del continuo, y se la denota con:

$$f = c(F)$$

La obtención de números cardinales trasfinitos de potencia mayor, se logra mediante consideraciones análogas a las estudiadas, basadas en el proceso diagonal de Cantor. Se llega así a poner de manifiesto una jerarquía y distinción entre los conjuntos infinitos, cuyas tres categorías más usuales en matemática son:

- $\aleph_0$ número cardinal de los conjuntos numerables
- c número cardinal de los conjuntos que admiten la potencia del continuo
- f número cardinal de las funciones reales definidas en intervalos reales.

Se demuestra además:

$$\aleph_0 < c < f$$

EJERCICIOS

1. — *Demostrar que el conjunto de los números complejos de componentes naturales, es numerable.*

2. — *Demostrar que el intervalo abierto $(0;1)$ es coordinable con todo intervalo real $(a;b)$, siendo $a \neq b$*

   Sugerencia: probar primero que $(0:1) \sim (0;c)$ con $c \neq 0$, mediante la aplicación $f(x) = cx$

3. — *Probar que el conjunto bidimensional de los puntos del cuadrado*

$$\begin{cases} 0 < x < 1 \\ 0 < y < 1 \end{cases}$$

   es coordinable con los puntos del intervalo aierto $(0;1)$.

4. — *Demostrar que el intervalo $(-1;1)$ es coordinable con R, utilizando la aplicación de Frèchet:*

$$y = \frac{x}{1 + |x|}$$

5. — *Demostrar que la unión de un conjunto numerable con un conjunto que admite un subconjunto numerable es coordinable con el segundo.*

6. — *Utilizando el resultado del ejercicio anterior, demostrar que el conjunto de los irracionales tiene potencia c.*

SEGUNDA PARTE

CAPITULO IX

De la geometría clásica a la geometría moderna

En el desarrollo histórico de la geometría se señalan dos etapas fundamentales que corresponden a otras tantas concepciones esencialmente diferentes en su estructuración y fundamentos: la etapa intuitiva o experimental y la etapa racional.

La primera se extiende desde el nacimiento de la geometría como arte empírico o técnica experimental hasta el siglo VI antes de la era cristiana. Durante ella aparecen los primeros conocimientos geométricos, generalmente dispersos y desconectados entre sí, surgidos de necesidades materiales inmediatas, como la demarcación de terrenos y la medición de algunas superficies, y no son más que la consecuencia de observaciones directas o comprobaciones experimentales. Este período abarca las civilizaciones más antiguas: caldeos, babilonios y egipcios.

La segunda etapa se desarrolla a partir de los griegos, a cuyo genio creador estaba reservada la tarea de organizar y sistematizar esos conocimientos e incorporar otros nuevos hasta elaborar un cuerpo de doctrina científica, con criterio racional, en el que la deducción y el razonamiento sustituyen a la simple comprobación o a la intuición.

Este desarrollo racional de la geometría comienza con Tales de Mileto (siglo VI a.C.), continúa con Pitágoras y Platón y alcanza su nivel máximo en la escuela de Alejandría con Euclides, Arquímedes y Apolonio. Durante tres siglos la geometría se enriquece con el aporte considerable del trabajo de los geómetras griegos, pero es sólo con Euclides (siglo III a.C.) y su obra principal, **Los Elementos de Geometría,** cuando se estructura en su totalidad y aparece como un cuerpo orgánico y coherente, con un alto grado de perfección lógica.

Se carece de documentos originales de esta época; sólo se tienen noticias de la matemática griega a través de fuentes indirectas, por escritos y comentarios de investigadores, a veces varios siglos posteriores. Los pocos datos biográficos que se poseen sobre Euclides se deben a Proclo, matemático bizantino del siglo IV de nuestra era, y están condensados en un resumen histórico que acompaña su obra **Comentario al Libro I de Los Elementos de Euclides.**

Conforme a las referencias obtenidas, Proclo ubica a Euclides en el siglo III a.C. durante el reinado de Ptolomeo I. Sin embargo, la falta de testimonios directos hace que la existencia misma de Euclides se ponga en duda y se atribuya su obra a la labor conjunta o sucesiva de un grupo de geómetras.

1. "LOS ELEMENTOS"

Más que una obra de carácter original, **Los Elementos de Euclides** constituyen un tratado orgánico en el que se exponen sistemáticamente los resultados a que había arribado el genio griego, en el campo matemático, durante tres siglos de fecunda labor.

Es el libro más antiguo de fundamentación geométrica, en el que por vez primera se hace un desarrollo racional y coherente en sí mismo de la geometría, con un lenguaje claro y preciso y un ordenamiento lógico deductivo casi perfecto, sólo superado después de más de veinte siglos, cuando la refinada crítica moderna puso en evidencia algunas fallas en la construcción euclídea. Esto no obstante, los méritos de la obra son muy superiores a sus imperfecciones y ellos le valieron el ser elevada a un rango no alcanzado por tratado científico alguno, en el que se mantuvo casi hasta el presente, como texto obligado en los principales centros de estudio y como modelo de construcción y método aplicables no sólo a la geometría sino también a otros dominios de la ciencia.

El aspecto fundamental de la obra de Euclides es haber ordenado y estructurado como ciencia deductiva lo que hasta entonces era un conjunto de conocimientos desconectados por lo general y empíricos en su mayoría.

Siguiendo la orientación platónica de "cultivar la ciencia con el único objeto de conocer", Euclides deja de lado toda aplicación, numérica o geométrica, y se dedica a exponer, lógica y deductivamente, conocimientos geométricos puros, apelando a la razón como única fuente creadora.

Elabora así gran parte de la matemática forjada por sus antecesores y aun añade conocimientos nuevos. Pero **Los Elementos** no son ni una compilación ni un resumen de toda la geometría griega, ni tampoco contienen todas las propiedades que podrían deducirse del sistema de axiomas que fundamenta su obra. Como dice Proclo "son de admirar especialmente sus **Elementos de Geometría** por el orden que reina en ellos, por la elección de los teoremas y de los problemas considerados como fundamentales, puesto que no ha incluido todos aquellos que estaba en condiciones de dar, sino únicamente aquellos capaces de funcionar como elementos".

Los **Elementos** están constituidos por trece libros, con un total de cuatrocientas sesenta y cinco proposiciones, de las cuales trescientas setenta y dos son teoremas, y noventa y tres problemas teóricos.

Los cuatro primeros libros se refieren a cuestiones de geometría plana. El libro I, el más importante del tratado, contiene cuarenta y ocho proposiciones, que se pueden clasificar de la siguiente manera:

a) Construcciones, que se inician con el transporte de segmentos y siguen más adelante con el de ángulos y triángulos.
b) Criterios de igualdad de triángulos.
c) Perpendicularidad de rectas.
d) Relaciones entre ángulos que forman dos rectas secantes.
e) Relaciones entre lados y ángulos de un triángulo.
f) Paralelismo de rectas.
g) Equivalencia de triángulos y paralelogramos.
h) Relaciones entre los lados de un triángulo rectángulo (teorema de Pitágoras y su recíproco).

El libro II comienza con las propiedades algebraicas elementales de sumas y productos expresados geométricamente. Sigue con los problemas de división de un segmento en media y extrema razón, y termina con la generalización del teorema de Pitágoras a triángulos no rectángulos.

En los libros III y IV se tratan, respectivamente, las propiedades de la circunferencia y los polígonos regulares inscriptos y circunscriptos.

Los libros V y VI se ocupan de la proporcionalidad, y los siguientes, hasta el IX inclusive, de cuestiones aritméticas como teoría de la divisibilidad, proporciones y progresiones.

El libro X es el más extenso, pues contiene ciento quince proposiciones, y en él se tratan geométricamente las propiedades de algunas expresiones irracionales, cuadráticas y bicuadráticas.

Finalmente en los tres últimos libros se estudia la geometría del espacio.

2. LA AXIOMÁTICA DE EUCLIDES

El sistema axiomático construido por Euclides consiste en formular previamente las premisas (definiciones, postulados y nociones comunes), a partir de las cuales se deducen racionalmente las proposiciones restantes.

Si bien a la luz de la crítica moderna han aparecido algunas fallas en los cimientos del edificio euclídeo, no puede dejar de reconocerse el mérito de Euclides de haber establecido por vez primera los lineamientos generales que debe satisfacer una construcción racional y lógica de la geometría.

Así, casi todos los libros de **Los Elementos** se inician con la explicación de los **términos** o nombres de los objetos con los que se ha de trabajar. Al comienzo del libro I se dan veintitrés de estas definiciones, pero aparecen otras a lo largo del tratado hasta totalizar ciento dieciocho. Algunas de ellas son:

Punto es lo que no tiene partes.

Línea es una longitud sin anchura.

Recta es la línea que yace uniformemente en todos sus puntos.

Superficie es lo que sólo tiene longitud y anchura.

Ángulo es la inclinación de dos líneas de un plano que se encuentran. Si las líneas son rectas, el ángulo se llama rectilíneo.

Rectas paralelas son las rectas coplanarias que, prolongadas indefinidamente, no se encuentran.

Obviamente, el análisis más elemental de éstas y otras definiciones que aparecen en el tratado, conforme a los principios de la axiomática moderna, las derriba por su inconsistencia y oscuridad. En realidad, desde el punto de vista lógico, no pueden ser consideradas siquiera como definiciones; en general consisten en descripciones de objetos bajo una concepción intuitiva o experimental y en las cuales se utilizan otros conceptos o vocablos no definidos anteriormente. Su aparición en el texto obedece, sin duda, al afán de Euclides de explicar el significado de todos los elementos con los cuales habría de trabajar, incluso aquellos que la axiomática actual establece como primitivos o fundamentales y por lo tanto sin definición explícita. Cabe señalar que bien podrían haberse suprimido estas pseudodefiniciones sin que el texto euclídeo sufriese en su estructura, ya que las propiedades que se establecen luego se apoyan en las relaciones entre dichos entes y no en la naturaleza de los mismos, como se hace también en la geometría racional moderna.

Pese al afán señalado, se ha observado que Euclides omite a veces la explicación de algunos términos que utiliza, como en el caso de recta limitada o segmento y recta ilimitada.

En el libro I, después de los términos, siguen los axiomas, que Euclides divide en **postulados** y **nociones comunes** y con los cuales establece las proposiciones iniciales de su geometría. La distinción entre unos y otras es similar a la que existe entre problemas y teoremas. En efecto, los **postulados** constituyen las proposiciones fundamentales en que se apoyan los teoremas relativos a construcciones, mientras que las **nociones comunes** son la base para la demostración de los otros teoremas.

Los **postulados** son cinco:

I. Por un punto cualquiera se puede trazar una recta que pase por otro punto.

II. Toda recta limitada puede prolongarse indefinidamente en la misma dirección.

III. Con cualquier centro y cualquier radio se puede trazar una circunferencia.

IV. Todos los ángulos rectos son iguales entre sí.

V. Si una recta que corta a otras dos forma de un mismo lado ángulos interiores cuya suma es menor que dos rectos, estas dos rectas prolongadas indefinidamente se cortan del lado en que están dichos ángulos.

A "prima facie", estos postulados parecen referirse a cuestiones de naturaleza muy distinta. Mientras los tres primeros enuncian la posibilidad de ciertos trazados, los dos últimos indican una propiedad simple y otra que no lo es tanto.

Un análisis más cuidadoso permite descubrir la verdadera finalidad de estos postulados, que es la de afirmar la existencia de los elementos punto, recta y circunferencia y establecer la forma de construirlos o determinarlos. Esto surge inmediatamente de los tres primeros. El IV es necesario para poder hablar en el siguiente de "dos rectos" como de una cantidad determinada. El V da una condición de existencia y obtención de un punto como intersección de dos rectas. Como veremos más adelante, este postulado es fundamental en la teoría euclídea del paralelismo.

Es necesario advertir que este sistema de postulados no es completo para la construcción rigurosa de las proposiciones subsiguientes. Euclides, en efecto, utiliza a veces propiedades elementales no enunciadas previamente y que acepta en forma implícita. Esto ocurre en la primera de sus proposiciones, que se refiere a la construcción de un triángulo equilátero de lado dado, donde se admite tácitamente la existencia de intersecciones de rectas y circunferencias y de circunferencias entre sí. Tampoco se postula la continuidad de la recta, aunque se la utiliza frecuentemente. En la demostración del primer criterio de congruencia de triángulos se utiliza el principio de superposición mediante un movimiento, sin que el mismo se establezca anteriormente. Tampoco se formula la división de una recta por un punto y la división del plano por una recta, las que son frecuentemente utilizadas, y falta asimismo el importante postulado de Arquímedes, que Euclides admite en algunas demostraciones. Es notable también la ausencia de los postulados de la geometría del espacio.

En cuanto a las **nociones comunes**, su número varía según las distintas versiones del libro de Euclides, pero en general se consideran las siguientes:

I. Cosas iguales a una misma cosa son iguales entre sí.
II. Si a cosas iguales se agregan cosas iguales, las sumas son iguales.
III. Si a cosas iguales se quitan cosas iguales, los restos son iguales.
IV. Si a cosas desiguales se agregan cosas iguales, los resultados son desiguales.
V. Las cosas dobles de una misma cosa son iguales.
VI. Las mitades de una misma cosa son iguales.
VII. Las cosas que se pueden superponer son iguales.
VIII. El todo es mayor que la parte.

La función que corresponde a estas nociones comunes se advierte inmediatamente. Aparecen como enunciados inherentes a los conceptos de igualdad, desigualdad, suma, etc., de ciertos entes o cosas que hoy llamamos cantidades y constituyen el fundamento para el estudio de las relaciones de congruencia y equivalencia de figuras.

El conjunto de postulados y nociones comunes de Euclides constituyen, pues, tres tipos de axiomas según el sistema moderno de Hilbert: de enlace o incidencia, de paralelismo y de congruencia. Faltan los de continuidad y de orden, aunque la sistematización euclídea los considera implícitamente.

3. EL POSTULADO V Y LA TEORÍA DEL PARALELISMO

Los cuatro primeros postulados del sistema de Euclides son de estructura simple y enuncian propiedades inmediatas a nuestra intuición. No ocurre lo mismo con el V, de factura más complicada y menos evidente que los anteriores. Esta circunstancia se vuelve más notable al advertir el poco uso que Euclides hace de dicho postulado y su demora en aplicarlo. Después de demostrar que "dos rectas que forman con una tercera ángulos alternos internos iguales, o ángulos correspondientes iguales, o ángulos interiores de un mismo lado suplementarios, son paralelas" (proposiciones 27 y 28) utiliza por vez primera el postulado V para demostrar la proposición 29, recíproca de las anteriores. En lo que pareciera ser un propósito deliberado de eludir ese recurso, llega a sacrificar la sencillez de algunas demostraciones, complicándolas innecesariamente.

Esta evidente preocupación de Euclides por soslayar en lo posible el uso del postulado V y en edificar, hasta donde le fue posible, su geometría sin él, es suficiente para atribuirle la paternidad de la **Geometría Absoluta,** es decir independiente de toda teoría del paralelismo y en la cual se incluyen la euclidiana y las no euclidianas. Vale, pues, pese a su aparente contradicción, la conocida expresión de que Euclides fue el primer geómetra no euclidiano.

La teoría del paralelismo se afirma más adelante en el libro I con los teoremas relativos a las rectas paralelas a una tercera, a la unicidad de la paralela a una recta por un punto, a la equidistancia entre paralelas y la propiedad fundamental de la suma de los ángulos de un triángulo.

El postulado V llamó la atención a los comentaristas de la obra euclídea, aun a los más antiguos, que juzgaron que no era suficientemente evidente para aceptarlo como tal y que por lo tanto había que demostrarlo. Los intentos que a partir de entonces se llevaron a cabo para salvar lo que aparecía como primera falla en el edificio construido, se dirigieron sucesivamente en tres direcciones:

1º Sustituir la definición de rectas paralelas dada por Euclides, cambiando su forma gramatical negativa por una afirmación.

2º Reemplazar el postulado V por otro más simple o más acorde con los datos directos suministrados por la intuición o la experiencia.

3º Demostrarlo exclusivamente sobre la base de los postulados precedentes, es decir, sin el agregado de otras hipótesis.

Proclo, en su comentario, informa de los primeros tentativos. Ya en el siglo I a.C., Posidonio ensaya el cambio de la definición euclídea de paralelas por la siguiente: "rectas paralelas son rectas coplanarias equidistantes". Gémino, en la misma época, discute el sentido del paralelismo según Euclides y Posidonio; se apoya para ello en la posible existencia de rectas asintóticas, es decir, paralelas según el concepto euclídeo, que no se encuentran por más que se prolonguen, pero no paralelas en el sentido de Posidonio o sea, no equidistantes, tal como ocurre con la hipérbola y la concoide con respecto a sus asíntotas. Para que ambas definiciones concordasen habría que demostrar que "dos rectas que no se encuentran son equidistantes" o "el lugar de los puntos equidistantes de una recta es otra recta", lo cual hace Euclides basándose precisamente en su postulado.

Esta idea de demostrar el postulado fundándose en la hipótesis de la existencia de rectas equidistantes se mantuvo durante mucho tiempo y se reprodujo gran número de veces en la edad media y en el renacimiento. Entre los árabes, herederos del predominio griego en matemática, esa tendencia se manifiesta a través de distintos comentaristas del texto euclídeo, como Simplicio (siglo VI) y Al-Nirizi (siglo IX), pero, por lo general, las demostraciones aparecen viciadas por el uso tácito de otras hipótesis no formuladas previamente, como el postulado de Arquímedes. Igual defecto aparece en los trabajos de Nasir-Eddin (siglo XIII), que aporta la novedad de deducir el postulado V a partir del teorema relativo a la suma de los ángulos de un triángulo, que demuestra previamente de manera original.

Luego de una pausa de tres siglos, durante la cual las sucesivas versiones de los elementos dejan a un lado la cuestión del postulado V, las primeras impresiones en griego y en latín del comentario de Proclo provocan a mediados del siglo XVI la reanudación de las críticas y ensayos que se suceden, sin mayores variantes, sobre la idea anterior hasta fines del siglo XVII.

Por ese entonces, un recurso nuevo y original es presentado por J. Wallis al sustituir el postulado V por la siguiente afirmación: "para toda figura existe siempre una semejante de magnitud arbitraria". Justifica esta hipótesis como una extensión del pensamiento euclídeo expuesto en el postulado III que admite, en esencia, la existencia de círculos semejantes. Sin embargo en cuanto evidencia inmediata para la intuición, ella no aporta ventajas sobre el postulado V.

De naturaleza muy distinta es el enfoque dado a la cuestión por el padre jesuita Gerolamo Saccheri (1667-1733) considerado como el precursor de la geometría no euclidiana y seguido más tarde por Johann Heinrich Lambert (1728-1777) y A. M. Legendre (1752-1833).

Saccheri hace uso de un tipo de razonamiento que el mismo Euclides utilizó, y según el cual, tomando como hipótesis la falsedad de la proposición que se desea demostrar, se deduce igualmente que es verdadera.

Toma entonces las 28 primeras proposiciones del libro I, que, como se ha observado, son independientes del postulado V y, admitiendo la falsedad de éste, trata de hallar entre las consecuencias una contradicción lógica que afirme la verdad del postulado.

Aun sin entrar en el detalle de las demostraciones, es interesante conocer las líneas generales de su razonamiento y sus resultados, no sólo porque inician el camino que un siglo después conduciría a la solución definitiva del problema, sino también porque en el fondo de sus hipótesis, aunque él no lo advirtiera, yacía latente la simiente de las posteriores geometrías no euclidianas.

Considera para ello un cuadrilátero birrectángulo isósceles ABCD ($\widehat{A} = \widehat{B}$; $AD = BC$). Demuestra fácilmente, sin recurrir al postulado V que $\widehat{C} = \widehat{D}$; pero al no admitir el postulado euclídeo no puede afirmarse que dichos ángulos sean rectos. Aparecen entonces tres casos igualmente posibles: que sean rectos, obtusos o agudos. Deduce de inmediato que dichas hipótesis conducen respectivamente a que $AB = CD$; $AB > CD$ y $AB < CD$ y recíprocamente y, de esto, que: si en un caso particular se verifica una de las tres posibilidades respecto de los ángulos $\widehat{C}$ y $\widehat{D}$, ella es verdadera en cualquier otro caso. Para tal demostración, Saccheri recurre también, implícitamente, a los postulados de continuidad y de Arquímedes.

De las propiedades anteriores deduce que, según se verifique la hipótesis del ángulo recto, la del obtuso o la del agudo, la suma de los ángulos interiores de un triángulo será respectivamente igual, mayor o menor que dos ángulos rectos.

Demuestra luego que la hipótesis del ángulo recto es equivalente a la de Euclides y trata de comprobar que las otras dos encierran una contradicción. Lo consigue fácilmente en el caso del ángulo obtuso y por lo tanto desecha esa posibilidad. No obtiene resultados tan inmediatos partiendo de la tercera hipótesis, pero en su empeño por demostrar la validez del postulado V y arraigado en él el convencimiento de que era imposible lo contrario, añade una nueva hipótesis que lo lleva a incursionar en el terreno de lo infinitud. La extrapolación de ciertas propiedades que valen para distancias finitas le permite hallar el absurdo buscado, pero naturalmente, su razonamiento queda viciado por tal defecto.

En realidad, tal absurdo no existe y es probable que el mismo Saccheri, de no estar atado por su propósito de reivindicar el postulado V hubiese podido adelantar el camino hacia el descubrimiento de las geometrías no euclidianas.

Es oportuno destacar que las conclusiones de Saccheri corresponden precisamente a los tres sistemas geométricos que surgen de las distintas posturas adoptadas frente a la teoría del paralelismo.

Así la hipótesis del ángulo recto, del ángulo agudo y del ángulo obtuso y sus consecuencias relativas a la suma de los ángulos de un triángulo, concuerdan respectivamente con la geometría euclídea y las no euclidianas de Lobatchefsky y de Riemann.

Lambert parte de consideraciones análogas a las de Saccheri, considerando un cuadrilátero trirrectángulo y las tres hipótesis posibles respecto del cuarto ángulo. La hipótesis del ángulo recto lo lleva fácilmente al postulado de Euclides; rechaza la del ángulo obtuso que conduce a una contradicción con el postulado de Arquímedes pero no encuentra ninguna refutación lógica a la hipótesis del ángulo agudo. En cambio obtiene, a partir de ella, nuevas e interesantes propiedades: descubre que la diferencia entre $2R(n-2)$ y la suma de los ángulos de un polígono, que llama **deficiencia**, es proporcional al área del mismo y que la medida de un segmento sería independiente de la unidad, por ser ésta absoluta, es decir, única y no arbitraria, como lo es el ángulo recto en el caso de los ángulos. Intuye también que de ser válida la hipótesis del ángulo obtuso, la geometría plana sería como la geometría sobre una esfera.

Otro geómetra que llega a análogos resultados a partir de las tres hipótesis es Legendre, quien demuestra la propiedad de que la suma de los ángulos de un triángulo es igual a dos rectos.

4. REVISIÓN CRÍTICA DE LA GEOMETRÍA EN EL SIGLO XIX

Al cabo de veinte siglos, notables esfuerzos realizados por los más autorizados geómetras seguían siendo estériles y el problema suscitado por el postulado V, no tenía todavía solución. Las tentativas consistieron siempre en sustituir el mismo por otro equivalente, es decir, demostrable en base a él y recíprocamente, con lo cual lo único que se lograba era simplemente darle otra forma o trasladar la cuestión a otro terreno no más ventajoso.

Esto hizo pensar a algunos matemáticos, en los comienzos del siglo XIX, que la teoría del paralelismo implicaba un problema sin solución y que antes de seguir con el intento de demostrar la proposición euclídea había que preguntarse si era en realidad demostrable. Afrontada así la cuestión importaba averiguar a qué consecuencias conduciría la hipótesis contraria a las sustentadas por el postulado de Euclides o sus equivalentes.

Frutos notables de esta búsqueda fueron la creación de las geometrías no euclidianas y la conclusión de que el postulado V es indemostrable, es decir, que es independiente de los anteriores, y por lo tanto podría ser sustituido por cualquier otra hipótesis compatible con los postulados precedentes sin que ello condujese a alguna contradicción.

Al llegar a este punto se abría el camino a muchas variantes posibles. Con sólo sustituir uno o varios de los postulados iniciales se tendrían otras tantas geometrías distintas. Así, además de las no euclidianas, nacieron otras como las no arquimedianas, que no reconocen el postulado de Arquímedes, las no arguesianas, no pitagóricas, no pascalianas y otras que, si bien son de limitado alcance o de relativo interés en sus conclusiones, influyeron notoriamente en el estudio de los fundamentos de la geometría.

Fue necesaria, en efecto, una revisión profunda de las bases y conceptos fundamentales y se afianzó la idea de la necesidad del rigor y precisión en la enunciación de los conceptos y de las demostraciones, a fin de asegurar su validez y la de sus conclusiones.

Eminentes geómetras como Pasch, Veronese, Peano, Hilbert y Schur emprendieron, a partir de la segunda mitad del siglo anterior, la delicada tarea de ahondar en los cimientos de la geometría a fin de consolidar su estructura fundamental y de planificar el desarrollo lógico ulterior de esta ciencia. Como resultado de estos trabajos surgen las normas a que debe ajustarse una construcción racional de la geometría, sin los defectos impugnables a la obra de Euclides.

Ante todo, la existencia simultánea de distintas geometrías edificadas en base a hipótesis opuestas y perfectamente coherentes, sin embargo, cada una de ellas en sí misma, obligó a meditar sobre la validez de sus respectivos resultados. Así, mientras en una geometría se afirma que la suma de los ángulos de un triángulo es igual a dos rectos, en otra se obtiene que es mayor que ese valor, y en otra que es menor que el mismo. ¿Cuál de estas conclusiones es la verdadera, si es que alguna de ellas puede considerarse como tal? Si nos atenemos a los datos de nuestro reducido espacio físico y nos sometemos a los resultados de la verificación experimental, la primera conclusión aparece como verdadera, y las otras dos erróneas. Sin embargo este juicio es apresurado y a lo sumo podríamos afirmar que la tesis euclídea se cumple en el espacio perceptible a escala humana pero no podemos extrapolar al punto de asegurar que lo mismo ocurre en otros campos vedados a nuestra experimentación directa, sea el de lo infinitamente grande o el de lo infinitamente pequeño. Una verificación material, una comprobación experimental no satisfacen al lógico ni al matemático. Ellos nutren sus convicciones en la razón y admiten como verdadera toda conclusión que emane de un proceso lógico deductivo, con total independencia del mundo físico circundante. Esto obliga a controlar el uso, a veces indebido y abusivo de la palabra "verdad" en matemática, liberándola de todo sometimiento a la realidad material.

De estas observaciones resulta que también varía la noción misma de espacio geométrico. En el dominio de las ciencias naturales y en el de la física, el investigador se surte con los elementos que le provee el medio circundante; éste es el **espacio físico** o sea el conjunto de todos los objetos materiales. Existe otro tipo de espacio, el **intuitivo**, que es el escenario donde juegan las imágenes creadas por la intuición, es decir, por el convencimiento nacido de una especie de percepción natural e irracional. La intuición nace generalmente de una experiencia limitada y de los escasos datos de nuestro mundo sensible; por eso al lógico, el espacio intuitivo no le es suficiente y más aún, desconfía de los peligros a que inevitablemente suele conducir una falsa intuición.

Para que la geometría pueda elevarse a la condición de ciencia pura y racional debe fundamentarse con prescindencia de todo lazo que la ate al mundo de los sentidos y de la apreciación directa. Los entes y conceptos que elabora una geometría así concebida y sus conclusiones originan un nuevo tipo de espacio, el **espacio abstracto**, entidad conceptual esencialmente intelectual y sin existencia objetiva.

Esto no significa que la intuición quede totalmente dejada de lado en la investigación matemática; al contrario, se recurre también a ella, pero sólo como una ayuda o guía y nunca como elemento de juicio definitivo, ni como sustituto de una demostración. Como recurso didáctico es valiosa al nivel de la enseñanza elemental; es muy útil sobre todo en la elaboración conceptual y en el descubrimiento de propiedades, pero su uso debe ser oportuno y medido.

Otra característica distingue al espacio geométrico y es la posible multiplicidad de sus dimensiones. En la geometría clásica euclídea el espacio es tridimensional. Recordemos que la **dimensión** de un espacio está dada por el número de coordenadas necesarias para fijar la posición de uno de sus puntos; la recta, el plano y el espacio euclídeo son otros tantos espacios de una, dos y tres dimensiones, respectivamente. La superficie de una esfera un espacio de dos dimensiones, pues un punto de ella queda determinado por sus dos coordenadas geográficas; una curva en la que se fije un punto O de origen, es un espacio de una dimensión, pues un punto M cualquiera de ella queda determinado por la longitud del arco OM.

El desarrollo de la geometría analítica permitió extender el concepto de coordenadas y condujo al estudio de los **espacios multidimensionales**, conquistas ambas que permitieron encarar y resolver satisfactoriamente numerosas cuestiones, no sólo dentro de la matemática pura, sino también en el campo de sus aplicaciones.

Como sabemos, la geometría analítica estudia las propiedades geométricas de las figuras a través de las propiedades algebraicas de las ecuaciones que la representan. La recta, por ejemplo, tiene como expresión analítica en el plano, la ecuación de primer grado con dos incógnitas $ax + by + c = 0$ y recíprocamente toda ecuación de este tipo representa a una recta. La ecuación del plano es $ax + by + cz + d = 0$, la de una circunferencia es $(x - a)^2 + (y - b)^2 - r^2 = 0$ donde a y b son las coordenadas del centro y r el radio, etc.

Si se quiere, por lo tanto, hallar el punto de intersección de dos rectas, basta resolver un sistema de dos ecuaciones lineales con dos incógnitas. Inversamente, la solución de un sistema de este tipo es siempre el punto de intersección de las rectas representadas por las ecuaciones del sistema. De igual manera, resolver un sistema de tres ecuaciones lineales con tres incógnitas significa hallar el punto común a tres planos. La generalización al caso de más ecuaciones con correlativo número de incógnitas es imposible dentro del espacio tridimensional.

En general, el estudio de las funciones de cuatro o más variables dirigió la búsqueda de los matemáticos a similares interpretaciones geométricas que posibilitaran la concepción de los resultados. Surgió entonces la idea de considerar las **n** variables como coordenadas de ciertas figuras o "puntos" de un espacio ideal de igual número de dimensiones, mediante una simple extensión de los conceptos iniciales. Se llamó entonces **punto** a un conjunto ordenado de números reales: $(x_1 ; x_2 ; \ldots ; x_n)$. El conjunto de todos estos puntos es el **hiperespacio de n dimensiones.**

Se puede entonces definir el **hiperplano,** por generalización, como el conjunto de los puntos $P(x_1 ; x_2 ; \ldots ; x_n)$, del hiperespacio de n dimensiones que satisfacen la ecuación:

$$a_1x_1 + a_2x_2 + \ldots + a_n x_n + a_0 = 0$$

Con esto quedó resuelto el problema de caracterizar geométricamente la solución de un sistema de n ecuaciones lineales con n incógnitas.

Axiomáticamente, la generación del hiperespacio de n dimensiones es muy simple, sin más que utilizar el método de recurrencia. A partir de la recta, espacio de una dimensión, determinada por dos puntos, se obtiene el plano, espacio de dos dimensiones, determinado por una recta y un punto fuera de ella, etc.

Si bien esta concepción puramente intelectual del espacio puede resultar desconcertante a los espíritus no matemáticos, especialmente por la dificultad de intuir un espacio de más de tres dimensiones, la idea de una cuarta dimensión ha ido tomando cuerpo incluso en la mente del hombre común.

Las teorías multidimensionales se han extendido, como ya se dijo, fuera de los límites de la especulación puramente matemática. Los avances de la ciencia en sus distintas ramas probaron su importancia y necesidad. La física, por ejemplo, ha encontrado en ellas un auxilio inestimable, especialmente para el desarrollo de la teoría de la relatividad, que requiere un espacio de cuatro dimensiones.

5. LA AXIOMATIZACIÓN DE LA GEOMETRÍA

Al ocuparnos de los **Elementos de Euclides** dijimos que la obra podía considerarse como un modelo de construcción axiomática de la geometría. En efecto, a partir de un conjunto de premisas fundamentales, definiciones, postulados y nociones comunes, se obtienen deductivamente las proposiciones restantes. Oportunamente señalamos algunos defectos imputables tanto a las definiciones como a los postulados. La crítica moderna no sólo los puso en evidencia sino que logró subsanarlos, estableciendo los principios esenciales a que debe ceñirse una formulación axiomática rigurosa. La obra cumbre en tal sentido es el trabajo de Hilbert "Grundlagen der Geometrie", dado a publicidad en el año 1899. Su axiomatización de la geometría junto con la sistematización llevada a cabo por Klein con su teoría de grupos, permitió una reestructuración total de esta ciencia y la

condujo al alto grado de perfección lógica que hoy la caracteriza.
La formulación de Hilbert se apoya en dos cuestiones esenciales: los conceptos primitivos y las propiedades primitivas o axiomas.

Conceptos primitivos

Se ha visto que una de las principales objeciones hechas a la obra de Euclides es la oscuridad con que presenta los conceptos o términos, caracterizados en forma poco rigurosa y, generalmente, con el empleo de otros términos no aclarados previamente. Esto se debe al hecho de que es imposible definir de manera explícita todos los conceptos de una teoría. Si para explicar uno de ellos recurrimos a otros anteriores, éstos, a su vez, deberán definirse en base a alguno ya conocido y así sucesivamente. Esta cadena necesariamente debe tener un origen, uno o varios conceptos iniciales o primitivos a partir de los cuales pueden definirse los demás, pero que a su vez, no pueden definirse según el mismo criterio, precisamente por ser los primeros de la cadena.

Estos conceptos primitivos, que en la teoría aritmética de Peano son número, conjunto y siguiente, en geometría son también varios y pueden elegirse arbitrariamente según la ordenación que se dé a la misma. Un concepto que es primitivo en una determinada ordenación puede no serlo necesariamente en otra y, por lo tanto, en ésta será susceptible de definición explícita, aunque no lo sea en la primera.

Por otra parte, al matemático no le interesa la interpretación material o intuitiva de los entes primitivos, que pueden inclusive no tenerla y ser en cambio el fruto de una creación libre de la inteligencia.

Sin embargo, los conceptos primitivos pueden y deben caracterizarse de manera unívoca y rigurosa. Hilbert indicó cómo lograrlo indirectamente a través de ciertas relaciones lógicas que deben satisfacer y cuya formulación constituye el sistema de axiomas o postulados en que se fundamenta la teoría.

Las definiciones

La geometría moderna considera, por lo tanto, distintos tipos de conceptuación o de definición.

a) Definiciones nominales explícitas

Tienen por objeto la presentación de un término nuevo con el cual se designa a una determinada categoría de entes, mediante el enunciado de una proposición en la que figura el término a definir y un conjunto de palabras o combinación de conceptos que tienen el mismo significado lógico que el que se ha de atribuir al nuevo término.

Ejemplos: las definiciones usuales de segmento, de circunferencia, de ángulo, etc.

Este tipo de definición representa en realidad una convención de lenguaje, por la cual se simplifica la referencia a un concepto más o menos complejo mediante un nombre que lo identifique. No se trata, pues, de definiciones creadoras, en el sentido de que no introducen un nuevo ente, sino a lo sumo dan un nombre a un concepto ya existente. Son tautológicas, pues establecen una equivalencia lógica entre el significado del nombre introducido y el del predicado que lo acompaña en la proposición.

Definiciones de esta clase son, por lo tanto, prescindibles, a no ser por la importante economía de lenguaje que representan.

Entre ellas se encuentran las clásicas definiciones por **género próximo y diferencia específica,** mediante las cuales se señalan las cualidades esenciales que distinguen al ente a definir (diferencia) entre otros más generales que lo comprenden (género).

Ejemplo: se llama rombo al paralelogramo que tiene dos lados consecutivos iguales. Los paralelogramos constituyen el género, y el tener dos lados consecutivos iguales, la característica diferencial.

b) Definiciones por abstracción

Este método de conceptuación, a diferencia del anterior, es creador, pues permite la introducción de nuevos conceptos nacidos a expensas de otros por un proceso natural de abstracción.

Se ha visto (capítulo III) que toda relación de equivalencia en un conjunto produce en el mismo una partición. Cada clase de equivalencia del conjunto cociente agrupa a todos los entes u objetos del conjunto dado que son equivalentes respecto de dicha relación. Esto lleva a considerar la existencia de una cualidad común que agrupa a los objetos de una misma clase y los diferencia de los no pertenecientes a ésta. Es decir, cada clase constituye un nuevo ente que admite como representante a cualquiera de los objetos de dicha clase, y que se puede considerar identificado con la característica común que los vincula.

Esta idea es la base de las definiciones por abstracción que permiten caracterizar un concepto nuevo, como cualidad que asocia a todos los objetos pertenecientes a una misma clase de equivalencia.

Ejemplos de este tipo de conceptuación, uno de los más fecundos en la matemática, son las definiciones de dirección, de superficie, de volumen, de forma. En aritmética, constituyen el fundamento del método genético en la ampliación sucesiva de los campos numéricos.

c) Definiciones por recurrencia

Se basan en el principio de inducción completa y tienen por objeto la creación de nuevos conceptos como extensión o generalización de otro anterior, por reiteración del criterio usado para definir a este último.

Ejemplos típicos de este método son las definiciones de suma y de producto en el sistema de Peano para los números naturales. En geometría se definen de esta manera la suma de segmentos o de ángulos consecutivos, el producto de los mismos por un número natural, etc.

d) Definiciones implícitas

Es obvio advertir que ninguno de los tipos de definiciones anteriores es apto para caracterizar a los conceptos primitivos por ser éstos precisamente los conceptos iniciales de la teoría.

El problema de caracterizar estos entes de manera única y rigurosa fue resuelto por Hilbert y al método de conceptuación que utilizó se le llama definición implícita.

Consiste en establecer las relaciones primitivas o fundamentales que los ligan por medio del sistema de axiomas o postulados que constituyen el punto de partida de toda la teoría y de los cuales se obtendrán deductivamente todas las proposiciones restantes o teoremas. Dichas relaciones tampoco se definen previamente por el hecho de ser las primeras, pero quedan a su vez caracterizadas a través de los axiomas.

No importa entonces que se ignore el significado de los entes primitivos; estableciendo entre ellos las relaciones esenciales que los vinculan, éstas se encargarán por sí solas de definirlos en forma implícita.

Un sistema de axiomas cumple dentro de la teoría una doble función: la de caracterizar los entes y relaciones primitivas y la de formular las primeras proposiciones lógicas de las cuales se deducen racionalmente todas las otras proposiciones que sucesivamente integren dicha teoría. Dado el carácter abstracto de la matemática, tales axiomas son proposiciones lógicas arbitrarias a las que sólo se exige el cumplimiento de las condiciones esenciales tratadas en el capítulo VI.

6. FORMULACIÓN DE HILBERT PARA LA MÉTRICA EUCLIDIANA

Hilbert utiliza como entes primitivos tres conceptos: punto, recta y plano y varias relaciones también primitivas, como "pertenece", "entre", "congruente", "paralelo" y "continuo". No importa la naturaleza de unos y otras ni es necesario atribuirles un significado; sólo se exige que satisfagan el sistema de axiomas propuesto.

Establece luego cinco sistemas de axiomas o postulados: de enlace o incidencia, de ordenación, de congruencia, de paralelismo y de continuidad.

Axiomas de enlace o incidencia

Introducen los entes primitivos y definen implícitamente la relación primitiva de incidencia o pertenencia

I_1 — Dos puntos distintos determinan una recta.

I_2 — Dos puntos cualesquiera de una recta determinan esta misma recta.

I_3 — Sobre toda recta existen, por lo menos dos puntos, y en todo plano existen por lo menos tres puntos no pertenecientes a la misma recta.

I_4 — Tres puntos distintos que no pertenecen a una misma recta, determinan un plano.

I_5 — Tres puntos distintos de un plano que no pertenecen a una misma recta determinan el mismo plano.

I_6 — La recta determinada por dos puntos de un plano, pertenece al plano.

I_7 — Si dos planos tienen un punto común, tienen por lo menos otro punto común.

I_8 — Existen por lo menos cuatro puntos que no están en un mismo plano.

Los tres primeros axiomas caracterizan la relación de incidencia entre puntos y rectas. Los dos siguientes, la incidencia entre puntos y planos. El I_6, la incidencia entre recta y plano y el I_7 la incidencia entre planos. El último axioma fija el carácter tridimensional del espacio.

Axiomas de ordenación

Establecen implícitamente el significado de la relación primitiva "entre", punto de partida para establecer después los criterios de ordenación en la recta, en el plano y en el espacio.

O_9 — Si A, B y C son tres puntos pertenecientes a una recta y B está entre A y C, B está también entre C y A.

O_{10} — Si A y C son dos puntos pertenecientes a una recta existe un punto B de la recta que está entre A y C y existe un punto D sobre la misma, tal que C está entre A y D.

O_{11} — Dados tres puntos de una recta existe siempre uno y sólo uno de ellos situado entre los otros dos.

O_{12} — Si A, B y C son tres puntos que no pertenecen a una misma recta y a es una recta del plano que determinan, la cual no pasa por ninguno de dichos puntos, si a corta al segmento AB, corta también al segmento BC o al AC.

Obsérvese que el axioma O_{10} equivale a considerar a la recta como un conjunto denso de puntos.

El axioma O_{12} permite ordenar los puntos del plano, ya que en base al mismo se deduce la propiedad de la división del plano por una recta.

Axiomas de congruencia

Caracterizan la relación primitiva "congruente" entre segmentos y entre ángulos.

C_{13} — Dado un segmento AB y un punto A perteneciente a la misma recta que el AB o a otra recta a', se puede encontrar siempre sobre dicha recta un punto B' y sólo uno a un lado prefijado de A' tal que el segmento AB es congruente con el A'B'. Todo segmento es congruente consigo mismo independientemente del orden de sus extremos, es decir AB = AB y AB = BA.

C_{14} — Si un segmento AB es congruente con el segmento A'B' y es también congruente con el A''B'', entonces A'B' es congruente con el A''B''.

C_{15} — Si A, B, C son puntos de una recta dados en ese orden y A', B', C' son puntos de la misma o de otra recta dados también en ese orden y tales que AB es congruente con A'B' y BC es congruente con B'C', entonces AC es congruente con A'C'.

C_{16} — Dado un ángulo pq y uno de los semiplanos determinados por una recta a existe en éste una semirrecta y sólo una del mismo origen que una semirrecta de a y que forma con esta última semirrecta un ángulo congruente con el pq. Todo ángulo es congruente consigo mismo independientemente del orden de sus lados, es decir, $\widehat{pq} = \widehat{pq}$ y $\widehat{pq} = \widehat{qp}$.

C_{17} — Dos triángulos que tengan dos lados y el ángulo comprendido congruentes, tienen también los otros dos ángulos congruentes.

Los tres primeros axiomas de este grupo definen implícitamente la relación primitiva "congruencia de segmentos". El C_{13} y el C_{14} establecen las propiedades reflexiva, simétrica y transitiva de dicha relación que queda caracterizada por lo tanto como una relación de equivalencia. El C_{15} fundamenta la definición de suma de segmentos.

Los dos axiomas restantes definen implícitamente la relación primitiva "congruencia de ángulos" y constituyen el fundamento del estudio de la congruencia de figuras planas y del espacio. Se observa que falta el axioma relativo a la transitividad de la relación y el análogo al C_{16} para la congruencia de ángulos; ello se debe a que es posible demostrar ambas propiedades luego de introducir el C_{17}.

Axiomas de paralelismo

Se trata en realidad de un axioma único que caracteriza la geometría euclídea fijando su posición en la teoría de las paralelas. En efecto, en base a los postulados precedentes, es posible demostrar la existencia de una recta al menos, que pase por un punto dado y no corte a otra recta dada coplanar con la primera. Hilbert postula la unicidad de dicha recta con el siguiente axioma.

P_{18} — (Axioma de Euclides). Dada una recta y un punto no perteneciente a ella existe a lo sumo una recta perteneciente al plano que aquellos determinan, que pasa por el punto y no corta a la recta dada.

Axiomas de continuidad

Introducen la noción de continuidad en la recta.

K_{19} — (Axioma de Arquímedes). Sea A_1 un punto cualquiera de una recta situado entre dos puntos arbitrarios A y B de la misma. Sean además los puntos A_2, A_3, A_4, . . . , tales que A_1 esté entre A y A_2, A_2 entre A_1 y A_3, etc., y que los segmentos AA_1, A_1A_2, etc., sean congruentes entre sí. Existe entonces en la serie de puntos A_1, A_2, A_3, . . . un cierto punto A_n, tal que B está entre A y A_n.

K_{20} — (Axioma de integridad). Los elementos (punto, recta y plano) de la geometría forman un sistema de entes tales que no puede ser ampliado sin que se modifiquen los axiomas precedentes.

Estos dos axiomas fundamentan la teoría de la medida de segmentos y el tratamiento analítico de la geometría. El axioma de Arquímedes permite asignar a cada punto de la recta un número real que es la medida, con respecto a una unidad, del segmento que determina el punto con otro de la misma recta tomado como origen. La correspondencia inversa, es decir, el atribuir a todo número real un punto de la recta, sólo puede establecerse si se admite el axioma de integridad.

Los cinco grupos de axiomas propuestos por Hilbert constituyen el fundamento de la geometría métrica euclidiana tridimensional.

Con su obra, Hilbert dejó abierto un camino, enmarcado en las exigencias de rigor y perfección que caracterizaron al siglo XIX, para el tratamiento de la geometría tradicional.

Trabajos posteriores, como el de Enriques, introdujeron algunas variantes que, si bien respetaron los aspectos fundamentales del sistema de Hilbert, permitieron su adecuación a la enseñanza.

La teoría de los grupos de transformaciones de Klein abrió, por su parte, un panorama más amplio al permitir el tratamiento conjunto de las distintas geometrías, poniendo en evidencia sus relaciones y diferencias.

CAPITULO X

Las estructuras geométricas

Según se ha visto en el capítulo anterior, la discusión del trabajo de Euclides trajo como consecuencia, no sólo la dilucidación del problema discutido, sino el nacimiento de una nueva posición matemática, con la que ésta adquiere su verdadero significado. Se arribó así a la génesis de la matemática moderna. En ese sentido Hilbert analizó el problema geométrico, que fue desarrollado, según se anticipó, por Félix Klein, en su famoso programa de Erlangen, aparecido nada menos que en 1872.

En el planteo de Klein, que naturalmente puede superarse en nuestros días, está contenido, sin embargo, el fundamento de la matemática actual: La matemática es una ciencia deductiva que se construye por método formal mediante ciertas estructuras que son aplicables a todas las ramas, las que en consecuencia, dejan de ser disciplinas independientes. Y ese mismo planteo permite, además, precisar el significado de la geometría dentro de la matemática.

Puesto que la finalidad de este capítulo es analizar las estructuras de los diferentes desarrollos geométricos posibles, y las coincidencias y divergencias entre tales geometrías pueden caracterizarse con los elementos y criterios puntualizados por Klein, introduciremos primero tales elementos.

1. TRANSFORMACIONES GEOMÉTRICAS

En el capítulo III, parágrafo 5, se estudió el concepto de aplicación entre conjuntos, dándose como sinónimos de tal término, los de función, transformación, correspondencia o proyección. Es usual, sin embargo, reservar el término función para las aplicaciones entre conjuntos numéricos y su equivalente transformación, para las aplicaciones entre conjuntos cuyos elementos son entes geométricos, adquiriendo primordial interés las transformaciones de tipo biyectivo, que en tal caso son designadas operaciones geométricas.

A estas transformaciones geométricas puede entonces aplicarse el concepto de composición de aplicaciones (capítulo IV, parágrafo 4), resultando que la composición de dos transformaciones es siempre otra aplicación entre entes geométricos, o sea es una transformación, recordando además que tal composición de transformaciones es siempre asociativa y suele llamarse producto de las mismas.

Así, con este criterio pueden definirse las transformaciones fundamentales de la geometría euclídea clásica: traslaciones, rotaciones, movimientos, simetrías (central, axial), homotecias y semejanzas, con las que pueden estudiarse todas las propiedades de ese cuerpo de geometría.

2. TRANSFORMACIONES MÉTRICAS

Traslaciones

Definición

> **Dado un vector $\vec{a}$ de un plano, se llama traslación de vector $\vec{a}$ a la aplicación de los puntos del plano sobre los puntos de ese mismo plano que asigna como homólogo de un punto cualquiera el extremo del vector equipolente a $\vec{a}$ trazado por el punto dado.**

La traslación de vector $\vec{a}$ suele notarse $T(\vec{a})$ y es usual, si A' es la imagen de A a través de $T(\vec{a})$, expresar:

$$T(\vec{a}) \cdot A = A'$$

Es decir que al aplicar al punto A la transformación $T(\vec{a})$ se obtiene como resultado A' (y de ahí se infiere el sentido de "operación" contenido en la aplicación)

Es usual también, la siguiente escritura:

$$T(\vec{a}) \begin{Bmatrix} A \,, B \,, C \,, \ldots, X, \ldots \\ A' \,, B' \,, C' \,, \ldots, X', \ldots \end{Bmatrix}$$

que indica que los puntos A , B , . . . , X , . . . constituyen el primer conjunto, es decir desde el punto de vista geométrico pertenecen a una figura o más genéricamente a una forma Σ, siendo los A' , B' , . . . , X', . . . las respectivas imágenes de aquéllos, engendrando entonces una nueva figura Σ', transformada de la Σ, a través de $T(\vec{a})$, pudiendo entonces indicarse la aplicación de Σ sobre Σ':

$$T(\vec{a}) \cdot \Sigma = \Sigma'$$

Rotaciones o giros

Definición

Dados en un plano un punto O y un ángulo orientado α, se llama giro o rotación de centro O y amplitud α a la aplicación entre los puntos del plano y los puntos del plano, que asigna como homólogo de O al mismo punto O y a cualquier otro $A \neq O$, el A' intersección de la circunferencia de centro O y radio $\overline{OA}$ y la semirrecta $\overrightarrow{OA'}$ tal que el ángulo $\widehat{AOA'}$ sea igual al α.

Es decir, si A' es la imagen de A, a través del giro de centro O y amplitud α, que se expresa por $G(O, \alpha)$, se tendrá $\forall A \neq 0$:

$$G(O, \alpha) \cdot A = A' \,/\, A' \in [C(O, \overline{OA}) \cap \overrightarrow{OA'}] \wedge \widehat{AOA'} = \alpha$$

Movimientos geométricos directos

Definición

Dado, en un cierto orden, un conjunto de traslaciones y rotaciones en número finito, se llama movimiento geométrico directo a la transformación que resulta al componer sucesivamente las dadas, en ese orden.

Es decir que un movimiento directo es un "producto" de traslaciones y rotaciones en número finito.

Si se tiene:

$$T(\vec{a}) \cdot \Sigma = \Sigma'$$
$$T(\vec{b}) \cdot \Sigma' = \Sigma''$$
$$G(O, \alpha) \cdot \Sigma'' = \Sigma'''$$

el movimiento directo $\mathcal{M}_D$ es la transformación que aplicada directamente a Σ da como imagen Σ''':

$$G(O, \alpha) \cdot T(\vec{b}) \cdot T(\vec{a}) \cdot \Sigma = \Sigma'''$$

O sea:

$$\mathcal{M}_D \cdot \Sigma = \Sigma'''$$

Puede demostrarse, sin dificultad, aún cuando escapa al contenido de esta obra, que todo movimiento directo es independiente del orden de composición de las traslaciones y giros que lo integran.

Simetría central

Definición

Dado un punto O de un plano, se llama simetría de centro O a la aplicación entre los puntos del plano y los puntos del mismo plano que asigna como homólogo de O el mismo O y de $A \neq O$ el A' perteneciente a la recta OA y tal que A y A' equidisten de O.

Indicando la simetría central de centro O por S(O), se tendrá, $\forall A \neq O$

$$S(O) \cdot A = A' / [A' \in OA \wedge \overline{OA} = \overline{OA'}]$$

Simetría axial

Definición

Dada una recta e de un plano, se llama simetría axial de eje e a la aplicación entre los puntos del plano y los puntos del mismo plano, que asigna como homólogo de cualquier punto de e el mismo punto y de $A \notin e$ el A' tal que e sea la mediatriz de $\overline{AA'}$.

Es decir, $\forall A \notin e$:

$$S(e) \cdot A = A' / [AA' \perp e \text{ en } A_0 \wedge \overline{AA_0} = \overline{A_0A'}]$$

Movimientos geométricos inversos

Definición

Dado, en un cierto orden, un conjunto de un número impar de simetrías axiales, se llama movimiento geométrico inverso a la transformación que resulta al componer sucesivamente las dadas, en ese orden.

Es decir que un movimiento inverso es un "producto" de un número impar de simetrías axiales.

Si se tiene:

$$S(e_1) \cdot \Sigma = \Sigma'$$
$$S(e_2) \cdot \Sigma' = \Sigma''$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$S(e_{2n-1}) \cdot \Sigma^{2n-2} = \Sigma^{2n-1}$$

el movimiento inverso $\mathcal{M}_1$ es la transformación que aplicada directamente a Σ da como imagen Σ^{2n-1}

$$S(e_{2n-1}) \ldots . S(e_2) \cdot S(e_1) \cdot \Sigma = \Sigma^{2n-1}$$

O sea:

$$\mathcal{M}_1 \cdot \Sigma = \Sigma^{2n-1}$$

Movimientos geométricos

Definición

Se llama movimiento geométrico a cualquier movimiento geométrico directo o inverso.

Homotecia

Definición

Dado un punto O del espacio y un número real k, se llama homotecia de centro O y razón k a la aplicación que asigna como homólogo de O el mismo punto O y a todo punto A distinto de O un A' tal que pertenece a la recta OA y la razón de los segmentos orientados $\overline{OA}$ y $\overline{OA'}$ es el número k.

Es decir $\forall A \neq 0$

$$\mathcal{H}(O, k) \cdot A = A' / \left[A' \in OA \wedge \frac{\overline{OA}}{\overline{OA'}} = k \right]$$

Semejanza

Definición

Dado un conjunto de movimientos y homotecias, en un cierto orden y en número finito, se llama semejanza a la transformación compuesta de aquéllas en ese orden.

Si tenemos:

$$\mathcal{M}_1 \cdot \Sigma = \Sigma'$$
$$\mathcal{H}_1(O_1, k_1) \cdot \Sigma' = \Sigma''$$
$$\mathcal{M}_2 \cdot \Sigma'' = \Sigma'''$$
$$\mathcal{H}_2(O_2, k_2) \cdot \Sigma''' = \Sigma^{IV}$$

Entonces

$$\underbrace{\mathcal{H}_2 . \mathcal{M}_2 . \mathcal{H}_1 . \mathcal{M}_1}_{\text{Sem.}} \cdot \Sigma = \Sigma^{\text{IV}}$$

Es decir:

$$\text{Sem.}\ \Sigma = \Sigma^{\text{IV}}$$

Definición

Se llama transformación idéntica o identidad a la aplicación tal que cada elemento es imagen de sí mismo.

Definición

Dos transformaciones entre los mismos conjuntos se dicen equivalentes si coinciden las imágenes de cualquier elemento a través de ambas aplicaciones.

Como $\forall A$,

$$S(O) \cdot A = A'$$
$$G(O, \pi) \cdot A = A'$$

Luego $S(O)$ y $G(O, \pi)$ son transformaciones equivalentes, y se indica:

$$S(O) \doteq G(O, \pi)$$

Corolario

Toda simetría central $S(O)$ **es equivalente al giro** $G(O, \pi)$

Corolario

Toda simetría axial es equivalente a algún movimiento inverso.

Es una simple consecuencia de la definición de movimiento inverso.

Observación

De acuerdo con las definiciones de transformaciones métricas y la composición de transformaciones, pueden demostrarse los corolarios siguientes:

Corolario

Toda traslación es siempre equivalente al producto de dos simetrías axiales de ejes paralelos.

Corolario

Todo giro es equivalente al producto de dos simetrías axiales de ejes concurrentes en el centro de giro.

Las conclusiones anteriores permiten demostrar el fundamental teorema:

Teorema

Todo movimiento directo es equivalente al producto de dos simetrías axiales.

Resultando entonces los siguientes corolarios:

Corolario

La transformación compuesta de movimientos de cualquier tipo es equivalente a otro movimiento.

Corolario

La transformación compuesta de simetrías (en número finito), de cualquier tipo es equivalente a un movimiento.

Definición

Una transformación se dice involutiva si es equivalente a su inversa.

Sea la simetría de centro O

$$S(O) \cdot A = A'$$

Por significado de aplicación inversa:

$$S^{-1}(O) \cdot A' = A \qquad (1)$$

Y aplicando a A' la S(O):

$$S(O) \cdot A' = A \qquad (2)$$

De (1) y (2), por definición:

$$S(O) \doteq S^{-1}(O)$$

Esto es, la simetría central es una transformación involutiva.

3. GRUPO DE TRANSFORMACIONES MÉTRICAS

Cuando se intenta estudiar la estructura algebraica de un conjunto de transformaciones, para su ley de composición, el axioma G_2 de grupo se satisface siempre, puesto que tal composición es asociativa en todos los casos. Por eso la estructura de grupo queda definida por tres condiciones: existencia de ley de composición interna; existencia de elemento neutro para esa ley y existencia del simétrico para cualquier elemento del conjunto. Como enunciado equivalente al axiomático de estructura de grupo podría expresarse, como es usual en los desarrollos geométricos: Un conjunto de transformaciones geométricas adquiere una estructura de grupo si contiene:

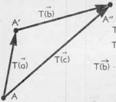
1. — Al producto de dos transformaciones cualesquiera del conjunto.

2. — A la transformación idéntica.

3. — A la inversa de toda transformación del conjunto.

Es inmediato, con este criterio, que el conjunto de **todas** las traslaciones forma grupo. En efecto:

1. — El producto de dos traslaciones $T(\vec{b})$ y $T(\vec{a})$ es otra traslación $T(\vec{c})$, donde $\vec{c} = \vec{a} + \vec{b}$



O sea:

$$T(\vec{a}) \cdot A = A'$$

$$T(\vec{b}) \cdot A' = A''$$

$$\left.\begin{array}{l} T(\vec{b}) \cdot T(\vec{a}) \cdot A = A'' \\ T(\vec{c}) \cdot A = A'' \end{array}\right\} \Rightarrow T(\vec{b}) \cdot T(\vec{a}) = T(\vec{c})$$

2. — La transformación idéntica puede considerarse como la traslación de vector nulo y en consecuencia pertenece al conjunto.

3. — La inversa de cualquier traslación pertenece al conjunto. Ello es cierto puesto que la inversa de una traslación $T(\vec{a})$ es la traslación de vector opuesto:

$$[T(\vec{a})]^{-1} = T(-\vec{a})$$

De idéntica manera, al formar el conjunto de todas las simetrías axiales (por ejemplo), resulta de inmediato que tal conjunto no adquiere estructura de grupo, puesto que el producto de dos simetrías axiales de ejes coplanares es una traslación o un giro, pero nunca otra simetría.

Si en lugar de los conjuntos de transformaciones de una misma clase, analizamos el formado por todos los movimientos, todas las simetrías y todas las semejanzas, llegamos a la conclusión de que tal conjunto posee estructura de grupo.

En efecto, se observa que se satisfacen las condiciones 2 y 3. En cuanto a la 1, también resultará satisfecha no bien se planteen las alternativas posibles:

a) El producto de dos movimientos es otro movimiento.

b) El producto de dos simetrías es un movimiento.

c) El producto de dos semejanzas es otra semejanza.

d) Movimiento por simetría (que es equivalente a un movimiento) es un movimiento.

e) Movimiento por semejanza es una semejanza.

f) Simetría por semejanza equivale a movimiento por semejanza o sea es otra semejanza.

Luego, cumpliéndose las tres condiciones establecidas, estamos en presencia de un grupo de transformaciones geométricas, que por su importancia en el estudio de las geometrías recibe el nombre de GRUPO FUNDAMENTAL.

Es decir:

Grupo Fundamental = {Movimientos, Simetrías, Semejanzas}

4. TRANSFORMACIONES PROYECTIVAS

Proyecciones

Definición

Dada una figura constituida por puntos y rectas y un punto no perteneciente a ella, llamado centro de la proyección, se llama proyección desde ese punto a la aplicación que asigna como homólogo de cada punto o cada recta dados, la recta o el plano que, respectivamente, determinan con el centro.

Sea: $\Sigma = \{A, B, C, \ldots a, b, c, \ldots\}$ la forma dada y $O \notin \Sigma$.

$OA = a'$; $OB = b'$; $\ldots O, a = \alpha'$; $O, b = \beta'$; ....

Luego:

$$\text{Proy}_O \cdot A = a'$$
$$\text{Proy}_O \cdot B = b'$$
$$\ldots\ldots\ldots\ldots$$

$$\text{Proy}_O \cdot a = \alpha'$$
$$\text{Proy}_O \cdot b = \beta'$$
$$\ldots\ldots\ldots\ldots$$

Los elementos $\alpha', b', \ldots \alpha', \beta', \ldots$ determinan la forma Σ' imagen de Σ a través de la Proy_o:

$$\text{Proy}_O \cdot \Sigma = \Sigma'$$

Observación

De manera idéntica podría definirse la proyección de una figura formada por puntos y rectas copuntuales desde una recta no perteneciente a ninguno de esos puntos y copuntual con las dadas, siendo en ese caso la figura imagen, la formada por los planos que la recta eje de proyección forma con los puntos o rectas del dominio.

Sección

Definición

Dada una figura formada por rectas y planos y un plano, llamado cuadro, no perteneciente a la forma, se llama sección de esa forma con ese cuadro a la aplicación que asigna como homólogo de cada recta y cada plano de la figura, el punto o la recta que determinan, respectivamente, con el cuadro.

Sea $\Sigma = \{a, b, c, \ldots \alpha, \beta, \gamma, \ldots\}$ la forma dada y $\pi \notin \Sigma$

$a, \pi = A'$; $b, \pi = B'$; $\ldots$; $\alpha, \pi = a'$; $\beta, \pi = b'$; $\ldots$

Luego:

$$\text{Sec}_\pi \cdot a = A'$$
$$\text{Sec}_\pi \cdot b = B'$$
$$\ldots\ldots\ldots\ldots$$
$$\text{Sec}_\pi \cdot \alpha = a'$$
$$\text{Sec}_\pi \cdot \beta = b'$$
$$\ldots\ldots\ldots\ldots$$

Los elementos $A', B', \ldots a', b', \ldots$ determinan la forma Σ' imagen de Σ a través de la Sec_π.

Es decir:

$$\text{Sec}_\pi \cdot \Sigma = \Sigma'$$

Observación

De manera idéntica podría definirse la sección de una forma constituida por planos y rectas todas coplanares con una recta no perteneciente a la forma, pero coplanar con los de ella, siendo en este caso la imagen, la figura constituida por los puntos de intersección de la recta eje con los planos y rectas de la forma.

Definición

Se llama colineación a la transformación que es el producto de cualquier número finito de proyecciones y secciones.

Observación

El ejemplo más simple y más "visible" que puede darse de una colineación es el de la fotografía. Entre un objeto real y su fotografía existe siempre una colineación, ya que aquélla es la transformada o imagen (y aquí vale más que nunca el término) del objeto a través de la proyección desde el objetivo de la cámara fotográfica, seguida por la sección con la película sensible. Y si se amplía esa foto se realiza una nueva colineación de modo que entre el objeto y la ampliación fotográfica existe una colineación total que es el producto de las siguientes transformaciones: proyección desde el objetivo de la cámara fotográfica, sección con la película sensible, proyección desde el foco de la máquina ampliadora, sección con el papel de la ampliación.

5. GRUPO DE TRANSFORMACIONES PROYECTIVAS

Resulta mucho más simple que en el caso de las transformaciones métricas, probar que el conjunto formado por todas las colineaciones posibles, adquiere estructura de grupo.

En efecto:

1. — Puesto que una colineación es una composición de un número finito de proyecciones y secciones, la composición de dos colineaciones es también el producto de proyecciones y secciones en número finito y en consecuencia, es otra colineación.

2. — La transformación idéntica es una colineación.

3. — La transformación inversa de una proyección es una sección, y la inversa de una sección es una proyección, luego la inversa de una colineación es otra colineación.

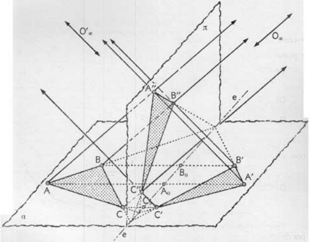
Queda entonces demostrada la existencia de un nuevo grupo geométrico: el de las colineaciones, que recibe el nombre de grupo proyectivo.

6. RELACIONES ENTRE EL GRUPO FUNDAMENTAL Y EL GRUPO PROYECTIVO

Según se ha visto, se ha conseguido definir dos conjuntos de transformaciones geométricas con cuyos elementos pueden desarrollarse dos diferentes tipos de geometría: la métrica euclidiana y la proyectiva. El problema que se plantea de inmediato es discutir si existe alguna relación entre tales grupos a fin de poder caracterizar los alcances relativos de esas geometrías.

Aun cuando, aparentemente, las transformaciones que engendran ambos grupos son diferentes, puede demostrarse que toda transformación métrica es también una colineación, no siendo en general cierta la implicación recíproca; con lo cual se arribaría a la conclusión de que el grupo fundamental es un subgrupo propio del grupo proyectivo.

Demostraremos una sola de las implicaciones directas, por ejemplo: "Toda simetría axial es también una colineación", pudiendo demostrarse todas las demás con criterio similar al que se usará en esta demostración.



Sea la simetría axial de eje e en el plano α, en la que ABC y A'B'C' son formas simétricas.

Es decir:

$$S(e) \cdot ABC = A'B'C' \qquad (1)$$

 Consideremos un plano $\pi \in e$ y tal que $\pi \perp \alpha$ y un punto impropio O_∞ no pertenecientes a los planes α o π. Proyectemos la forma ABC desde O_∞ y seccionemos con π.

$$\mathrm{Sec}_\pi \cdot \mathrm{Proy}_{O_\infty} \cdot ABC = A''B''C'' \qquad (2)$$

Unamos A'' con A', B'' con B', y C'' con C' quedando determinadas las rectas A'A''; B'B'', C'C'', que, demostraremos, son paralelas.

En efecto:

$$[BB' \perp e \text{ y } \pi \perp \alpha] \Rightarrow BB' \perp \pi \Rightarrow B''B_0 \perp BB' \Rightarrow BB''B' \text{ isósceles}$$

$$\Rightarrow \widehat{B''BB'} = \widehat{B''B'B} \qquad (3)$$

Análogamente $\widehat{AA''A'}$ isósceles

$$\Rightarrow \widehat{A''AA'} = \widehat{A''A'A} \qquad (4)$$

Pero $\widehat{B''BB'} = \widehat{A''AA'}$ por lados // (4)

De (2), (3), y (4):

$$\widehat{B''B'B} = \widehat{A''A'A} \qquad (5)$$

y como B'B // A'A (6)

y plano BB'B'' // plano AA'A'' (7)

De (5), (6) y (7)

$$B'B'' \,/\!/\, A'A''$$

De igual forma:

$$A'A'' \,/\!/\, C'C''$$

O sea:

$$B'B'';\ A'A'';\ C'C'' \equiv O'_\infty$$

Luego si la forma A''B''C'' se proyecta desde $O'\infty$ y se secciona con α se obtiene A'B'C':

$$\mathrm{Sec}_\alpha \cdot \mathrm{Proy}_{O'\infty} \cdot A''B''C'' = A'B'C' \qquad (8)$$

De (1) y (8)

$$\underbrace{\mathrm{Sec}_\alpha \cdot \mathrm{Proy}_{O'\infty} \cdot \mathrm{Sec}_\pi \cdot \mathrm{Proy}_{O_\infty}} \cdot ABC = A'B'C'$$

Pero la composición de aplicaciones comprendida por la llave es, por definición, una colineación C:

$$C \cdot ABC = A'B'C' \qquad (9)$$

Y de (1) y (9):

$$S(e) \doteq C$$

llegando así a la demostración buscada.

Probaremos ahora que la implicación recíproca no es, generalmente, válida, esto es, que una colineación no es equivalente a una de las ocho transformaciones métricas. Por tratarse de un enunciado negativo bastará encontrar un ejemplo donde sea imposible tal equivalencia. Basta para ello tomar como colineación el producto de la proyección desde un punto O de una forma ABC de un plano α, por la sección con un plano α' no paralelo al α.

$$\mathrm{Sec}_{\alpha'} \cdot \mathrm{Proy}_{O} \cdot ABC = A'B'C'$$

Resulta en tales condiciones, que:

$$\hat{A} \neq \hat{A}'\,;\ \hat{B} \neq \hat{B}', \text{y}\, \hat{C} \neq \hat{C}'\,,$$

y como todas las transformaciones métricas conservan los ángulos, ninguna de ellas puede ser equivalente a esa colineación.

En consecuencia:

$$\boxed{\text{Grupo Fundamental} \subset \text{Grupo Proyectivo}}$$

7. LAS GEOMETRÍAS

La interpretación matemática rigurosa de esta importante conclusión, que permitió y permite definir el problema de las estructuras geométricas, fue establecida por Klein, quien comienza por definir la geometría elemental métrico euclidiana.

Definición

La geometría estudia las propiedades invariantes de las figuras, respecto del grupo formado por todos los movimientos, más todas las simetrías, más todas las semejanzas, es decir, respecto del grupo fundamental.

O sea, son propiedades geométricas las que no dependen de la posición de la figura, ni de su magnitud ni su sentido, esto es, se conservan en los movimientos, semejanzas y simetrías.

Así, la famosa relación pitagórica del triángulo rectángulo es una propiedad métrica, puesto que es válida en cualquier triángulo rectángulo, cualquiera sea su posición relativa, su magnitud u orientación.

Si bien la geometría métrica, por nacer de la observación de la naturaleza, crea figuras abstractas que pertenecen a un espacio de tres dimensiones, nada impide, como se ha visto en el capítulo anterior, que por esa misma calidad de entes abstractos que maneja, pueda engendrar espacios abstractos de cualquier número de dimensiones y sustituir el grupo fundamental por cualquier otro grupo de transformaciones. De esta manera puede darse la definición más general de geometría.

Definición

La geometría es la ciencia que estudia las propiedades invariantes de los espacios abstractos de cualquier número de dimensiones, respecto de cada uno de los grupos de transformaciones que en ellos puedan definirse.

8. LAS ESTRUCTURAS GEOMÉTRICAS

La definición general anterior nos lleva a analizar la alternativa siguiente:

Sea A una geometría construida sobre la base de un grupo de transformaciones G_A y consideremos otro grupo G_B, más amplio que aquél, ésto es $G_A \subset G_B$. A una propiedad cualquiera P invariante para G_A se le aplican las transformaciones de G_B, pudiendo ocurrir:

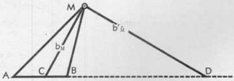
a) P es invariante también para cualquier aplicación de G_B.

b) P no se conserva al aplicar G_B.

Es inmediato que si se produce la primera alternativa, P no es propiedad característica de la geometría A, sino de la que depende del grupo más amplio G_B. En el segundo caso P es propiedad específica de A.

En este sencillo planteo, que fuera formulado también por Klein, está estrictamente determinada la delimitación de los contenidos de cada estructura geométrica.

Ejemplo



En geometría métrica, al estudiar las bisectrices de un ángulo M, interior de un triángulo no isósceles ABM y de su ángulo adyacente.

se llega fácilmente a la relación:

$$\frac{\overline{AC}}{\overline{BC}} = \frac{\overline{AD}}{\overline{BD}} \qquad (1)$$

La razón $\dfrac{\overline{AC}}{\overline{BC}}$, considerando los segmentos orientados, se llama razón simple de la terna ABC y se indica: $(ABC) = \dfrac{\overline{AC}}{\overline{BC}}$

Análogamente: $(ABD) = \dfrac{\overline{AD}}{\overline{BD}}$

Dada una cuaterna de puntos de una recta orientada, se llama razón doble o relación anarmónica de esa cuaterna al número real que es el cociente entre las dos razones simples que determinan los dos primeros puntos con el tercero y cuarto, respectivamente.

Se expresa:

$$(ABCD) = (ABC) : (ABD) = \frac{\overline{AC}}{\overline{BC}} : \frac{\overline{AD}}{\overline{BD}}$$

Aplicando este concepto en (1) y tomando en cuenta los signos

$$(ABCD) = -1$$

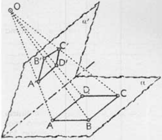
Es decir: "la relación anarmónica de la cuaterna determinada por los extremos de un lado de un triángulo no isósceles y las intersecciones de la recta de ese lado con las bisectrices de los ángulos interior y exterior, opuestos a ese lado, vale siempre -1". Y puesto que se define el **grupo armónico** de puntos como una cuaterna de puntos de una recta cuya relación anarmónica valga -1, resulta de lo visto, que por simples relaciones métricas se ha llegado al concepto de grupo armónico de puntos y en el triángulo ABM, (ABCD) es grupo armónico.

Si a un grupo armónico de puntos se le aplica cualquiera de las transformaciones del grupo fundamental, es inmediato que la cuaterna transformada es otra cuaterna armónica. Es decir, la relación de cuaterna armónica es invariante a través del grupo fundamental.

Pero puede demostrarse, aun cuando la demostración escapa a la naturaleza de este libro, que si a una cuaterna armónica se le aplica cualquier colineación, se obtiene también otra cuaterna armónica.

Luego la propiedad de una cuaterna de puntos de ser armónica es propiedad específica de la geometría proyectiva y no de la geometría métrica.

Por el contrario, si se considera la propiedad: "los lados opuestos de un paralelogramo son iguales", tal propiedad es invarante a través del grupo fundamental, pero como se verá en las operaciones siguientes, no lo es en cualquier colineación.



En ABCD

$$\overline{AD} = \overline{BC} \text{ y } \overline{AB} = \overline{CD}$$

Proyectemos el paralelogramo ABCD desde un punto O no perteneciente a α y seccionemos con α' secante con α.

$Sec_{\alpha'} \cdot Proy_O \cdot ABCD = A'B'C'D'$, donde $A'B'C'D'$ no es un paralelogramo y en general:

$$\overline{A'D'} \neq \overline{B'C'} \text{ y } \overline{A'B'} \neq \overline{C'D'}$$

Luego la propiedad enunciada no se conserva invariante al pasar al grupo más amplio y en consecuencia es característica de la geometría del grupo restringido.

9. METODOLOGÍA DE LAS ESTRUCTURAS

Sean las geometrías fundadas por los grupos G_A y G_B, tales que G_A es subgrupo propio de G_B. Consideremos una forma Σ invariante para G_A y no para G_B, es decir una Σ que no se modifique para las transformaciones de G_A, pero es modificada por las de G_B (que no pertenezcan a G_A). Sea ahora R una relación entre Σ y otra figura cualquiera, perteneciendo R a las relaciones o propiedades que estudia la geometría de G_B.

Si se aplica a R una de las transformaciones de G_B que también pertenezca a G_A (siempre posible pues $G_A \subset G_B$), Σ queda invariante, lo mismo que la figura arbitraria, luego R subsiste sobre Σ y en consecuencia R es una propiedad de la geometría de G_A. En caso de aplicar a R una de las transformaciones de G_B que no pertenecen a G_A, se modifica Σ y por lo tanto R deja de subsistir.

En este razonamiento queda contenida la metodología de los desarrollos geométricos, que puede sintetizarse en los dos enunciados del llamado principio de Klein.

I. — "Al sustituir un grupo G_A por otro más amplio G_B, quedan invariantes sólo algunas propiedades de la geometría fundada en el grupo G_A; tales propiedades corresponden a la geometría del nuevo grupo G_B. Las restantes aparecen, desde el nuevo punto de vista, no como propiedades de las figuras en sí, sino como propiedades de éstas respecto de una forma notable que se agrega a las mismas, la cual está caracterizada por la propiedad de que, fijada ésta, las únicas transformaciones de G_B que pueden realizarse, sin alterarla, son las de G_A."

Recíprocamente:

II. — "Dado un espacio y en él un grupo G_B, para estudiar las propiedades de este espacio, respecto de una figura Σ, se puede agregar ésta a las figuras del sistema, estudiando el sistema así ampliado desde el punto de vista del grupo G_B. O bien se considera dicho sistema sin ampliación, estudiando sus propiedades invariantes respecto de todas las operaciones de G_B que no alteran la forma Σ."

En consecuencia, el principio I permite generalizar toda geometría adoptando grupos cada vez más amplios, que contienen a los anteriores como subgrupos. Por el contrario, el II permite crear geometrías especiales contenidas en otras, fundadas en los subgrupos que se obtienen al fijar una figura Σ, es decir por "adjunción" de Σ.

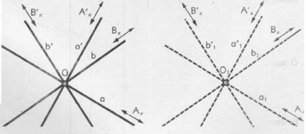
10. APLICACIÓN DEL PRINCIPIO DE KLEIN EN LA MÉTRICA Y LA PROYECTIVA

En el presente parágrafo analizaremos con más detalle la aplicación del principio antes mencionado, al caso concreto de las dos estructuras geométricas más conocidas, la métrica y la proyectiva. Para ello es necesario introducir la forma Σ, invariante para las operaciones del grupo fundamental y que sea modificada por las colineaciones que no pertenezcan a tal grupo.

Para determinar esa forma consideraremos primero la aplicación que recibe el nombre de involución circular.

Definición

Dado el conjunto de las infinitas rectas de un plano, pertenecientes a un punto O (haz de rayos), se llama involución circular a la aplicación del conjunto en sí mismo que asigna como homóloga de cada recta del haz a la recta del haz que es perpendicular a la misma.



Si designamos por I_R tal aplicación, $\forall a \in O$:

$$I_R \cdot a = a' / a \perp a' \wedge O \in a'$$

Obsérvese que si se aplica I_R a a', como la perpendicularidad satisface la propiedad simétrica:

$$I_R \cdot a' = a \qquad (1)$$

Y por definición de aplicación inversa:

$$I_R^{-1} \cdot a' = a \qquad (2)$$

De (1) y (2):

$$I_R \doteq I_R^{-1}$$

Y en consecuencia la aplicación I_R es una transformación involutiva, lo que justifica la designación dada desde el principio.

Se observa además que en I_R no pueden existir elementos homólogos de sí mismos (elementos unidos), pues la perpendicularidad no satisface la propiedad reflexiva. Se dice en tal caso que tal transformación involutiva, o simplemente involución, es de tipo elíptico, siendo además una colineación.

Si A_∞ es la dirección o punto impropio de la recta a, A'_∞ el impropio de a', etc., tales puntos impropios resultan también de seccionar los pares de homólogos de I_R con la recta impropia (r_∞) del plano sostén del haz de centro O.

Esto es:

$$Sec_{r\infty} \cdot I_R \cdot a = A'_\infty$$
$$Sec_{r\infty} \cdot I_R \cdot a' = A_\infty$$

O sea que si a y a' son homólogos a través de la aplicación I_R:

$a \overset{I_R}{\longleftrightarrow} a'$, A_∞ y A'_∞ son homólogos a través de la aplicación: $Sec_{r\infty} \cdot I_R \cdot Proy_O$, puesto que:

$$Proy_O \cdot A_\infty = a$$
$$I_R \cdot a = a'$$
$$Sec_{r\infty} \cdot a' = A'_\infty$$

O sea:

$$Sec_{r\infty} \cdot I_R \cdot Proy_O \cdot A_\infty = A'_\infty, \text{ de donde:}$$

$$A_\infty \xrightarrow{Sec_r \cdot I_R \cdot Proy_O} A'_\infty$$

Es decir, los pares (A_∞, A'_∞), (B_∞, B'_∞), ... son homólogos a través de la aplicación compuesta $Sec_{rx} \cdot I_R \cdot Proy_O = I_A$, que es también de tipo involutivo.

Obsérvese por último que el homólogo de un punto A_x es independiente de la I_R que se considere en el plano. En efecto, si en lugar de I_R se considera otra involución circular en el haz de centro O_1, se tendrá:

$$\left.\begin{array}{l} Proy_{O_1} \cdot A_x = a_1 / a_1 \parallel a \\ I_{R_1} \cdot a_1 = a'_1 / a'_1 \perp a_1 \end{array}\right\} \Rightarrow a'_1 \parallel a'$$

Luego: $$Sec_{rx} \cdot a'_1 = A'_x$$

O sea:

$$Sec_{rx} \cdot I_{R_1} \cdot Proy_{O_1} \cdot A_x = A'_x$$

Y en consecuencia:

$$Sec_{rx} \cdot I_R \cdot Proy_O = Sec_{rx} \cdot I_{R_1} \cdot Proy_{O_1}$$

Lo que equivale a decir que la involución I_A no depende de la involución circular que se considera, o lo que es lo mismo, que para cada plano existe una sola involución I_A. Tal unicidad da carácter importantísimo a I_A; por tal razón se la denomina la involución absoluta del plano.

La involución absoluta de un plano es, como las circulares, de tipo elíptico, es decir, carece de puntos unidos. Si se introduce el concepto de "imaginario", entonces esa involución tiene dos puntos unidos, imaginarios, únicos para cada plano, a los que se denomina puntos cíclicos de ese plano.

Esta involución absoluta de cada plano —engendrada a partir de las involuciones circulares, cualquiera de las cuales la individualiza— es la forma Σ que buscábamos. En efecto, si aplicamos a una involución circular cualquier transformación del grupo fundamental, como todas ellas conservan los ángulos, se obtiene otra involución circular y en consecuencia no se modifica la involución I_A, en el infinito. Pero si a una involución circular se la secciona con una recta cualquiera y al resultado de esa sección se lo proyecta desde un punto arbitrario, la nueva involución no es circular y por lo tanto en el infinito no se obtendrá la involución absoluta. Es esa, entonces, la forma necesaria para considerar los métodos posibles de desarrollo de la geometría métrica. Según el principio de Klein resultan entonces dos métodos:

a) Estudiar la geometría del grupo más amplio (el proyectivo), pero no desde el punto de vista de las propiedades de las figuras en sí mismas, sino de las figuras ampliadas mediante la adjunción de la involución absoluta del plano. En esta forma se tendrá el desarrollo por método proyectivo de la geometría métrica.

b) Estudiar las propiedades proyectivas que quedan invariantes, no para todas las colineaciones, sino para aquellas que no modifican la involución absoluta, que según se ha visto son las del grupo fundamental. Tendremos así el método métrico, cuyos recursos son entonces los movimientos, las simetrías y las semejanzas.

Ejemplo

En geometría proyectiva se demuestra, como consecuencia del denominado teorema de Steiner que cinco puntos del plano tres a tres independientes (no alineados) determinan una cónica y sólo una. Si se adjunta la involución absoluta se prueba que todas las circunferencias del plano pasan por los dos puntos cíclicos del mismo.

Consecuencia inmediata de las propiedades anteriores es el siguiente corolario: tres puntos no alineados determinan una circunferencia y sólo una.

Se ha obtenido así una propiedad de la geometría métrica por método proyectivo, ya que la determinación de la circunferencia por tres puntos no resulta como propiedad de la circunferencia en sí misma, sino en relación con la figura agregada: la involución absoluta.

Por el contrario, la misma propiedad de la circunferencia puede demostrarse por el método clásico de considerar las mediatrices de dos de los segmentos que determinan los tres puntos dados. Y aunque en los planteos tradicionales no se ponga de manifiesto, tal razonamiento implica simplemente aplicar simetrías. Esto es, se demuestra la propiedad usando una de las colineaciones que conserva la involución absoluta: estamos en presencia del método métrico.

11. GEOMETRÍAS ELEMENTALES

Puesto que la geometría es una rama de la ciencia matemática, al igual que ésta, debe desarrollarse sobre la base deductivo-formalista, existiendo la posibilidad de establecer distintos sistemas axiomáticos, que serán entonces diferentes puntos de partida para concretar también diferentes estructuras.

Si nos limitamos al espacio tridimensional, tres son las estructuras geométricas esenciales: la geometría proyectiva, la geometría afín y la geometría métrica euclidiana. De la proyectiva y la métrica, tomadas como modelos para fundamentar este capítulo han surgido ya características estructurales. Sintetizaremos esas conclusiones efectuando el enlace final entre ellas y de ellas con la geometría afín.

Geometría proyectiva

Según la definición de geometría, resulta que la geometría proyectiva es la ciencia que estudia las propiedades invariantes de las formas, respecto del grupo de todas las colineaciones, es decir respecto del grupo proyectivo. Tales propiedades dependen entonces de aquellas transformaciones y pueden demostrarse con recursos específicamente geométricos o bien asociando elementos de algunos cuerpos numéricos y especialmente el de los números reales. Entiéndase que tales recursos no originan distintas geometrías, como ciertas designaciones han confundido y confunden todavía, sino que significan solamente distintos métodos de desarrollo. En el primer caso se tiene el método sintético; en el segundo el analítico, es decir, que el nombre de geometría analítica, tan usado, no corresponde exactamente a una geometría, sino a una manera de desarrollarla. En la actualidad, y ante la formulación algebraica que se introduce en la matemática moderna se prefiere no separar ortodoxamente tales métodos, sino recurrir a uno u otro, según faciliten el avance del conocimiento.

Desarrollada la geometría proyectiva por método sintético o analítico, o por ambos, resulta que son invariantes en la misma, la incidencia, la pertenencia, el orden y las relaciones anarmónicas o razones dobles que se conservan a través de todas las colineaciones.

Geometría afín

En la geometría proyectiva, un punto, una recta y un plano pueden ser indistintamente propios o impropios y sin necesidad de especificar la naturaleza de los mismos, toda propiedad proyectiva es válida en todos los casos de combinaciones posibles de esos entes. En otras palabras, un punto propio o impropio, una recta propia o impropia, un plano propio o el impropio, son, proyectivamente equivalentes, no existiendo diferencia geométrica entre ellos: es decir en geometría proyectiva no existe el paralelismo.

Si los axiomas estructurales de la geometría que se pretende construir, introducen una distinción entre elementos propios e impropios, y del grupo de colineaciones se consideran solamente las que conservan esa diferencia, es decir, las que aplicadas a elementos propios o impropios, dan por imágenes, respectivamente, elementos propios o impropios, se obtiene un grupo restringido del grupo proyectivo.

Las transformaciones de tal grupo deben conservar, entonces, el paralelismo. Si la geometría es bidimensional, deberá conservarse la recta impropia del plano; si es tridimensional, el plano en el infinito del espacio.

Pertenecen a ese grupo todas las transformaciones del grupo fundamental, más las colineaciones que conservan el paralelismo, es decir, las proyecciones y secciones paralelas.

El grupo así constituido está incluido en el proyectivo y contiene a su vez al fundamental: es el llamado grupo afín y la geometría que de él resulta es el perfecto eslabón de enlace entre la proyectiva y la métrica euclidiana. Tal geometría se denomina geometría afín o métrica paralela.

La estructura afín adquiere una importancia fundamental en los desarrollos geométricos modernos que son de naturaleza vectorial, como se discutirá en el capítulo XII, donde el manejo de vectores libres implica la utilización de vectores equipolentes y en tales condiciones se construye, en realidad, una geometría afín.

Son invariantes en la geometría afín la incidencia, la pertenencia, el paralelismo, la ordenación y la razón simple de tres puntos de una recta.

Las áreas y los volúmenes son también invariantes, pero **relativos,** puesto que al realizar una transformación afín, el área o el volumen de la forma original queda multiplicado por un factor constante; en cambio la razón de dos áreas es un invariante absoluto.

Geometría métrica euclidiana

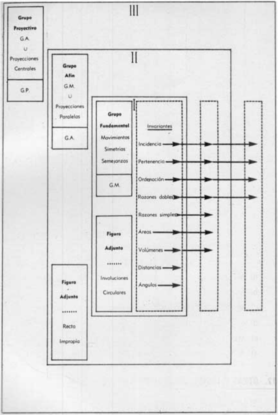
Introducida la geometría afín, puede obtenerse el grupo fundamental como subgrupo del afín, considerando las colineaciones de este último que conservan la perpendicularidad, lo que equivale, según se ha visto, a mantener invariante la involución absoluta del plano (si se desarrolla geometría plana), o el círculo en el infinito (si se desarrolla la geometría del espacio). Tales colineaciones, que conservarán todos los ángulos, transformarán una forma cualquiera en otra directa o inversamente semejante y son precisamente los movimientos, las simetrías y las semejanzas.

Resulta así, en este ordenamiento estructural:

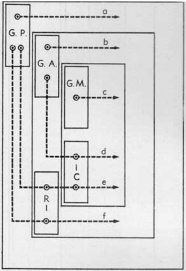
$$\boxed{\text{Grupo Fundamental} \subset \text{Grupo Afín} \subset \text{Grupo Proyectivo}}$$

Aparecen como invariantes de la geometría métrica, la incidencia, la pertenencia, la congruencia, el paralelismo, la perpendicularidad, las áreas y los volúmenes. Son invariantes específicos: los ángulos como invariante absoluto, y las distancias —de ahí el nombre de métrica— como invariante relativo.

Teniendo en cuenta todo lo expuesto, y si nos atenemos al caso del espacio bidimensional (aún cuando lo mismo puede hacerse para tres dimensiones), podría construirse el siguiente esquema de vinculación de estructuras, donde el grupo métrico está representado por el rectángulo I, el afín por el II y el proyectivo por el III.



Y considerando la distribución de elementos de la figura anterior; podría representarse como sigue la metodología de las geometrías correspondientes a esos grupos.



a) Método proyectivo para la proyectiva elemental

b) Método afín para la geometría afín

c) Método métrico para la geometría métrico euclidiana

d) Método afín para la geometría métrico euclidiana

e) Método proyectivo para la geometría métrico euclidiana

f) Método proyectivo para la geometría afín.

12. OTRAS ESTRUCTURAS GEOMÉTRICAS

El capítulo siguiente contiene el desarrollo de las estructuras geométricas no euclidianas, analizándose las relaciones entre ellas y con la métrico euclidiana. Pero además de las estructuras hasta ahora discutidas y las reservadas para ese capítulo pueden plantearse muchas otras cuyo análisis completo escapa notablemente al alcance de esta obra. Sin embargo queremos mencionar, al menos, otros dos tipos geométricos: la geometría proyectiva superior y la geometría de posición o topología.

Geometría proyectiva superior

Las geometrías elementales engendran espacios tridimensionales; sus entes primitivos son el punto, la recta y el plano y las formas transformadas son de naturaleza real. Una primera ampliación consiste, como se vio en la definición general de la geometría, en concebir espacios abstractos de cualquier número de dimensiones. Pero no es ésta la única condición de importancia. Interesa también ampliar el significado del elemento generador de esos espacios de modo tal que los axiomas que lo definen implícitamente puedan ser satisfechos por cualquier forma geométrica. Por último es necesario que las transformaciones puedan ser aplicadas tanto a formas reales como complejas.

Con tales condiciones se desarrolla la denominada geometría proyectiva superior.

Definición

Se llama geometría proyectiva superior a la que tiene como grupo característico el formado por todas las colineaciones (aplicables aun a formas complejas) en un espacio abstracto de cualquier número de dimensiones, cuyo elemento generador puede ser cualquier forma geométrica.

Topología o geometría de posición

Si se construye una figura Σ cualquiera sobre una lámina plástica muy elástica, al someter dicha lámina a fuerzas de cualquier tipo, sin que la desgarren, se obtendrá una deformación de la misma, y sobre ella una figura Σ', transformada de Σ a través de esa deformación.

Las formas Σ y Σ', que en general no pueden vincularse por una colineación proyectiva, presentan sin embargo estas relaciones:

Σ y Σ' están vinculados por una aplicación puntual f biyectiva, pues a todo punto de Σ corresponde uno y sólo uno de Σ' y recíprocamente.

Además, si dos puntos de Σ son infinitamente próximos, sus transformados en Σ' son también infinitamente próximos, por cuanto hay deformación, pero sin rotura.

Esta idea puede concretarse de la siguiente manera:

Definición

Una aplicación f de Σ en Σ' es continua, si las imágenes de puntos infinitamente próximos de Σ son puntos infinitamente próximos de Σ'.

Definición

Una aplicación biyectiva f de Σ en Σ' es bicontinua si son continuas f y su inversa f^{-1}.

Definición

Se llama homeomorfismo o transformación topológica a toda transformación biyectiva y bicontinua.

El grupo de todas las transformaciones topológicas, que evidentemente contiene al grupo proyectivo permite engendrar una nueva estructura geométrica: la topología, geometría de posición o análisis situs.

En geometría métrica, una circunferencia, una elipse, una parábola y una hipérbola son figuras diferentes con propiedades métricas distintas.

En proyectiva, todas esas figuras son equivalentes entre sí; son simplemente cónicas con las mismas propiedades proyectivas.

En topología, todas las poligonales simples y cerradas, todas las curvas cerradas y en consecuencia las elipses, etc., son formas topológicamente equivalentes, pues puede pasarse de una a otra por transformaciones bicontinuas.

Todas esas líneas son las llamadas **curvas cerradas de Jordán** con los mismos invariantes topológicos, que resultan así ser propiedades esenciales de las formas, de tipo absolutamente cualitativo.

CAPITULO XI

Geometrías no euclidianas

La teoría de la relatividad es una creación genial de la mente humana. Cuando le preguntaron a Einstein cuál fue su comienzo, respondió simplemente: "El desafío a un axioma". Esta frase, casi extraña, es el fundamento de la matemática moderna y, en especial, de la geometría.

Los números hipercomplejos fueron aceptados cuando Hamilton se decidió a abandonar, después de múltiples ensayos, el axioma de conmutatividad de la multiplicación. Las lógicas multivalentes nacieron cuando Lukasiewicz dejó de lado el axioma aristotélico del tercero excluido. La geometría comenzó a jerarquizarse y clarificarse en todos sus aspectos cuando Bolyai y Lobatchefsky se decidieron a negar el discutido postulado del paralelismo euclídeo.

1. Geometría de Euclides

Ya se ha considerado en este libro la obra de Euclides y sus imperfecciones. Para facilitar la comprensión de las geometrías no euclidianas, es conveniente volver a considerar los cinco axiomas que sirven de base a su geometría plana:

I. Desde cualquier punto se puede trazar una recta a cualquier otro.

II. Toda recta limitada puede prolongarse indefinidamente en la misma dirección.

III. Con cualquier centro y cualquier radio se puede trazar una circunferencia.

IV. Todos los ángulos rectos son iguales (1) entre sí.

---

(1) Actualmente la palabra "igual' se reserva exclusivamente, como ya se ha visto, para designar un único objeto. Es decir, un ángulo o un ente cualquiera, solamente es igual a sí mismo.

Si dos ángulos tienen igual medida, o sea, les corresponde a ambos como medida el mismo número real, los ángulos son congruentes.

$$\text{med } \hat{A} = \text{med } \hat{B} \iff \hat{A} \equiv \hat{B}$$

V. Si una recta, al cortar a otras dos, forma de un mismo lado ángulos internos cuya suma es menor que dos rectos, esas dos rectas prolongadas indefinidamente se cortan del lado en que están los ángulos cuya suma es menor que dos rectos.

Respecto del postulado V ya se ha dicho que Euclides, considerado paradójicamente como el primer geómetra no euclidiano, evita utilizarlo mientras le es posible y que las 28 proposiciones iniciales de su obra constituyen, con los cuatro primeros postulados, la **geometría absoluta** plana de Euclides, independiente del postulado de paralelismo.

Utilizando esta geometría absoluta puede demostrarse que, en un plano, por un punto exterior a una recta pasa **por lo menos** una paralela a dicha recta.

El postulado II requiere también una explicación especial. En realidad, su enunciado asegura únicamente que la recta no es un conjunto acotado de puntos, pero siempre se supuso, de acuerdo con la tácita aceptación de Euclides, que la recta era de longitud infinita. Recién en 1854, Bernhard Riemann (1826-1866), en su famosa disertación en la Universidad de Göttingen, hizo la distinción entre ambos conceptos. Es decir, el axioma II exige solamente que una recta no tenga extremos, pero esto no contradice el hecho de que pueda tener longitud finita.

Euclides utiliza la infinitud de la recta recién en la proposición 16 y esta suposición es la que lleva a probar la existencia de una paralela por un punto exterior a una recta.

Vale decir, considerando el postulado II sin suposiciones implícitas, con el enunciado más preciso de que "una recta es un conjunto no acotado", el postulado del paralelismo admite tres expresiones diferentes que aseguran: 1º) la no existencia de paralelas, 2º) la existencia de una paralela única, o 3º) la existencia de más de una paralela. En el cuadrilátero de Saccheri esas posibilidades corresponden respectivamente a la hipótesis del ángulo obtuso, recto o agudo.

Cada una de estas alternativas es independiente de los otros cuatro postulados y da origen a una geometría distinta. Es decir, el postulado V separa a la geometría en tres tipos: elíptica, parabólica o euclídea, e hiperbólica. Las geometrías elíptica e hiperbólica son consideradas como las geometrías no euclidianas propiamente dichas.

2. LA NEGACIÓN DEL AXIOMA V

Ya se han indicado varios enunciados equivalentes al postulado del paralelismo euclídeo. El más difundido es el propuesto por Playfair, cuya versión aparece comúnmente en los textos de geometría para enseñanza secundaria:

"Por un punto exterior a una recta pasa una y solamente una paralela a dicha recta."

Conviene insistir en que la existencia de una paralela puede probarse si se supone la infinitud de la recta. En ese caso, el postulado no se refiere a su existencia sino a su unicidad.

Exigiendo la infinitud de la recta, el axioma puede enunciarse así:

"Por un punto exterior a una recta pasa **a lo sumo** una paralela a dicha recta."

Por lo tanto, para probar la independencia de este axioma en el sistema de Euclides-Hilbert, sólo puede negarse la unicidad de la paralela, es decir, suponer que por un punto exterior a una recta pasa **más de una** paralela a dicha recta.

Friedrich Gauss (1777-1855) en Alemania fue el primero en considerar la posibilidad de una geometría que negase el postulado V. Gauss nunca publicó sus trabajos y la idea fue conocida a través de Johann Bolyai (1802-1860) en Hungría y de Nicolai Lobatchefsky (1793-1856) en Rusia.

Los tres matemáticos citados consideraron independientemente esta alternativa y sustituyeron el axioma de Euclides por el siguiente:

"La paralela a una recta por un punto exterior a ella no es única."

Por varios años, la geometría anterior, conocida como la geometría de Lobatchefsky, fue la única geometría no euclidiana hasta la presentación de Riemann, quien negó, no ya la unicidad de la paralela sino su existencia, con el postulado siguiente:

"Por un punto exterior a una recta no pasa ninguna paralela a dicha recta."

La geometría de Euclides y la de Lobatchefsky pueden desarrollarse según la rigurosa formulación de Hilbert con la única sustitución, para la segunda, del postulado de paralelismo. La geometría de Riemann exige, en cambio, otro sistema de axiomas y su desarrollo riguroso escapa a consideraciones elementales.

3. COMPATIBILIDAD DE LA GEOMETRÍA EUCLÍDEA

Como se ha indicado en el capítulo VI, ningún sistema axiomático tiene valor si no se establece, en primer término, su consistencia o compatibilidad, es decir, si no existen modelos para el mismo.

Antes de analizar las geometrías no euclidianas es importante considerar un modelo para la geometría euclídea. La geometría de Euclides, al ser compatible, proporciona también interpretaciones de las geometrías no euclídeas, como se verá más adelante.

Un modelo sencillo lo proporciona la geometría analítica. Claro está que se trata de una prueba de consistencia relativa, pues al establecer un modelo que depende de la aritmética del número real, la geometría de Euclides resulta **tan consistente como** el sistema de los números reales.

El método consiste en interpretar los primitivos de Hilbert para la geometría plana y luego probar los 15 axiomas correspondientes como teoremas algebraicos.

Los términos primitivos son dos conjuntos de elementos (puntos y rectas) y tres relaciones (pertenencia, orden y congruencia). Estos primitivos pueden interpretarse algebraicamente de la siguiente manera:

1) **punto:** par ordenado de números reales.

2) **recta:** conjunto de puntos $L = \{(x\,;y) \,/\, ax + by + c = 0\}$

   La expresión $ax + by + c = 0$ se llama ecuación de la recta. En ella a, b y c son números reales, $a^2 + b^2 > 0$ y si dos ecuaciones son tales que sus primeros miembros difieren en un factor constante, ambas ecuaciones definen la misma recta.

3) **relación de pertenencia** entre punto y recta: el punto $(x_0\,; y_0)$ pertenece a la recta de ecuación $ax + by + c = 0$ si y sólo si $ax_0 + by_0 + c = 0$.

4) **relación de orden** entre tres puntos: el punto $(x_0\,; y_0)$ está **entre** los puntos $(x_1\,; y_1)$ y $(x_2\,; y_2)$ si y sólo si existe un número real $t\,(0 < t < 1) \,/\, x_0 = x_1 + t\,(x_2 - x_1) \wedge y_0 = y_1 + t\,(y_2 - y_1)$

5) **relación de congruencia** entre dos pares de puntos :

   el par de puntos $[(x_1\,; y_1)\,;\,(x_2\,; y_2)]$ es congruente con el par $[(x_1'\,; y_1')\,;\,(x_2'\,; y_2')]$ si y sólo si

$$(x_2 - x_1)^2 + (y_2 - y_1)^2 = (x_2' - x_1')^2 + (y_2' - y_1')^2$$

5') **relación de congruencia** entre dos ángulos:

   el ángulo $[(x_1\,; y_1)\,,(x_0\,; y_0)\,,(x_2\,; y_2)]$ es congruente con el ángulo $[(x_1'\,; y_1')\,,(x_0'\,; y_0')\,,(x_2'\,; y_2')]$ si y sólo si

$$\frac{(x_1 - x_0)\,(x_2 - x_0) + (y_1 - y_0)\,(y_2 - y_0)}{\sqrt{(x_1 - x_0)^2 + (y_1 - y_0)^2}\;\sqrt{x_2 - x_0)^2 + (y_2 - y_0)^2}} =$$

$$= \frac{(x_1' - x_0')\,(x_2' - x_0') + (y_1' - y_0')\,(y_2' - y_0')}{\sqrt{(x_1' - x_0')^2 + (y_1' - y_0')^2}\;\sqrt{(x_2' - x_0')^2 + (y_2' - y_0')^2}}$$

Puede probarse que esta interpretación de los términos primitivos de la geometría plana de Euclides transforma a los axiomas en proposiciones verdaderas. La comprobación es sencilla en algunos casos y complicada en otros, pero puede establecerse por métodos algebraicos exclusivamente.

Como ejemplo, demostraremos el primer axioma de pertenencia o incidencia:

Dos puntos distintos determinan una recta.

Será necesario probar que dados dos puntos distintos $(x_0\,; y_0)$ y $(x_0'\,; y_0')$ existe una y sólo una recta cuya ecuación $ax + by + c = 0$ es verificada simultáneamente por ambas cuplas.

1º parte: existe por lo menos una recta que pasa por $(x_0\,; y_0)$ y $(x_0'\,; y_0')$.

En efecto, la ecuación

$$(y_0' - y_0)x + (x_0 - x_0')y + (x_0'y_0 - x_0y_0') = 0$$

define una recta pues reune las condiciones exigidas y puede comprobarse fácilmente que el primer miembro se anula al reemplazar x e y por x_0 e y_0 y también por x_0' e y_0'.

2º parte: la recta hallada es única.

Sea $ax + by + c = 0$ (1) la ecuación de otra recta cualquiera que pase por los mismos puntos.

Entonces,

$$[ax_0 + by_0 + c = 0 \wedge ax_0' + by_0' + c = 0] \quad (2)$$
$$\Rightarrow a(x_0' - x_0) + b(y_0' - y_0) = 0$$

Como a y b no pueden ser nulos simultáneamente, supongamos:

$$a \neq 0 \Rightarrow y_0' - y_0 \neq 0 \text{ pues si } y_0' - y_0 = 0 \ (3) \Rightarrow$$
$$\Rightarrow a(x_0' - x_0) = 0 \Rightarrow x_0' - x_0 = 0 \quad (4)$$

De (3) y (4) los puntos $(x_0 ; y_0)$ y $(x_0' ; y_0')$ coincidirían.

Al dividir ambas expresiones en (2) por $a \neq 0$, se obtiene:

$$x_0 + \frac{b}{a}y_0 + \frac{c}{a} = 0 \wedge x_0' + \frac{b}{a}y_0' + \frac{c}{a} = 0$$

Si $\frac{b}{a} = p \wedge \frac{c}{a} = q$, entonces

$$x_0 + py_0 + q = 0 \wedge x_0' + py_0' + q = 0$$

Como $y_0' - y_0 \neq 0$, al resolver el sistema anterior queda :

$$p = \frac{x_0 - x_0'}{y_0' - y_0} \wedge q = \frac{x_0'y_0 - x_0y_0'}{y_0' - y_0}$$

Reemplazando en (1) después de haber dividido por $a \neq 0$:

$$x + \frac{x_0 - x_0'}{y_0' - y_0}y + \frac{x_0'y_0 - x_0y_0'}{y_0' - y_0} = 0$$

$$\Rightarrow (y_0' - y_0)x + (x_0 - x_0')y + (x_0'y_0 - x_0y_0') = 0$$

que es la ecuación de la recta obtenida en la primera parte. Por lo tanto, queda probada su unicidad.

De la misma forma pueden probarse como teoremas algebraicos los restantes postulados de la geometría euclidiana.

4. GEOMETRÍA ABSOLUTA

Como se ha expresado anteriormente, es posible un desarrollo geométrico fecundo sin recurrir al postulado de paralelismo. Este desarrollo, que postula la infinitud de la recta, es común a las geometrías euclídea e hiperbólica y constituye un ejemplo de sistema axiomático no categórico.

Es interesante conocer los enunciados de algunos teoremas válidos en ambas hipótesis para la geometría del plano:

T_1 : Si dos rectas de un plano son perpendiculares a una tercera, entonces dichas rectas no se cortan.

T_2 : Por un punto exterior a una recta pasa por lo menos una paralela a dicha recta.

T_3 : Dadas dos rectas y una transversal, si existe un par de ángulos alternos internos congruentes, entonces las dos rectas no se cortan.

Obsérvese que el recíproco de este teorema:

"Si dos rectas cortadas por una transversal son paralelas, entonces los ángulos alternos internos son congruentes", no puede demostrarse sin el axioma de unicidad de la paralela.

T_4 : Los ángulos de la base de un triángulo isósceles son congruentes.

T_5 : En todo triángulo, un ángulo exterior es mayor que cada uno de los ángulos interiores no adyacentes.

T_6 : Las diagonales del cuadrilátero de Saccheri son congruentes.

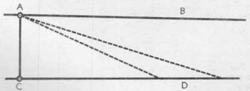
T_7 : Los ángulos opuestos a la base del cuadrilátero de Saccheri son congruentes.

T_8 : En el cuadrilátero de Saccheri el lado opuesto a la base es congruente o mayor que ella.

T_9 : En todo triángulo, la suma de los ángulos interiores es menor o congruente con un ángulo llano.

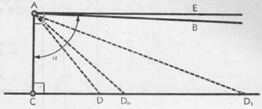
Para aclarar el significado de los teoremas T_1 y T_2 en la geometría absoluta, conviene considerar la siguiente **definición de paralelas,** debida a Gauss y propuesta también por Bolyai en su obra "La ciencia absoluta del espacio".

"Si dos rectas coplanares AB y CD no se cortan, mientras que toda recta que pasa por A entre AB y AC corta a CD, entonces AB es paralela a CD."



En su tratado "Teoría de las paralelas" Lobatchefsky considera el significado de esta definición y la vincula con el ángulo de paralelismo.

Si se considera en un plano una recta cualquiera r, un punto exterior A y la perpendicular AC a r, las rectas que pasan por A pueden clasificarse en dos categorías: las que intersectan a CD y las que no la cortan. Estos dos conjuntos no son vacíos pues al primero pertenece, por ejemplo, la recta AD y al segundo la recta AE perpendicular a AC en A, que no corta a CD de acuerdo con el teorema T_1.



Puede probarse que existe por lo menos una recta **frontera** entre ambos conjuntos, que pertenece al conjunto de las no secantes.

Si se elige sobre CD una sucesión de puntos $D_0, D_1, \ldots, D_{n-1}, D_n, \ldots$ tal que cada triángulo $AD_{n-1}D_n$ sea isósceles de base AD_n, dicha recta puede hallarse como límite de la sucesión AD_n para $n \to \infty$ y es la "primera" que no corta a CD, o sea, es paralela a CD según la definición de Gauss.

El ángulo α que forma dicha paralela con la vertical es el **ángulo de paralelismo.**

Toda recta que forme con AC un ángulo menor que α intersecta a CD y es secante o no paralela a CD. Toda recta que forme con AC un ángulo mayor que α y menor o congruente con un ángulo recto no corta a CD y es no secante o paralela a CD en el sentido euclídeo.

El ángulo de paralelismo es agudo o recto y depende de la longitud del segmento AC.

Es decir, $\forall h : \alpha = \Pi(h)$ donde h es la longitud del segmento AC y Π es la función que la vincula con el ángulo de paralelismo. En el caso euclídeo, por supuesto, la función Π es constante y α es recto.

Si h crece, el ángulo de paralelismo no crece, es decir

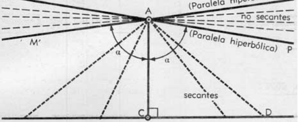
$$h' > h \Rightarrow \Pi(h') \leqslant \Pi(h)$$

Puede probarse además que el paralelismo es una relación simétrica y que si dos rectas son paralelas a una tercera son paralelas entre sí.

5. GEOMETRÍA DE LOBATCHEFSKY

El postulado hiperbólico de paralelismo establece la no unicidad de la paralela a una recta por un punto exterior a la misma.

Utilizando este postulado y las conclusiones de la geometría absoluta puede probarse que existen solamente **dos** paralelas a una recta por un punto exterior.



Es decir, existen dos rectas que pasan por A, forman con la vertical AC ángulos agudos iguales y no cortan a CD y además todas las rectas que pasan por A y son interiores a los ángulos CAM o CAM' cortan a la recta CD, mientras las rectas interiores al ángulo pp' no cortan a CD.

Las rectas p y p' son las paralelas hiperbólicas o simplemente paralelas en la geometría de Lobatchefsky. Las rectas interiores a MAM' son las rectas secantes y las interiores a pp' son las no secantes o paralelas en el sentido euclídeo.

En la geometría de Lobatchefsky no existen, por supuesto, figuras distintas que sean semejantes, ya que la existencia de figuras semejantes y no congruentes es equivalente a la unicidad de la paralela.

En la geometría de Euclides, al existir figuras no congruentes y semejantes, las longitudes se miden con respecto a una unidad arbitraria de medida y son, por lo tanto, "relativas". Los ángulos, en cambio, admiten unidad de medida "absoluta", susceptible de definición geométrica, como es el ángulo recto o el ángulo de un radián. Es decir, en la geometría euclídea, los ángulos son "absolutos" pero las distancias no. En la geometría de Lobatchefsky, a cada ángulo de paralelismo corresponde una única distancia y entonces, tanto los ángulos como las distancias son absolutos. Lo mismo sucede en la geometría elíptica.

En el caso hiperbólico, la función Π que vincula ángulos de paralelismo y distancias es estrictamente decreciente, es decir:

$$h' > h \Longrightarrow \Pi(h') < \Pi(h)$$

y además,

$$\text{si } h \to \infty\text{, entonces } \Pi(h) \to 0\,.$$

Algunas proposiciones de la geometría hiperbólica son las siguientes:

1) Los ángulos opuestos a la base en el cuadrilátero de Saccheri son agudos.
2) En todo triángulo, la suma de sus ángulos interiores es menor que un ángulo llano (la medida de la diferencia entre ambos es el defecto esférico.)
3) En todo triángulo, el defecto esférico es proporcional al área.
4) Dos triángulos son semejantes si y sólo si son congruentes.
5) Dos rectas paralelas no son equidistantes.
6) Ningún cuadrilátero es rectángulo.

6. COMPATIBILIDAD DE LA GEOMETRÍA HIPERBÓLICA

Corresponde ahora probar la consistencia de la geometría de Lobatchefsky. Para ello, resulta conveniente buscar un modelo en la geometría euclídea, cuya compatibilidad puede demostrarse en la forma indicada anteriormente.

El modelo siguiente es el de Henri Poincaré (1854-1912).

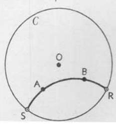
Interpretación

punto: punto interior a un círculo fundamental C.

recta: diámetro del círculo fundamental, excluidos los extremos, o arco de circunferencia perpendicular al círculo C e interior al mismo.

Las **relaciones de pertenencia y de orden** tienen el mismo significado de la geometría euclídea.

Para interpretar la **relación de congruencia** entre segmentos y entre ángulos es conveniente dar previamente algunas definiciones.



La longitud del "segmento" AB sobre la "recta" SR se define así:

$$AB = \left| \log_e \frac{\frac{\overline{AR}}{\overline{BR}}}{\frac{\overline{AS}}{\overline{BS}}} \right| = |\log_e (ABRS)|$$

Dos pares de puntos, o sea, dos segmentos, son congruentes si y sólo si sus longitudes son iguales.

El ángulo formado entre dos "rectas" hiperbólicas es el ángulo formado por sus tangentes en el vértice (si son circunferencias) y dos ángulos son congruentes en el mismo sentido de la geometría euclídea.

Pueden probarse ahora los axiomas del plano.

Ejemplo

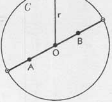
Axioma 1 de pertenencia:

Dos puntos distintos determinan una y sólo una recta.

En el modelo indicado se debe demostrar que por dos puntos cualesquiera, interiores al círculo C, pasa una sola circunferencia perpendicular a C (o un solo diámetro de C)

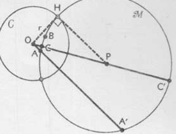
Sea O el centro del círculo fundamental, r su radio y A y B dos puntos interiores al mismo.

1er. caso) A y B alineados con O



La demostración es inmediata, pues el diámetro AB es la única recta que pasa por ambos.

 2º caso) A y B no alineados con O



a) existe una circunferencia perpendicular al círculo fundamental que pasa por A y B.

Sea A′ un punto de la semirrecta $\overrightarrow{OA}$ / $OA \cdot OA' = r^2$

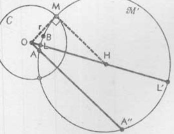
La circunferencia $\mathcal{M}$ que pasa por A, B y A′ es perpendicular a C. En efecto, sea P el centro de dicha circunferencia. $\overrightarrow{OP}$ la corta en los puntos C y C′.

Por propiedades demostradas en la geometría de Euclides:

$$r^2 = OA \cdot OA' \,(1) = OC \cdot OC' = (OP - PH)\,(OP + PH) = OP^2 - PH^2$$

$r^2 = OP^2 - PH^2 \Rightarrow OP^2 = OH^2 + HP^2 \Rightarrow OHP$ rectángulo en H $\Rightarrow$ la circunferencia $\mathcal{M}$ es perpendicular a la circunferencia C

b) la circunferencia perpendicular a C por A y B es única.



Si existe otra circunferencia $\mathcal{M}'$ perpendicular a $\mathcal{C}$ por A y B, $\overrightarrow{OA}$ corta a esa circunferencia en un punto A'' / $r^2 + MH^2 = OH^2$

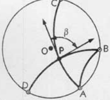
$$\Rightarrow r^2 = OH^2 - MH^2 = (OH - MH)(OH + MH) = OL \cdot OL' = OA \cdot OA'' \quad (2)$$

De (1) y (2):

$$[r^2 = OA \cdot OA' \wedge r^2 = OA \cdot OA''] \Rightarrow A' = A''$$

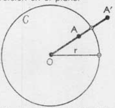
O sea, la circunferencia $\mathcal{M}'$ es la misma circunferencia $\mathcal{M}$ que, por lo tanto, es única.

Es interesante considerar, en este modelo de Poincaré, la validez del postulado del paralelismo hiperbólico.



Sea P un punto del modelo y AB una recta que no pasa por él. AC es una paralela a AB (A no existe como punto en el modelo, pues no es interior a $\mathcal{C}$ como exige la interpretación) y BD es la otra, ya que separan las rectas secantes de las no secantes.

Para probar que todos los axiomas son proposiciones verdaderas es necesario utilizar inversión en el plano.



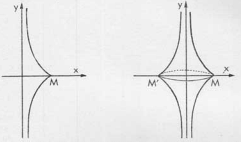
Si A es un punto interior al círculo $\mathcal{C}$ distinto del centro O, A' es su inverso con respecto a $\mathcal{C}$ si y sólo si $A' \in \overrightarrow{OA} \wedge OA \cdot OA' = r^2$, donde O es el centro de $\mathcal{C}$ y es llamado el centro de inversión y r es la potencia de dicha inversión. Se establece así una aplicación biyectiva entre los puntos interiores del círculo distintos del centro y sus respectivos inversos. Aplicando algunas propiedades de esta transformación en el plano puede probarse la totalidad de los axiomas hiperbólicos.

Si el círculo fundamental se reemplaza por una esfera, el modelo de Poincaré para geometría plana de Lobatchefsky puede extenderse a la misma en el espacio, con interpretaciones adecuadas.

Se obtienen también otros modelos para la geometría hiperbólica plana utilizando recursos de geometría diferencial. En efecto, Beltrami (1835-1900) demostró que cualquier superficie de curvatura [1] constante y negativa puede utilizarse como plano para la geometría hiperbólica. Un ejemplo lo constituye la geometría sobre la "pseudoesfera" o "tractoide".

Para definir esta superficie se considera la curva plana conocida con el nombre de "tractriz" [2], simétrica con respecto a uno de los ejes coordenados y que tiene al otro eje como asíntota.

La pseudoesfera se obtiene haciendo girar la tractriz alrededor de su asíntota como eje de rotación.



La pseudoesfera puede interpretarse como plano de Lobatchefsky limitado y las rectas hiperbólicas son las geodésicas de la superficie, o sea, las curvas de menor longitud que unen, sobre la superficie, dos puntos de la misma.

Un inconveniente de esta superficie es que presenta una curva singular, la circunferencia MM', pero Hilbert demostró que no existe en el espacio ordinario una superficie de curvatura negativa constante que no presente singularidades. Esto implica que en dichas superfi-

---

(1) Curvatura de Gauss o simplemente curvatura de una superficie en un punto P es el número $K = k \cdot k'$ donde k y k' son las curvaturas planas máxima y mínima en el punto P de las secciones con planos normales a la superficie. La curvatura plana es el recíproco del radio del círculo osculador y su fórmula diferencial

$$k = \frac{y''}{(1 + y'^2)^{3/2}}$$

La curvatura de Gauss de un plano o de una superficie desarrollable es nula.

(2) Si la asíntota es el eje de ordenadas, la ecuación del gráfico de la tractriz es:

$$y = k \cdot \log \frac{k + \sqrt{k^2 - x^2}}{x} - \sqrt{k^2 - x^2},$$

donde k es constante y la curvatura de la tractoide que engendra es $-\frac{1}{k^2}$

cies sólo pueden verificarse las propiedades de la geometría hiperbólica que corresponden a regiones acotadas del plano.

7. GEOMETRÍAS DE RIEMANN

1º) Geometría esférica

Como se ha visto anteriormente, la geometría elíptica acepta como postulado la no existencia de paralelas que corresponde a la hipótesis del ángulo obtuso en el cuadrilátero de Saccheri.

Algunas proposiciones de la geometría elíptica son válidas en la geometría esférica, o sea, en la geometría sobre una esfera y sus círculos máximos.

Por ejemplo:

1) La suma de los ángulos interiores de un triángulo es mayor que dos rectos (la medida de la diferencia entre ambos es el exceso esférico).
2) En todo triángulo, el exceso esférico es proporcional al área.
3) Dos triángulos son semejantes si y sólo si son congruentes (un triángulo queda determinado cuando se conocen sus tres ángulos).

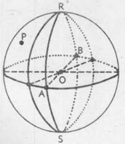
Un modelo sencillo para la geometría elíptica se puede obtener modificando someramente el primer postulado de Euclides. Se considera a la geometría esférica como una geometría no euclidiana donde no existen las paralelas.

El postulado I modificado es:

"Dos puntos distintos determinan **por lo menos** una recta."

Para hallar el modelo mencionado se puede interpretar **punto** como punto de una superficie esférica fundamental y **recta** como circunferencia máxima.

Es sencillo verificar en este modelo los cuatro postulados de Euclides con la modificación introducida al primero.



Con respecto al primer postulado, por propiedades de la geometría de Euclides, dos puntos de una superficie esférica determinan una circunferencia máxima. Esa circunferencia es única salvo que los dos puntos considerados sean extremos de un mismo diámetro, en cuyo caso determinan infinitas circunferencias máximas.

Para el segundo postulado, la circunferencia no tiene extremos aunque su longitud es finita. Además todas las "rectas" tienen la misma longitud.

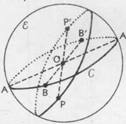
Los postulados III y IV son inmediatos.

En cuanto al postulado del paralelismo elíptico, no existen paralelas ya que cualquier par de "rectas" se cortan en dos puntos diametralmente opuestos (antipodales).

2º) Geometría elíptica

Si se quiere obtener un modelo para la geometría elíptica sin alterar el postulado I, es decir, donde dos puntos determinen una recta y solamente una, hay que modificar la interpretación de **punto** de la geometría esférica.

Para ello basta considerar como punto elíptico a todo par de puntos diametralmente opuestos en la superficie esférica que reciben el nombre de puntos antipodales o asociados.



Si P es un punto de la superficie esférica $\mathcal{E}$, $\overline{P}$ es el par (P ; P'), donde P' es el otro extremo del diámetro OP. Los puntos del plano elíptico son los puntos $\overline{P}$ de la superficie esférica $\mathcal{E}$.

Si C es una circunferencia máxima de la superficie esférica, la recta elíptica $\overline{C}$ es el conjunto de los puntos $\overline{P}$ para los cuales P pertenece a C.

Para interpretar congruencia debe considerarse como distancia entre dos puntos $\overline{A}$ y $\overline{B}$ la longitud del menor de los arcos comprendidos entre A (o A') y B(o B').

La idea de estudiar interpretaciones geométricas planas sobre superficies considerando como rectas a las geodésicas de las mismas, se debe a Riemann, y las geometrías esférica y elíptica reciben generalmente el nombre de geometrías de Riemann.

8. RESUMEN

El siguiente cuadro ofrece una síntesis de las principales diferencias existentes entre las tres geometrías consideradas.

Geometría	parabólica (Euclides)	hiperbólica (Lobatchefsky)	elíptica (Riemann)
cuadrilátero de Saccheri	áng. recto	áng. agudo	áng. obtuso
paralela	única	dos paralelas e infinitas no secantes	ninguna
longitud de la recta	infinita	infinita	finita
suma de ángulos de un triángulo	dos rectos	menor que dos rectos	mayor que dos rectos
triángulos semejantes de áreas diferentes	existen	no existen	no existen
rectángulos	existen	no existen	no existen
medida de segmentos	relativa	absoluta	absoluta
curvatura de Gauss constante y	nula	negativa	positiva
dos rectas perpendiculares a una tercera son	paralelas	no secantes	secantes

Analizando el cuadro anterior, queda latente una pregunta: ¿cuál de las tres geometrías corresponde al espacio físico?

La respuesta es desconocida. Si bien la geometría euclídea parece intuitivamente la única admisible, las geometrías no euclidianas responden mejor a ciertas teorías físicas. En un estudio reciente, por ejemplo, se llegó a la conclusión de que las propiedades del espacio óptico corresponden a la geometría de Lobatchefsky y éste es sólo uno entre muchos casos similares.

Queda entonces planteada la duda. Más aún, si el espacio no es euclídeo, este hecho quedaría comprobado si, al medir los ángulos interiores de un triángulo, la suma difiere de π y esa diferencia no es imputable a errores de medición. En cambio, si la suma es igual a dos rectos, nunca podrá comprobarse. Ninguna experiencia física puede asegurar esa precisión total.

CAPÍTULO XII

Geometria vectorial

1. DESARROLLO VECTORIAL DE LA GEOMETRÍA

El objeto principal de este capítulo es la introducción del método vectorial aplicado al desarrollo de la geometría. Tal desarrollo, por razones de espacio, no tiene la pretensión de ser completo, ni siquiera general, puesto que está restringido al espacio euclídeo tridimensional, aunque su extensión al espacio n-dimensional es natural y simple.

Con el estudio del espacio vectorial de las matrices columnas, y en función de las dos leyes de composición que lo caracterizan, se introduce la geometría en el plano afín a través de algunas propiedades elementales, desde el punto de vista vectorial.

A partir de la geometría afín y en función del producto escalar o interno, se define el concepto de distancia y de perpendicularidad, con el objeto de adjuntar una métrica en el plano euclídeo. Finalmente se proponen las demostraciones de algunas propiedades usuales de la geometría métrica.

2. ESPACIO VECTORIAL DE MATRICES COLUMNAS SOBRE EL CUERPO DE LOS REALES

Sean los intervalos naturales iniciales

$$I_3 = \{1, 2, 3\} \quad \text{e} \quad I_1 = \{1\}$$

Consideramos el producto cartesiano

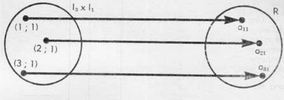
$$I_3 \times I_1 = \{(1\,;\,1), (2\,;\,1), (3\,;\,1)\}$$

Definición.

Matriz del tipo 3×1 **sobre el cuerpo** R **de los reales, es toda aplicación de** $I_3 \times I_1$ **en** R.

El dominio de las aplicaciones $f : I_3 \times I_1 \rightarrow R$, es $I_3 \times I_1$; el rango es R. Cualquier aplicación de este tipo queda determinada por los valores que toma sobre R, es decir, por el conjunto imagen. Convenimos en asignar como homólogo de cada elemento $(i ; j) \in I_3 \times I_1$, el número real a_{ij}.

Desde un punto de vista gráfico, se tiene:



Identificamos la aplicación o matriz f con el conjunto cuyos elementos son a_{11}, a_{21}, a_{31}, no necesariamente distintos. Por comodidad, para designar tal matriz se propone el símbolo:

$$A = \begin{pmatrix} a_{11} \\ a_{21} \\ a_{31} \end{pmatrix}$$

Sea M el conjunto de todas las matrices del tipo 3×1; cada una de ellas está caracterizada por una terna ordenada de números reales. Definimos en M la siguiente ley de composición interna, llamada adición de matrices:

$$\begin{pmatrix} a_{11} \\ a_{21} \\ a_{31} \end{pmatrix} + \begin{pmatrix} b_{11} \\ b_{21} \\ b_{31} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} \\ a_{21} + b_{21} \\ a_{31} + b_{31} \end{pmatrix}$$

Según se ha visto en el capítulo correspondiente a leyes de composición, se trata de una aplicación de $M \times M$ en M.

Definimos también una ley de composición externa, llamada producto escalar de un número real por una matriz:

$$k \cdot A = \begin{pmatrix} k \cdot a_{11} \\ k \cdot a_{21} \\ k \cdot a_{31} \end{pmatrix}$$

Esta ley externa es una aplicación de $R \times M$ en M.

Con estas definiciones, el conjunto M adquiere estructura de espacio vectorial sobre el cuerpo de los reales, ya que se verifican los axiomas que lo caracterizan. Por consiguiente, la cuaterna (M, R, +, ·) es un R– espacio vectorial.

Cada elemento de M, es decir, cualquier matriz 3×1 es un vector.

El vector nulo es $0 = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$

El vector opuesto del $\begin{pmatrix} x \\ y \\ z \end{pmatrix}$ es $\begin{pmatrix} -x \\ -y \\ -z \end{pmatrix}$

Una interpretación de este espacio es el conjunto de los vectores del espacio euclídeo tridimensional aplicados en el origen del sistema de referencia. Los números x, y, z se llaman coordenadas o componentes del vector. Análogamente, con las mismas definiciones, el conjunto de las matrices 2×1 es un espacio vectorial sobre el cuerpo de los reales; cada vector del plano euclídeo está representado por una matriz $\begin{pmatrix} x \\ y \end{pmatrix}$

3. DEPENDENCIA LINEAL DE VECTORES EN EL PLANO

Sabemos que dos vectores A y B son linealmente independientes, si y sólo si la única combinación lineal de los mismos que engendra al vector nulo es la trivial. Es decir

$$k_1 \cdot A + k_2 \cdot B = 0 \quad \text{sólo se verifica para } k_1 = k_2 = 0$$

Por otra parte, los vectores A y B son linealmente dependientes si y sólo si existen escalares no simultáneamente nulos, tales que se verifica la combinación lineal anterior. En este caso, uno de los vectores es un múltiplo del otro. En efecto:

Sean A y B linealmente dependientes; entonces por definición, existen escalares k_1 y k_2 tales que

$$k_1 \cdot A + k_2 \cdot B = 0 \quad \text{siendo } k_1^2 + k_2^2 \neq 0$$

Si $k_2 \neq 0$, se tiene:

$$B = -\frac{k_1}{k_2} \cdot A \quad \text{o sea } B = k \cdot A$$

El teorema recíproco también se verifica.

Interesa determinar una condición analítica de dependencia lineal. Sean entonces los vectores no nulos A y B, linealmente dependientes, es decir:

$$B = k \cdot A \quad \text{siendo } k \neq 0$$

Con la notación matricial se tiene

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = k \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} kx \\ ky \end{pmatrix}$$

Por definición de igualdad resulta: $\begin{cases} x' = kx \\ y' = ky \end{cases}$

relaciones que aseguran la anulación del determinante $\begin{vmatrix} x & x' \\ y & y' \end{vmatrix}$ por tener dos columnas proporcionales; cuando tenga sentido aritmético podrá escribirse $\dfrac{x}{x'} = \dfrac{y}{y'}$

Esta condición analítica es también suficiente, y por lo tanto valen las equivalencias:

A y B linealmente dependientes $\Leftrightarrow \dfrac{x}{x'} = \dfrac{y}{y'} \Leftrightarrow \begin{vmatrix} x & x' \\ y & y' \end{vmatrix} = 0$

A y B linealmente independientes $\Leftrightarrow \dfrac{x}{x'} \neq \dfrac{y}{y'} \Leftrightarrow \begin{vmatrix} x & x' \\ y & y' \end{vmatrix} \neq 0$

4. BASE CANÓNICA EN R^2

Sean los vectores del plano

$$I = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{y} \quad J = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Son linealmente independientes, puesto que el determinante

$\begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = 1 \neq 0$, de acuerdo con la condición analítica anterior. Para que el par o bivector I, J constituya una **base**, **además** de ser un conjunto linealmente independiente, debe verificarse **que** todo vector del plano puede expresarse como una combinación lineal de los mismos.

En efecto:

Sea un vector genérico $A = \begin{pmatrix} x \\ y \end{pmatrix}$

por definición de adición se tiene

$$A = \begin{pmatrix} x \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ y \end{pmatrix}$$

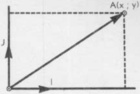
y por definición de producto por un escalar:

$$A = x \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + y \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Es decir:

$$A = x \cdot I + y \cdot J \quad (1)$$

La base I, J se llama **canónica,** y la forma (1) del vector A recibe el nombre de **descomposición canónica.**



5. CAMBIO DE BASE EN R^2

Demostramos la siguiente proposición:

Dos vectores linealmente independientes del plano constituyen una base.

Sean los vectores U y V linealmente independientes y en la forma canónica:

$$(1)\ \begin{cases} U = aI + bJ \\ V = a'I + b'J \end{cases}$$

Siendo, por hipótesis, un conjunto linealmente independiente, se verifica la condición

$$\Delta = \begin{vmatrix} a & a' \\ b & b' \end{vmatrix} \neq 0 \quad (2)$$

Para probar que todo vector del plano puede proponerse como combinación lineal de U y V, es preciso determinar I y J en función de aquéllos.

Resolvemos el sistema (1) respecto de I y J; se trata de un sistema crameriano con solución única de acuerdo con (2).

Así

$$\Delta I = \begin{vmatrix} U & b \\ V & b' \end{vmatrix} = b'U - bV$$

$$\Delta J = \begin{vmatrix} a & U \\ a' & V \end{vmatrix} = aV - a'U$$

Luego

$$I = \frac{b'U - bV}{\Delta}$$

$$J = \frac{aV - a'U}{\Delta}$$

O bien:

$$I = \frac{b'}{\Delta}U - \frac{b}{\Delta}V$$

$$J = -\frac{a'}{\Delta}U + \frac{a}{\Delta}V$$

Sintetizando la notación, resulta:

$$(3)\ \begin{cases} I = k_1U + k_2V \\ J = k_1'U + k_2'V \end{cases}$$

Sea ahora un vector genérico del plano en la forma canónica:

$$A = xI + yJ \qquad (4)$$

De (3) y (4) se tiene

$$A = x \cdot (k_1U + k_2V) + y \cdot (k_1'U + k_2')V$$

Es decir:

$$A = (x \cdot k_1 + y \cdot k_1')U + (x \cdot k_2 + y \cdot k_2')V$$

Esto prueba que el par U , V constituye una base por el solo hecho de ser vectores linealmente independientes. Llamando x', y' a las componentes de A respecto de la base U , V, resulta

$$A = x'U + y'V$$

Las fórmulas relativas al cambio de base son:

$$\begin{cases} x' = k_1 \cdot x + k_1' \cdot y \\ y' = k_2 \cdot x + k_2' \cdot y \end{cases}$$

siendo x e y las componentes de A según la base canónica, y además:

$$k_1 = \frac{b'}{\Delta}\ ;\ k_2 = -\frac{b}{\Delta}\ ;\ k_1' = -\frac{a'}{\Delta}\ ;\ k_2' = \frac{a}{\Delta}$$

Fórmulas en las que a , b , a' y b' son las componentes canónicas de los vectores U y V, linealmente independientes.

De acuerdo con lo que antecede, se puede probar fácilmente que las definiciones de adición de vectores y de producto de un escalar por un vector, así como también la dependencia e independencia lineal, son intrínsecas, es decir, independientes de la base elegida.

6. GEOMETRÍA EN EL PLANO AFÍN

Definición

Punto es todo par ordenado de números reales.

Definición

Plano afín propio R^2 es el conjunto de todos los pares ordenados de números reales.

Definición

Vector fijo $\overrightarrow{AB}$ es el par ordenado (A ; B), **de los puntos** A y B.

A es el origen del vector y B se llama extremo.

Definición

Dados dos puntos $A(x_1 ; y_1)$ **y** $B(x_2 ; y_2)$, **se llaman coordenadas o componentes canónicas del vector fijo** $\overrightarrow{AB}$, **a los números reales** $x_2 - x_1$ **e** $y_2 - y_1$.

Definición

Dos vectores fijos son equipolentes, si y sólo si tienen las mismas coordenadas o componentes.

La relación así definida satisface los axiomas: reflexivo, simétrico y transitivo; por consiguiente es de equivalencia. Queda determinada entonces una partición del conjunto de los vectores fijos del plano en clases de equivalencia, cada una de las cuales se llama vector libre.

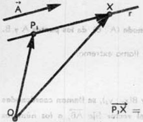
Definición

Vector libre del plano R^2 es toda clase de equivalencia determinada por la relación de equipolencia en el conjunto de los vectores fijos del plano.

En otras palabras: vector libre v, es el conjunto de todos los vectores equipolentes a $\vec{v}$. El conjunto cociente asociado a dicha relación es el conjunto de todos los vectores libres del plano. Podemos elegir como representante de cada clase de equivalencia, al vector aplicado en el origen del sistema de referencia (en tal caso denotamos cada vector por la letra correspondiente al extremo) y de este modo, el conjunto de los vectores libres del plano se puede identificar con el conjunto M de las matrices 2×1. En consecuencia, tal conjunto de vectores libres adquiere estructura de espacio vectorial sobre el cuerpo de los números reales.

La recta en el plano

Sean el punto P_1 y el vector libre (no nulo) $\vec{A} = pI + qJ$. El par $(P_1\,;\,\vec{A})$ define unívocamente a la recta r. En efecto



$\forall X \in r$ se tiene:

$$\vec{X} = \vec{P}_1 + \overrightarrow{P_1X} \quad (1)$$

El vector libre $\vec{A}$ puede considerarse sobre la recta r.

Como $\overrightarrow{P_1X}$ y $\vec{A}$ son linealmente dependientes, se verifica:

$$\overrightarrow{P_1X} = t\cdot\vec{A} \quad (2)$$

siendo t un número real.

De (1) y (2) resulta:

$$\vec{X} = \vec{P}_1 + t\cdot\vec{A} \quad (3)$$

La relación (3) es la **ecuación vectorial paramétrica de la recta** determinada por un punto y una dirección. Para todo $t \in R$, resulta $X \in r$.

El vector $\vec{A}$ se llama vector director de la recta, y $\{t\cdot\vec{A}\}$ es el conjunto de los vectores directores de r.

En particular: cuando $t = 0$, X se identifica con P_1.

Expresando (3) mediante la descomposición canónica, podemos obtener las ecuaciones cartesianas paramétricas de la recta. En efecto, sean:

$$\vec{X} = xI + yJ$$
$$\vec{P}_1 = x_1I + y_1J$$
$$\vec{A} = pI + qJ$$

se tiene así:

$$xI + yJ = x_1I + y_1J + t\cdot(pI + qJ)$$

asociando respecto de I y J

$$xI + yJ = (x_1 + tp)I + (y_1 + tq)J$$

y por definición de igualdad de vectores:

$$(4)\ \begin{cases} x = x_1 + tp \\ y = y_1 + tq \end{cases}$$

Las relaciones (4), constituyen las **ecuaciones cartesianas paramétricas de la recta.**

Eliminando t entre ambas, resulta

$$\frac{x - x_0}{p} = \frac{y - y_1}{q}$$

que es la **ecuación cartesiana de la recta determinada por un punto y una dirección.**

Segmento orientado

Sean los puntos distintos A y B. La ecuación vectorial de la recta que determinan es:

$$\vec{X} = \vec{A} + t \cdot \overrightarrow{AB}$$

Si $t = 0$ entonces $\vec{X}$ se identifica con A

Para $t = 1$ se obtiene el punto B

Definición

Segmento orientado $\overrightarrow{AB}$ es el conjunto de los puntos de la recta que se obtienen para todo t perteneciente al intervalo cerrado $[0 ; 1]$.

Rectas paralelas

Definición

Dos rectas son paralelas si y sólo si admiten el mismo conjunto de vectores directores.

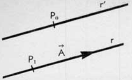
Sean r y r', cuyos conjuntos de vectores directores son, respectivamente C y C'. Entonces:

$$r \parallel r' \Leftrightarrow C = C'$$

La relación de paralelismo así definida es reflexiva, simétrica y transitiva. Cada clase de equivalencia asociada recibe el nombre de dirección, o punto impropio, el cual queda representado eventualmente por un vector del plano.

Se verifica el postulado V de Euclides. En efecto:

Sean el punto P_0 y la recta cuya ecuación es



$\vec{X} = \vec{P_1} + t \cdot \vec{A}$, tales que $P_0 \notin r$.

Consideramos ahora la recta que pasa por P_0 y cuya dirección es la de $\vec{A}$:

$$r' \to \vec{X} = \vec{P_0} + t \cdot \vec{A}$$

Resulta $r' \parallel r$, pues ambas admiten el mismo conjunto de vectores directores. Además r' es único pues está determinada por un punto P_0 y el vector $\vec{A}$.

Definición

Plano afín es la unión de R^2 y el conjunto de todas las direcciones.

Nota: Aunque no es el propósito de este capítulo, aclaramos que con las nociones dadas y definiciones convenientes, pueden estudiarse las transformaciones usuales de la geometría afín desde un punto de vista analítico vectorial.

7. GEOMETRÍA MÉTRICA EUCLIDIANA EN EL PLANO

Interesa introducir una métrica en el plano, para lo cual es necesario llegar a los conceptos de distancia entre pares de puntos, y de perpendicularidad.

Definición

Producto escalar o interno en el espacio vectorial V, es toda aplicación de $V \times V$ en R, tal que a cada par de vectores: $\vec{A} = xI + yJ$ y $\vec{A'} = x'I + y'J$, le hace corresponder el número real $xx' + yy'$.

La notación que utilizaremos es:

$$\vec{A} \cdot \vec{A'} = xx' + yy'$$

Es decir: el producto escalar de dos vectores es la suma de los productos de las componentes homónimas.

Propiedades del producto escalar

Con la definición dada de producto interno, es posible demostrar las siguientes proposiciones:

a) **El producto escalar es conmutativo.**

En efecto

$$\vec{A} \cdot \vec{A'} = xx' + yy' = x'x + y'y = \vec{A'} \cdot \vec{A}$$

b) **El producto escalar es distributivo respecto de la suma de vectores.**

$$\vec{A} \cdot (\vec{B} + \vec{C}) = \vec{A} \cdot \vec{B} + \vec{A} \cdot \vec{C}$$

c) **Es asociativo respecto de la ley externa.**

$$\forall k \in R \text{ es}: (k\vec{A}) \cdot \vec{B} = k(\vec{A} \cdot \vec{B}) = \vec{A} \cdot (k\vec{B})$$

d) **El producto escalar de un vector por sí mismo, es decir, su cuadrado, es no negativo.**

$\forall \vec{A}$, se tiene:

$$\vec{A}^2 = \vec{A} \cdot \vec{A} = x^2 + y^2 \geqslant 0$$

e) **El cuadrado de un vector es cero si y sólo si es el vector nulo.**

$$\vec{A}^2 = 0 \Longleftrightarrow \vec{A} = \vec{0}$$

f) **Productos notables.**

$$(\vec{A} \pm \vec{B})^2 = \vec{A}^2 + \vec{B}^2 \pm 2\,\vec{A} \cdot \vec{B}$$

$$(\vec{A} + \vec{B}) \cdot (\vec{A} - \vec{B}) = \vec{A}^2 - \vec{B}^2$$

Norma y módulo de un vector

a) **Definición: Norma de un vector $\vec{A}$ es el producto escalar de dicho vector por sí mismo.**

$$N(\vec{A}) = \vec{A} \cdot \vec{A} = \vec{A}^2$$

Resulta entonces $N(\vec{A}) = x^2 + y^2$

b) **Definición: Módulo o longitud de un vector es la raíz cuadrada no negativa de su norma.**

$$|\vec{A}| = +\sqrt{N(\vec{A})} = +\sqrt{\vec{A}^2} = +\sqrt{x^2 + y^2}$$

c) **El módulo del producto de un escalar por un vector es igual al módulo del escalar por el módulo del vector.**

En efecto:

$$|\lambda \cdot \vec{A}| = |\sqrt{(\lambda \cdot \vec{A})^2}| = |\sqrt{\lambda^2 \cdot \vec{A}^2}| = |\lambda| \cdot |\vec{A}|$$

d) **El módulo de todo vector es no negativo. Es cero si y sólo si el vector es nulo.**

En símbolos

$$|\vec{A}| \geqslant 0 \wedge (|\vec{A}| = 0 \Leftrightarrow \vec{A} = \vec{0})$$

La demostración es simple y queda a cargo del lector.

Desigualdad de Schwarz

El módulo de un producto escalar es menor o igual que el producto de los módulos.

Se trata de probar que

$$|\vec{A} \cdot \vec{B}| \leqslant |\vec{A}| \cdot |\vec{B}|$$

Partimos de la identidad de Lagrange:

$$(x^2 + y^2)(x'^2 + y'^2) - (xx' + yy')^2 = (xy' - x'y)^2 \quad (1)$$

la que se verifica desarrollando las operaciones.

De (1) resulta:

$$(x^2 + y^2)(x'^2 + y'^2) - (xx' + yy')^2 \geqslant 0 \quad (2)$$

Expresamos la (2) en términos de producto escalar:

$$|\vec{A}|^2 \cdot |\vec{B}|^2 - |\vec{A} \cdot \vec{B}|^2 \geqslant 0 \Rightarrow$$

$$\Rightarrow |\vec{A}|^2 \cdot |\vec{B}|^2 \geqslant |\vec{A} \cdot \vec{B}|^2$$

y como las bases son no negativas

$$|\vec{A}| \cdot |\vec{B}| \geqslant |\vec{A} \cdot \vec{B}| \Rightarrow$$

$$\Rightarrow |\vec{A} \cdot \vec{B}| \leqslant |\vec{A}| \cdot |\vec{B}|$$

La igualdad se cumple cuando el segundo miembro de (1) vale cero, y en tal caso los vectores son linealmente dependientes

Módulo de la suma

El módulo de la suma de dos vectores es menor o igual que la suma de los módulos.

Por la desigualdad de Schwarz, sabemos que:

$$|\vec{A} \cdot \vec{B}| \leqslant |\vec{A}| \cdot |\vec{B}|$$

por propiedad de los módulos de números reales:

$$-|\vec{A}| \cdot |\vec{B}| \leqslant \vec{A} \cdot \vec{B} \leqslant |\vec{A}| \cdot |\vec{B}|$$

Teniendo en cuenta la última desigualdad, vale la relación

$$2 \cdot \vec{A} \cdot \vec{B} \leqslant 2 \cdot |\vec{A}| \cdot |\vec{B}| \qquad (1)$$

Efectuemos ahora el cuadrado del módulo de la suma, que se identifica con su cuadrado:

$$|\vec{A} + \vec{B}|^2 = (\vec{A} + \vec{B})^2 = \vec{A}^2 + \vec{B}^2 + 2\vec{A} \cdot \vec{B}$$

Y teniendo en cuenta la misma identificación del cuadrado de un vector con el cuadrado de su módulo, tenemos

$$|\vec{A} + \vec{B}|^2 = |\vec{A}|^2 + |\vec{B}|^2 + 2\vec{A} \cdot \vec{B} \qquad (2)$$

Sumando (1) y (2), luego de cancelar, nos queda:

$$|\vec{A} + \vec{B}|^2 \leqslant |\vec{A}|^2 + |\vec{B}|^2 + 2|\vec{A}| \cdot |\vec{B}|$$

Es decir:

$$|\vec{A} + \vec{B}|^2 \leqslant (|\vec{A}| + |\vec{B}|)^2$$

Lo cual implica

$$|\vec{A} + \vec{B}| \leqslant |\vec{A}| + |\vec{B}|$$

Distancia y congruencia de segmentos

Definición

Distancia entre dos puntos A y B es el módulo del vector $\overrightarrow{AB}$.

Notación:

$$d(AB) = |\overrightarrow{AB}| = |B - A| = +\sqrt{(x' - x)^2 + (y' - y)^2}$$

Se demuestra que esta definición satisface las propiedades que caracterizan a todo espacio métrico, es decir:

a) La distancia es positiva o nula

$$d(AB) \geqslant 0$$

b) Es simétrica

$$d(AB) = d(BA)$$

c) Vale la propiedad triangular

$$d(AB) + d(BC) \geqslant d(AC)$$

Definición

Dos segmentos AB **y** CD **son congruentes si y sólo si**

$$d(AB) = d(CD)$$

$$AB = CD \Leftrightarrow d(AB) = d(CD)$$

Vectores ortogonales y bases ortonormales

Definición

Dos vectores no nulos son ortogonales, si y sólo si su producto escalar es cero.

$$\vec{A} \perp \vec{B} \Leftrightarrow \vec{A} \cdot \vec{B} = 0$$

Resulta entonces que la condición analítica de ortogonalidad es la anulación de la suma de los productos de sus componentes homónimas, es decir:

$$\vec{A} \perp \vec{B} \Leftrightarrow xx' + yy' = 0$$

Definición

Una base es ortonormal si y sólo si los vectores que la constituyen tienen módulo 1 y son ortogonales.

$$(U\,;\,V) \text{ es base ortonormal} \Leftrightarrow |\vec{U}| = |\vec{V}| = 1 \wedge \vec{U} \cdot \vec{V} = 0$$

Corolario

Los vectores de la base canónica constituyen un sistema ortonormal.

Propiedad

El producto escalar, y en consecuencia la distancia entre pares de puntos y la ortogonalidad, son intrínsecos, es decir, independientes de la base ortonormal elegida.

Sean los vectores
$$\vec{A} = xI + yJ$$
$$\vec{B} = x'I + y'J$$

respecto de la base ortonormal (I , J), se tiene:

$$(xI + yJ)\,(x'I + y'J) = xx' + yy' \qquad (1)$$

Consideremos ahora la descomposición de los mismos vectores respecto de otra base ortonormal (U , V):

$$\vec{A} = aU + bV$$
$$\vec{B} = a'U + b'V$$

Por definición del producto escalar, se tiene:

$$(aU + bV) \cdot (a'U + b'V) = aa' + bb' \qquad (2)$$

Al ser las bases ortonormales, se demuestra la igualdad numérica de (1) y (2) y en consecuencia la conservación del producto escalar.

Teorema de Pitágoras

Sea $\overset{\triangle}{ABC}$ rectángulo en A.

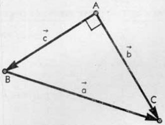
Por suma de vectores, es

$$\overrightarrow{AC} = \overrightarrow{AB} + \overrightarrow{BC}$$

Luego

$$\overrightarrow{BC} = \overrightarrow{AC} - \overrightarrow{AB} \Rightarrow$$

$$\Rightarrow \overrightarrow{BC}^2 = (\overrightarrow{AC} - \overrightarrow{AB})^2$$



En consecuencia

$$\overrightarrow{BC}^2 = \overrightarrow{AC}^2 + \overrightarrow{AB}^2 - 2\,\overrightarrow{AC} \cdot \overrightarrow{AB}$$

El doble producto es cero pues $\overrightarrow{AC}$ y $\overrightarrow{AB}$ son ortogonales.

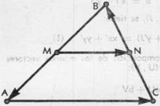
Resulta entonces

$$|\overrightarrow{BC}|^2 = |\overrightarrow{AC}|^2 + |\overrightarrow{AB}|^2$$

Es decir

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

Base media del triángulo



Para probar que $\overrightarrow{MN}$ es paralela a la base $\overline{AC}$ e igual a su mitad, basta demostrar que

$$\overrightarrow{MN} = \frac{1}{2}\overrightarrow{AC}$$

Por suma de vectores, es

$$\overrightarrow{MN} = \overrightarrow{MA} + \overrightarrow{AC} + \overrightarrow{CN} \quad (1)$$

Siendo M y N puntos medios de BA y CB, podemos escribir

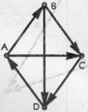
$$\overrightarrow{MN} = \frac{1}{2}\overrightarrow{BA} + \overrightarrow{AC} + \frac{1}{2}\overrightarrow{CB} = \overrightarrow{AC} + \frac{1}{2}(\overrightarrow{CB} + \overrightarrow{BA})$$

$$\overrightarrow{MN} = \overrightarrow{AC} + \frac{1}{2}\overrightarrow{CA} \text{ por adición de vectores}$$

$$\overrightarrow{MN} = \overrightarrow{AC} - \frac{1}{2}\overrightarrow{AC}$$

$$\overrightarrow{MN} = \frac{1}{2}\overrightarrow{AC} \qquad \text{como queríamos.}$$

Las diagonales de un rombo son perpendiculares



Siendo ABCD un rombo, se tiene:

$$|\overrightarrow{AB}| = |\overrightarrow{BC}|$$

y

$$\overrightarrow{CD} = -\overrightarrow{AB}$$

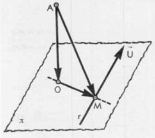
Para probar el teorema, analizamos el producto escalar:

$$\overrightarrow{AC} \cdot \overrightarrow{BD} = (\overrightarrow{AB} + \overrightarrow{BC}) \cdot (\overrightarrow{BC} + \overrightarrow{CD}) =$$

$$= (\overrightarrow{BC} + \overrightarrow{AB}) \cdot (\overrightarrow{BC} - \overrightarrow{AB}) = \overrightarrow{BC}^2 - \overrightarrow{AB}^2 = |\overrightarrow{BC}|^2 - |\overrightarrow{AB}|^2 = 0$$

la anulación del producto escalar prueba la perpendicularidad de las diagonales $\overrightarrow{AC}$ y $\overrightarrow{BD}$.

Teorema de las tres perpendiculares



Sean $AO \perp \pi$, $OM \cup \pi$, $OM \perp r$ y $\vec{U}$ un vector director de $r \subset \pi$. En estas condiciones, debemos probar que $r \perp AM$.
Para ello, consideramos el producto escalar:

$$\overrightarrow{AM} \cdot \vec{U} = (\overrightarrow{AO} + \overrightarrow{OM}) \cdot \vec{U} = \overrightarrow{AO} \cdot \vec{U} + \overrightarrow{OM} \cdot \vec{U} = 0$$

por hipótesis.
Resulta:

$$\overrightarrow{AM} \perp \vec{U} \Rightarrow AM \perp r$$

Ángulo de dos vectores no nulos

Según la desigualdad de Schwarz, es

$$|\vec{X} \cdot \vec{Y}| \leqslant |\vec{X}| \cdot |\vec{Y}|$$

O sea

$$-|\vec{X}| \cdot |\vec{Y}| \leqslant \vec{X} \cdot \vec{Y} \leqslant |\vec{X}| \cdot |\vec{Y}|$$

Luego

$$-1 \leqslant \frac{\vec{X} \cdot \vec{Y}}{|\vec{X}| \cdot |\vec{Y}|} \leqslant 1$$

La doble acotación de la fracción nos permite definir como ángulo Θ de los vectores X e Y, a aquél que cumple las siguientes condiciones:

1º) $$0 \leqslant \Theta \leqslant \pi$$

2º) $$\cos \Theta = \frac{\vec{X} \cdot \vec{Y}}{|\vec{X}| \cdot |\vec{Y}|}$$

Resulta entonces, la siguiente expresión para el producto escalar:

$$\vec{X} \cdot \vec{Y} = |\vec{X}| \cdot |\vec{Y}| \cdot \cos \Theta$$

APÉNDICE

CAPITULO XIII

Polinomios

Los polinomios en x cuyos coeficientes son números reales, tienen extraordinaria importancia en álgebra elemental.

Generalmente se llaman polinomios en una variable. En realidad, el nombre de variable debe reservarse para el caso de la función polinómica y los polinomios en x se designan como polinomios en una indeterminada, donde x es la indeterminada o sea, simplemente, una letra cualquiera o símbolo que se utiliza de manera exclusivamente formal.

Tradicionalmente, la expresión siguiente representa un polinomio en la indeterminada x, con coeficientes pertenecientes al cuerpo de los números reales:

$$p(x) = 4x^0 + 3x^1 + 0x^2 + \sqrt{2}x^3 \quad (1)$$

Esta expresión puede interpretarse correctamente para definir un polinomio si se tiene en cuenta que los signos + no representan necesariamente una suma y pueden ser reemplazados por otros símbolos cualesquiera. Además $x^0, x^1, \ldots, x^n, \ldots$ pueden no indicar potencias de x sino los lugares que los coeficientes ocupan en una sucesión infinita de enteros no negativos: $0, 1, 2, 3, \ldots, n, \ldots$

Es decir, el polinomio p(x) puede indicarse de cualquiera de las formas siguientes:

$$p(x) = (4x^0 ; 3x^1 ; 0x^2 ; \sqrt{2}x^3)$$

$$p(x) = (4x_0 ; 3x_1 ; 0x_2 ; \sqrt{2}x_3)$$

$$p = (4 \; ; \; 3 \; ; \; 0 \; ; \; \sqrt{2})$$

La notación (1) es la más utilizada y puede demostrarse que las operaciones indicadas con los símbolos de adición, multiplicación y potenciación corresponden efectivamente a dichas operaciones.

Teniendo en cuenta los conceptos anteriores, se puede dar la siguiente definición formal de polinomio en una indeterminada sobre un cuerpo.

Definición

Si A es un cuerpo, se llama polinomio en una indeterminada sobre A, a toda sucesión de elementos de A cuyos términos son nulos a partir de un índice de la sucesión en adelante.

Es decir,

si $a = (a_0, a_1, a_2, \dots, a_n, 0, 0 \dots) \wedge a_i \in A$ para $i = 0, 1, \dots, n, \dots,$

entonces a es polinomio en una indeterminada sobre A.

Así como en la expresión anterior se definió polinomio sobre un cuerpo, el conjunto A puede ser otra estructura cualquiera con dos operaciones, como anillo, anillo conmutativo, dominio de integridad, etcétera.

El mayor de los índices de la sucesión que corresponde a un elemento no nulo de A se llama **grado** del polinomio. En el ejemplo anterior, el grado del polinomio es n y se indica gr. $a = n$.

Los términos a_i se llaman **coeficientes** del polinomio y el coeficiente a_0 es el **término independiente o constante.** Si existe un solo coeficiente que no es nulo, el polinomio recibe el nombre especial de **monomio.**

Ejemplo:

$$m = (0, 0, \dots, a_h, 0, 0 \dots)$$

O sea, si $a_h \neq 0 \wedge a_i = 0 \ \forall i \neq h$, entonces m es un monomio.

Si todos los coeficientes son nulos o sea neutros para la adición definida en A, entonces el polinomio se llama polinomio idénticamente nulo o **polinomio nulo** y se conviene que dicho polinomio **no tiene grado.** Se lo designa directamente con el símbolo "0" y gr. 0 no existe.

1. ESPACIO VECTORIAL DE POLINOMIOS

Igualdad de polinomios

Sean a y b dos polinomios en una indeterminada sobre el mismo cuerpo C.

$a = (a_0, a_1, a_2, \dots, a_n, 0, 0, \dots)$ $b = (b_0, b_1, \dots, b_n, 0, 0, \dots)$

 La igualdad de polinomios es la relación de identidad. Es decir, dos polinomios son iguales si y sólo si sus coeficientes son iguales.

$$a = b \Leftrightarrow \forall i : a_i = b_i$$

Consecuencia: si $a = b$, entonces gr. $a =$ gr. b

Adición de polinomios

Si C es el cuerpo sobre el cual se ha definido un conjunto de polinomios, este conjunto de polinomios se designa C(x). En C(x) pueden establecerse leyes de composición internas o externas con operadores de otro conjunto.

Definiremos la adición como primera ley de composición interna entre polinomios:

Definición

Dados dos polinomios a **y** b **sobre C se llama suma de los mismos al polinomio** c **cuyos coeficientes se obtienen de la siguiente manera :** $\forall i : c_i = a_i + b_i$

O sea,

$$a = (a_0, a_1, \ldots, a_i, \ldots a_m, 0, \ldots)$$

$$b = (b_0, b_1, \ldots, b_i, \ldots, b_n, 0, \ldots)$$

$$c = a + b = (a_0 + b_0, a_1 + b_1, \ldots, a_i + b_i, \ldots, 0 + b_n, 0, \ldots)$$

Puede demostrarse fácilmente que la operación así definida es conmutativa y asociativa y que el elemento neutro es el polinomio nulo.

Cada polinomio tiene además, respecto de la adición, un elemento simétrico u opuesto.

En efecto, el polinomio a, admite como opuesto el polinomio

$$-a = (-a_0, -a_1, -a_2, \ldots, -a_m, 0, \ldots).$$

Por lo tanto, respecto de la adición, el conjunto C(x) de polinomios sobre el cuerpo C tiene estructura de grupo conmutativo.

Si C es solamente un anillo, en lugar de un cuerpo, las demostraciones indicadas también son válidas.

Para el grado del polinomio suma son válidas las siguientes consideraciones:

1º) si gr. $a >$ gr. b, entonces gr. $(a + b) =$ gr. a

2º) si gr. $a =$ gr. $b \wedge a + b \neq 0$,

$$\text{entonces} \begin{cases} a_n + b_n \neq 0 \Rightarrow \text{gr. } (a + b) = \text{gr. } a \\ a_n + b_n = 0 \Rightarrow \text{gr. } (a + b) < \text{gr. } a \end{cases}$$

En ambos casos, gr. $(a + b) \leqslant$ máximo [gr. a, gr. b]

Multiplicación por elementos de C

Definición

Si a **es un polinomio sobre** C **y** $\alpha \in$ C, **entonces**

$$\alpha a = (\alpha a_0 , \alpha a_1 , \ldots , \alpha a_n , \ldots)$$

Es decir, el producto αa es el polinomio cuyos coeficientes se obtienen multiplicando el elemento α de C por cada coeficiente de a.

Puede demostrarse en forma sencilla que si α y β son elementos de C, entonces:

$$\alpha(a + b) = \alpha a + \alpha b$$

$$(\alpha + \beta)a = \alpha a + \beta a$$

$$\alpha(\beta a) = (\alpha\beta)a$$

$$1\, a = a$$

Por lo tanto, esta multiplicación escalar de un polinomio por un elemento del cuerpo C, considerada como ley externa en el conjunto C(x) con operadores en C, y la adición de polinomios como ley interna en el conjunto C(x), confieren al conjunto de polinomios C(x) estructura de **espacio vectorial** sobre el cuerpo C de los coeficientes.

Si se consideran, en especial, los siguientes polinomios de C(x):

$$x_0 = (1 , 0 , 0 , \ldots\ldots)$$
$$x_1 = (0 , 1 , 0 , \ldots\ldots)$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$x_n = (0 , 0 , \ldots , 1 , \ldots)$$

donde los coeficientes son todos nulos menos el correspondiente al índice de x, que es la unidad del conjunto C, resulta que x_0 tiene grado 0, x_1 grado 1, x_2 grado 2, ..., x_n grado n, etc.

Todo polinomio $a = (a_0 , a_1 , a_2 , \ldots , a_n , 0 , 0 , \ldots)$ puede considerarse como suma de productos de escalares por monomios, es decir:

$$x_0 = (1 , 0 , 0 , \ldots\ldots)$$
$$a_0x_0 = (a_0 , 0 , 0 , \ldots\ldots)$$
$$x_1 = (0 , 1 , 0 , \ldots\ldots)$$
$$a_1x_1 = (0 , a_1 , 0 , \ldots\ldots)$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$x_n = (0 , 0 , \ldots , 1 , 0 , \ldots)$$
$$a_nx_n = (0 , 0 , \ldots , a_n , 0 , \ldots)$$

y por definición de adición de polinomios:

$$a_0x_0 + a_1x_1 + a_2x_2 + \dots\dots + a_nx_n = (a_0, a_1, a_2, \dots, a_n, \dots)$$

O sea,

$$a = a_0x_0 + a_1x_1 + \dots + a_nx_n$$

Por convención, x_n puede designarse x^n, entendiendo que, hasta ahora, x^n es un símbolo donde x y n no pueden separarse.

Para poner en evidencia el simbolismo con que se designa a la indeterminada, el polinomio suele indicarse:

$a(x) = a_0x^0 + a_1x^1 + \dots + a_nx^n$, como se señaló al comienzo del capítulo.

2. PRODUCTO DE POLINOMIOS

Definición

Si a y b son dos polinomios sobre C, se llama producto de los mismos al polinomio c cuyos coeficientes se obtienen de la siguiente manera:

$$\forall i : c_i = a_0b_i + a_1b_{i-1} + a_2b_{i-2} + \dots + a_ib_0$$

O sea el coeficiente de x^i en c es la suma de todos los productos posibles de la forma a_sb_r donde $s + r = i$

$$\begin{aligned} \text{Si } a(x) &= a_0x^0 + a_1x^1 + \dots + a_mx^m \\ b(x) &= b_0x^0 + b_1x^1 + \dots + b_nx^n, \\ \text{entonces } c(x) = a(x)b(x) &= (a_0b_0)x^0 + (a_0b_1 + a_1b_0)x^1 + \dots + \\ &+ (a_0b_i + a_1b_{i-1} + \dots + a_ib_0)x^i + \dots \\ &+ (a_mb_n)x^{m+n} \end{aligned}$$

3. ANILLO DE POLINOMIOS

Sea A(x) el conjunto de polinomios en x sobre el anillo conmutativo y unitario A. Si en A(x) se definen adición y multiplicación entre polinomios de acuerdo con las indicaciones anteriores, se verifican varias propiedades interesantes. Daremos una idea sobre la demostración de algunas de ellas.

Teorema 1

Si A es un anillo conmutativo y unitario, entonces el conjunto A(x) de polinomios sobre A es también anillo conmutativo y unitario.

Ya se ha indicado que $A(x)$ es un grupo conmutativo con respecto a la adición. De la misma forma elemental, basándose en las propiedades del anillo A, puede probarse que la multiplicación de polinomios es conmutativa, asociativa y distributiva respecto de la adición. Además, si 1 es la unidad para la multiplicación en A, el polinomio $1\,x^0$ es la unidad para la multiplicación en $A(x)$.

O sea, $A(x)$ es un anillo conmutativo y unitario.

Teorema 2

El anillo $A(x)$ de polinomios sobre A contiene un subanillo isomorfo con A respecto de la adición y multiplicación.

Para establecer el isomorfismo, se considera el conjunto $A' \subset A(x)$ formado por los elementos de $A(x)$ del tipo $ax^0 \,/\, a \in A$.

La aplicación $ax^0 \longleftrightarrow a$ es un isomorfismo entre A' y A que "preserva" sumas y productos.

En efecto,

$$ax^0 + bx^0 = (a+b)x^0 \longleftrightarrow a+b$$
$$ax^0 \cdot bx^0 = (a \cdot b)x^0 \longleftrightarrow a \cdot b$$

Este isomorfismo autoriza a identificar al polinomio ax^0 con el elemento a de A y, en especial, al polinomio $1\,x^0$ con el elemento 1 de A.

Mas aun, de acuerdo con consideraciones anteriores, el polinomio $1\,x^1$ puede identificarse con la indeterminada x; el producto de los polinomios $1\,x^1 \cdot 1\,x^1$ con x^2, y en general, la indeterminada x^i es la potencia de exponente i de x.

Teorema 3

Si A es un dominio de integridad, y $a(x)$ y $b(x)$ son polinomios no nulos de $A(x)$, entonces $\text{gr.}\,[a(x) \cdot b(x)] = \text{gr.}\,a(x) + \text{gr.}\,b(x)$.

Como $a(x)$ y $b(x)$ no son idénticamente nulos, los dos tienen grado.

$$\text{Sea gr. } a(x) = m \Rightarrow a_m \neq 0$$
$$\text{y gr. } b(x) = n \Rightarrow b_n \neq 0$$

Por la definición de multiplicación de polinomios, el mayor grado posible del producto es $m+n$ y además $\text{gr.}\,[a(x) \cdot b(x)] \leqslant \text{gr.}\,a(x) + \text{gr.}\,b(x)$.

Como $a_m \neq 0 \wedge b_n \neq 0 \wedge$ A es dominio de integridad

$$a_m \cdot b_n \neq 0 \Rightarrow \text{gr.}\,[a(x) \cdot b(x)] = m+n$$

Esta propiedad tan familiar al producto tradicional de polinomios, según la cual el grado del producto es la suma de los grados de los factores, no es válida si A no es dominio.

Por ejemplo, sea A el anillo de enteros módulo 6 y $a(x)$ y $b(x)$ dos polinomios sobre A.

(El anillo de enteros módulo 6 es el formado por el conjunto $\{0, 1, 2, 3, 4, 5\}$ y las dos operaciones adición y multiplicación módulo 6. Por ejemplo, $5 + 3 = 8 \equiv 2_{(6}$; $3 \cdot 5 = 15 \equiv 3_{(6)}$)

$$\begin{aligned} a(x) &= 2 + 3x^5 \\ b(x) &= 5x + 2x^2 \\ a(x) \cdot b(x) &= 4x + 4x^2 + 3x^6 + 0x^7 \end{aligned}$$

En este caso, $gr.\,[a(x) \cdot b(x)] < gr.\,a(x) + gr.\,b(x)$

En efecto,

$$\begin{aligned} gr.\,a(x) &= 5\,; m = 5\,; a_m = 3 \\ gr.\,b(x) &= 2\,; n = 2\,; b_n = 2 \\ a_m \cdot b_n &= 3 \cdot 2 \equiv 0_{(6} \\ gr.\,a(x) + gr.\,b(x) &= 5 + 2 = 7 \\ gr.\,[a(x) \cdot b(x)] &= 6 \end{aligned}$$

4. EL PROCESO DE SUSTITUCIÓN

Si $a(x) = a_0 + a_1x + a_2x^2 + \ldots\ldots + a_nx^n$ es un polinomio en x sobre A y $s \in A$, se define

$$a(s) = a_0 + a_1s + a_2s^2 + \ldots\ldots + a_ns^n$$

Por lo tanto, $a(s) \in A$ está asociado con el elemento $a(x) \in A(x)$ y el elemento $s \in A$.

Puede establecerse la siguiente aplicación:

$$\forall s \in A : a(x) \rightarrow a(s)$$

y puede probarse que: $a(x) + b(x) \rightarrow a(s) + b(s)$

$$a(x) \cdot b(x) \rightarrow a(s) \cdot b(s)$$

Esta aplicación es entonces un homomorfismo entre A(x) y A. Como, de acuerdo con el teorema 2, $A \subset A(x)$, se trata de un endomorfismo.

La aplicación definida es una aplicación de A(x) **sobre** A, ya que cada elemento a de A es imagen del elemento ax^0 de A(x), pero no es inyectiva, pues es inmediata la verificación de que polinomios distintos pueden tener la misma imagen.

Ejemplo, sobre el anillo de los enteros, si $s = 2 \wedge a(x) = 32 \wedge b(x) = x^5$ $a(x) \neq b(x) \wedge a(s) = b(s)$.

Por lo tanto, el homomorfismo definido no es un isomorfismo.

Para finalizar esta introducción a la teoría de polinomios, daremos la siguiente definición, que marca un comienzo para el estudio de la tradicional teoría de ecuaciones.

Definición

Si $a(x) \in A(x)$ y $\alpha \in A$ / $a(\alpha) = 0$, **entonces** α **es una raíz del polinomio** $a(x)$.

Obsérvese que en la expresión $a(\alpha) = 0$, el segundo miembro es el elemento nulo de A. En cambio, si se habla tradicionalmente de resolver la ecuación $a(x) = 0$, en esta expresión "0" es el polinomio idénticamente nulo.

Si A es un cuerpo, entonces un polinomio de grado n tiene **a lo sumo** n raíces distintas en A. Si A no se restringe a un cuerpo, un polinomio de grado n puede tener más de n raíces.

Ejemplo

Sea A el anillo de enteros módulo 6, ya considerado anteriormente, y el polinomio $a(x) = x^2 - x$, *con coeficientes en A.*

Puede verificarse fácilmente que este polinomio de segundo grado admite más de dos raíces distintas. En efecto, los números $0, 1, 3$ *y* 4 *son raíces del polinomio* $a(x)$.

EJERCICIOS

1. — *Si A es un anillo conmutativo y unitario, verificar que el conjunto de polinomios de $A(x)$ cuyo término constante es nulo, es un subanillo de $A(x)$.*

2. — *Si existe un homomorfismo entre los anillos A y B, verificar que existe también un homomorfismo entre $A(x)$ y $B(x)$.*

3. — *Sea $g(x) = x^6 - x$, un polinomio cuyos coeficientes pertenecen al anillo de enteros módulo 6. Hallar sus raíces.*

4. — *Hallar las raíces de los siguientes polinomios sobre las estructuras indicadas:*

   $p(x) = 2x + 2$ *sobre el cuerpo de enteros módulo 3. (Si n es primo, el anillo de enteros módulo n es un cuerpo.)*

   $q(x) = x^3 - x^2 - x + 2$ *sobre Z*

5. — *Factorear sobre el cuerpo de los números complejos:*

   $m(x) = x^2 + ix + 1$

   $n(x) = x^2 - 2x + i$

6. — *Verificar que $p(x) = x^2 + x + 2$ es primo sobre el cuerpo de enteros módulo 3.*

7. — *Sea $p(x) = a_0 + a_1x + \dots + a_nx^n$ sobre Z. Probar que si s es una raíz de $p(x)$, entonces s es divisor de a_0.*

CAPITULO XIV

Los sistemas de numeración

1. LA NUMERACIÓN

Para representar todas las palabras de un idioma basta recurrir a un conjunto finito de símbolos gráficos convencionales: **las letras** y a un conjunto de reglas que establece la gramática para combinarlas y enlazarlas entre sí, resultando imprescindible que el alfabeto, o conjunto de letras, tenga por lo menos dos elementos.

En matemática se presenta un problema idéntico cuando se pretende representar los números naturales, agravado aún por ser infinito el conjunto de los mismos. Demostraremos sin embargo, que al igual que en la gramática, bastará elegir un conjunto finito de símbolos gráficos —a los que en este caso llamaremos **cifras—** y un conjunto de reglas que constituirán lo que desde ahora designaremos **como sistema de numeración.**

El cardinal del conjunto de cifras —o la cantidad de cifras— de un sistema se llama **base** del mismo y como en el caso del alfabeto debe ser, por lo menos, igual a dos.

Como tal conjunto de cifras es finito, es ordenable y en consecuencia podemos suponerlo ordenado y considerar tales cifras en orden, de modo de reconocer cuál es la primera, segunda, tercera, etc. Así, si el sistema de numeración que se desea construir tiene por base el menor número natural posible, el dos, se requerirá la elección de dos únicos símbolos o cifras y el conjunto ordenado de las mismas, será:

$$\{0, 1\}$$

llamándose **sistema binario** al que depende de esa base.

Si por el contrario se desea construir un sistema de numeración de base diez, se necesitará disponer de diez símbolos. Se obtendrá así el conocido sistema decimal, cuyo conjunto ordenado de cifras es:

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

Para una base mayor que diez, doce por ejemplo, la generación de un sistema duodecimal —suponiendo que se quieran conservar los diez símbolos anteriores— exigiría crear otros dos símbolos más. Si aceptamos como nuevas cifras las figuras A y #, el conjunto de cifras del sistema duodecimal es:

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, \#\}$$

Con este criterio puede elegirse y considerar en forma ordenada el conjunto de cifras de cualquier sistema de numeración. Para una base genérica m, necesitaremos disponer de m símbolos.

Consideremos ahora el conjunto de los números naturales, N, ordenado de menor a mayor y en el que suponemos incluido el número cero como primer elemento. Llamamos N_m el subconjunto de N que contiene los m primeros números naturales.

Es decir:

N = {cero, uno, dos, ... anterior al emésimo, emésimo, siguiente del emésimo, ... }

y

N_m = {cero, uno, dos, ... anterior al emésimo}

Si llamamos S_m al conjunto de las m cifras elegidas para originar un sistema de numeración de base m, aceptando que tales cifras son: 0, 1, 2, ... A, Ф, Θ, se tendrá:

$$S_m = \{0, 1, 2, \ldots, A, \#, \Phi, \Theta\}$$

Entre N_m y S_m, puede definirse una aplicación biyectiva f, según la cual la imagen de un elemento de N_m —que está ordenado— es el elemento de S_m que ocupa el mismo lugar. Resulta así:

f (cero) = 0
f (uno) = 1
f (dos) = 2
....

f(anterior al emésimo) = Θ

La aplicación f es biyectiva y además conserva la relación de orden, lo que nos autoriza a convenir:

"Todo número natural de N_m —o sea todo número natural menor que la base—, será representado por el símbolo de S_m que es su imagen a través de la aplicación f".

Es decir: desde ahora en adelante en lugar de escribir primer número natural, segundo número natural, etc., escribiremos simplemente 0, 1, etc.; pero insistimos que 0, 1, ... son símbolos, figuras, dibujos arbitrarios que representarán según acabamos de convenir a los primeros números naturales. Estos son conceptos abstractos, aquéllos símbolos concretos que en consecuencia no son números, sino tan sólo su representación convencional.

Con este planteo hemos resuelto una parte del problema que compete a los sistemas de numeración, ya que según el mismo podemos representar con una cifra los números menores que la base elegida. Pero, ¿cómo representaremos la base misma y los números mayores que ella, usando exclusivamente los **m** símbolos creados?

Para responder a este interrogante, demostraremos el teorema siguiente, que suele llamarse:

Teorema fundamental de la numeración

Dados una base m de un sistema de numeración y un número natural p cualquiera, éste puede desarrollarse siempre bajo la forma de un polinomio y solamente uno, de las potencias de m, cuyos coeficientes son números naturales menores que la base.

H) $p \in N$; $m \in N$ $m >$ uno

T) $P(m) = u_n m^n + u_{n-1} m^{n-1} +$
$+ u_{n-2} m^{n-2} + \ldots + u_2 m^2 + u_1 m + u_0$ /

a) $P(m) = p$

b) $u_n < m$; $u_{n-1} < m$; ...... ; $u_1 < m$; $u_0 < m$

c) $P(m)$ es único

D) Efectuemos la división entera entre p y m : sea q_1 el cociente entero y u_0 el resto.

Según la ecuación e inecuación características de la división entera:

$$p = q_1 \cdot m + u_0 \ \wedge \ u_0 < m \qquad (1)$$

Reiterando el procedimiento, continuamos dividiendo cada nuevo cociente entero por m :

$$q_1 = q_2 \cdot m + u_1 \ \wedge \ u_1 < m \qquad (2)$$

$$q_2 = q_3 \cdot m + u_2 \ \wedge \ u_2 < m \qquad (3)$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

Como es $m > 1$, resulta $q_1 < p$; $q_2 < q_1$; $q_3 < q_2$; ... , es decir los cocientes son decrecientes. En una división resultará entonces $q_n < m$:

$$q_{n-1} = q_n \cdot m + u_{n-1} \ \wedge \ u_{n-1} < m \ / \ q_n < m \qquad (n)$$

Y volviendo a dividir se obtendrá cociente nulo y resto $u_n = q_n$

$$q_n = 0 \cdot m + u_n \ \wedge \ u_n < m \qquad (n+1)$$

Si escribimos nuevamente la igualdad (1) y multiplicamos las demás por m , m^2 , m^3 , ... m^n, respectivamente:

$$p = q_1 \cdot m + u_0$$
$$q_1 \cdot m = q_2 \cdot m + u_1 \cdot m$$
$$q_2 \cdot m^2 = q_3 \cdot m^3 + u_2 \cdot m^2$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$q_{n-1} \cdot m^{n-1} = q_n \cdot m^n + u_{n-1} \cdot m^{n-1}$$
$$q_n \cdot m^n = u_n \cdot m^n$$

Sumando y reduciendo términos semejantes:

$$p = u_0 + u_1 \cdot m + u_2 \cdot m^2 + \ldots + u_{n-1} \cdot m^{n-1} + u_n \cdot m^n$$

donde $u_0, u_1, \ldots u_n$ son menores que m, según su significado de restos y en consecuencia quedan demostrados los puntos a) y b) de la tesis.

Para probar la unicidad, supongamos que p puede expresarse por otro polinomio de las potencias de m, de coeficientes menores que m. Sea ese otro polinomio:

$$P'(m) = u'_0 + u'_1 \cdot m + u'_2 \cdot m^2 + \ldots . + u'_k \cdot m^k$$

O sea:

$$p = u'_0 + u'_1 \cdot m + u'_2 \cdot m^2 + \ldots . + u'_k \cdot m^k$$

$$\text{con } u'_0, u'_1, \ldots ., u'_k < m$$

Asociando, factoreando y conmutando:

$$p = (u'_1 + u'_2 \cdot m + \ldots . + u'_k \cdot m^{k-1}) \cdot m + u'_0 \wedge u'_0 < m$$

Llamando q'_1 a la expresión encerrada entre paréntesis:

$$p = q'_1 \cdot m + u'_0 \wedge u'_0 < m,$$

ecuación e inecuación que expresan que q'_1 es el cociente entero de la división de p por m y u'_0 su resto. Y como la división es una operación uniforme:

$$u'_0 = u_0 \quad \text{y} \quad q'_1 = q_1$$

Reiterando el razonamiento con q'_1, se obtendría:

$$u'_1 = u_1$$

Y así sucesivamente hasta

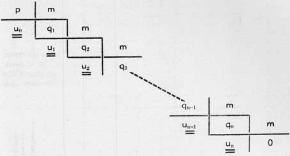
$$u'_k = u_n$$

Con lo cual P'(m) y P(m) tienen todos los coeficientes iguales, luego

$$P'(m) = P(m) \Longrightarrow P(m) \text{ es único.}$$

Observación

Un esquema elemental de las operaciones realizadas para llegar a los resultados precedentes es la distribución clásica de la división entera, aplicada reiteradamente hasta obtener un cociente cero. Los restos son los coeficientes del polinomio y el grado lo da el subíndice de cada resto, si se ha partido de u_0.



Corolario

Entre el conjunto N de los números naturales y el conjunto constituido por las formas polinómicas que se obtienen al aplicar, respecto de una base m, el teorema fundamental de la numeración, existe siempre una aplicación biyectiva.

Ello es inmediato, puesto que a cada número le corresponde un desarrollo de tipo polinómico, único respecto de m y recíprocamente a cada polinomio en m le corresponde un número natural y sólo uno, pues tal forma polinómica es una combinación de sumas y productos entre números naturales, que da por resultado otro número natural.

Observación

Una forma polinómica de las potencias de m:

$$p = u_n \cdot m^n + u_{n-1} \cdot m^{n-1} + \ldots . + u_1 \cdot m + u_0$$

queda caracterizada de manera única, por el conjunto de sus coeficientes, polinomio formal según se ha visto en el capítulo anterior:

$$\{u_n , u_{n-1} , u_{n-2} , \ldots . u_1 , u_0\}$$

Conjunto para el que puede convènirse en expresarlo por la escritura sucesiva de los coeficientes, sin signos de separación entre ellos:

$$u_n u_{n-1} u_{n-2} \ldots . u_1 u_0$$

Tal notación puede designarse como expresión formal inversa de la forma polinómica anterior.

Corolario

> **Entre el conjunto de los números naturales y el conjunto formado por las expresiones formales inversas de las formas polinómicas de aquéllos para una base m, existe siempre una aplicación biyectiva.**

Ello es inmediato, pues existe una biyección entre los números y las formas polinómicas y cada una de éstas tiene su expresión formal inversa, única, y recíprocamente:

$$p \xleftrightarrow{f_1} u_n \cdot m^n + u_{n-1} \cdot m^{n-1} + \ldots + u_1 \cdot m + u_0 \xleftrightarrow{f_2} u_n u_{n-1} \ldots u_1 u_0 \Rightarrow$$

$$\Rightarrow p \xleftrightarrow{f} u_n u_{n-1} \ldots u_1 u_0$$

Resulta entonces que a cada número natural le corresponde una expresión formal inversa y recíprocamente, respecto de una base de numeración m.

Esa expresión formal inversa está constituida por números naturales $u_n, \ldots, u_0$, todos menores que la base, los que por el isomorfismo antes introducido pueden presentarse por las cifras o símbolos elegidos para construir el sistema. Si se reemplaza cada u_i por el símbolo que le corresponde en la expresión formal inversa, se obtiene una sucesión de símbolos, que llamamos expresión cifrada del número natural p en el sistema de numeración de base m, resultando de inmediato el siguiente:

Corolario

> **Dado un número natural m, mayor que uno, considerado como base de un sistema de numeración y elegidos m símbolos para representar los m primeros números naturales, todo número natural tiene una expresión cifrada compuesta exclusivamente por esos símbolos y recíprocamente.**

De esta manera queda totalmente resuelto el problema de la numeración y respondido, sin excepciones, el interrogante planteado, pudiendo construirse tantos sistemas de numeración como se quiera, sin más que elegir una base y tantos símbolos como indique la misma.

Notación

En el estudio general de los sistemas de numeración y sus propiedades se conviene en indicar la expresión cifrada de un número p en un sistema de base m, por los mismos elementos $u_n, u_{n-1}, \ldots, u_0$, escribiendo la base como subíndice en un paréntesis abierto y subrayando cada uno de ellos, con lo que se indica que no se está utilizando el número u_n, sino el símbolo o cifra que le corresponde. Todavía, para facilitar las operaciones ulteriores, se iguala cada número natural p con su expresión cifrada.

Luego si

$$p \overset{f}{\longleftrightarrow} u_n u_{n-1} \ldots . u_1 u_0$$

se escribe la expresión cifrada de p:

$$p = \underline{u_n}\,\underline{u_{n-1}} \ldots \underline{u_1}\,\underline{u_0}{}_{(m}$$

2. PROPIEDADES DE LOS SISTEMAS DE NUMERACIÓN

I. — **Toda potencia enésima de la base se expresa por el uno seguido de tantos ceros como indica el exponente.**

T) $m^n = 10 \overset{n}{\ldots} 0$

D) La expresión polinómica de m^n es:

$$m^n = \text{uno} \cdot m^n + \text{cero} \cdot m^{n-1} + \ldots . + \text{cero} \cdot m + \text{cero}$$

Luego la expresión formal inversa es:

$$m^n \overset{f}{\longleftrightarrow} \text{Unocerocero} \ldots . \text{cero}$$

Y la expresión cifrada:

$$m^n = \overset{n}{\underline{\text{Uno}}\,\underline{\text{cero}}\,\underline{\text{cero}} \ldots . \underline{\text{cero}}}{}_{(m}$$

Y si el número uno tiene por símbolo: 1 y el número cero: 0, resulta:

$$m^n = 1\,0\,0 \overset{n}{\ldots .} 0_{(m}$$

II. — **La base de un sistema, en el mismo sistema se expresa siempre por $10_{(m}$**

T) $m = 10_{(m}$

D) Es una simple consecuencia de la propiedad anterior para $n = 1$.

$$m = 10_{(m}$$

Si se prefiere, puede obtenerse la expresión a través de las divisiones sucesivas:

$$\left.\begin{array}{r|l|l} m & m & \\ \hline \underline{0} & 1 & m \\ \hline & \underline{1} & 0 \end{array}\right\} \Rightarrow m = 10_{(m}$$

Observación

El número que representamos por $10_{(m}$ no debe leerse diez, salvo el único caso en que la base sea el natural diez, es decir en el sistema decimal.

> III. — **La expresión cifrada del producto de un número natural** p **por una potencia natural** k **de la base del sistema, se obtiene agregando a la derecha de la expresión cifrada de** p , k **ceros.**

H) $p = \underline{u_n}\,\underline{u_{n-1}} \ldots \underline{u_0}_{(m}$; m base ; $k \in N$

T) $p \cdot m^k = \underline{u_n}\,\underline{u_{n-1}} \overset{k}{\ldots}\ \underline{\text{cero}} \ldots \underline{\text{cero}}_{(m}$

D) Escribiendo la forma polinómica de p en base m:

$$p = u_n \cdot m^n + u_{n-1} \cdot m^{n-1} + \ldots. + u_1 \cdot m + u_0$$

Multiplicando por m^k:

$$p \cdot m^k = u_n \cdot m^{k+n} + u_{n-1} \cdot m^{k+n-1} + \ldots. + \\ + u_1 \cdot m^{k+1} + u_0 \cdot m^k$$

Forma polinómica que se puede completar:

$$p \cdot m^k = u_n \cdot m^{k+n} + u_{n-1} \cdot m^{k+n-1} + \ldots. + \\ + u_1 \cdot m^{k+1} + u_0 \cdot m^k + \text{cero} \cdot m^{k-1} + \overset{k}{\ldots.} + \text{cero} \cdot m^{\text{cero}}$$

donde los términos agregados, de coeficientes cero, son k.

Luego por significado de expresión cifrada:

$$p \cdot m^k = \underline{u_n}\,\underline{u_{n-1}} \ldots \underline{u_1}\ \underline{u_0}\ \underline{\text{cero}} \overset{k}{\ldots} \underline{\text{cero}}_{(m}$$

Observación

Las propiedades I, II y III, son a veces utilizadas para "demostrar" las "ventajas" del sistema de numeración decimal. Las demostraciones generales que se han desarrollado, cualquiera sea m , eliminan esa supuesta "ventaja" y por lo tanto el sistema decimal no tiene razones para ser "mejor" que los construidos con otras bases. Por el contrario, desde el punto de vista matemático, hubiera sido preferible, para múltiples estudios, la elección de una base que contuviera más divisores, como por ejemplo el número doce.

La objeción formulada se refiere al sistema de numeración decimal y no al sistema métrico decimal, cuya característica importante no es la de escribir los números en base diez, sino la de que todos los múltiplos y submúltiplos de las diferentes unidades se hallan vinculados por potencias naturales de diez. De construirse un sistema de numeración duodecimal, por ejemplo, el sistema de medidas debiera utilizar las potencias naturales de doce para vincular múltiplos y submúltiplos y en tal caso sería tan sencillo y cómodo como el sistema métrico decimal.

Probablemente la única razón valedera que justifica la subsistencia del sistema de numeración decimal en todo el cálculo operativo, es que la más antigua, y todavía en uso, máquina de calcular, es la construida con los dedos de las dos manos.

3. OPERACIONES EN LOS SISTEMAS DE NUMERACIÓN

Analizaremos los mecanismos operativos de la adición y la multiplicación solamente, ya que las restantes operaciones no son más que consecuencia de ellas.

Adición

Sean:

$$\underline{u_n}\ \underline{u_{n-1}} \dots \underline{u_1}\ \underline{u_0}_{(m} \quad \text{y} \quad \underline{v_k}\ \underline{v_{k-1}} \dots \underline{v_1}\ \underline{v_0}_{(m}$$

las expresiones cifradas en base m de dos números naturales q y r, respectivamente. Se desea encontrar la expresión cifrada, en la misma base, del número natural $s = q + r$.

Escribamos las correspondientes formas polinómicas:

$$q = u_n \cdot m^n + u_{n-1} \cdot m^{n-1} + \dots + u_1 \cdot m + u_0$$
$$r = v_k \cdot m^k + v_{k-1} \cdot m^{k-1} + \dots + v_1 \cdot m + v_0$$

donde $n \gtreqless k$. Supongamos $n \geqslant k$. Si $n < k$, en virtud de la conmutatividad de la suma, bastaría hacer: $s = q + r = r + q$

Sumando esas expresiones polinómicas y reduciendo términos semejantes:

$$q + r = u_n \cdot m^n + \dots + (u_k + v_k) \cdot m^k + \dots + \\ + (u_1 + v_1) \cdot m + (u_0 + v_0) \qquad (1)$$

Y en consecuencia la expresión cifrada de s, es:

$$s = \underline{u_n} \dots \underline{(u_k + v_k)} \dots \underline{(u_1 + v_1)}\ \underline{(u_0 + v_0)}_{(m}$$

De donde resulta la siguiente conclusión:

"La expresión cifrada de la suma de dos números naturales expresados en un mismo sistema de numeración tiene por cifras las respectivas sumas de las cifras de igual ubicación, contadas de derecha a izquierda".

Queda así justificado el clásico mecanismo utilizado en el sistema decimal —y que ahora resulta válido en cualquier sistema— de sumar las cifras "encolumnadas", de derecha a izquierda

Observación

Las cifras u y v son menores que m, pero al sumarlas, si tomamos por ejemplo u_0 y v_0, su suma puede ser:

$$u_0 + v_0 \gtreqless m$$

Si $u_0 + v_0 < m$, existe en el sistema una cifra para expresar tal suma.

Pero si $u_0 + v_0 \geqslant m$, no existe tal cifra único. En tal caso:

$$u_0 + v_0 = 1 \cdot m + u' \qquad \text{donde } u' < m$$

Reemplazando en (1):

$$q + r = u_n \cdot m^n + \ldots + (u_k + v_k) \cdot m^k + \ldots + \\ + (u_1 + v_1) \cdot m + 1 \cdot m + u'$$

O sea:

$$q + r = u_n \cdot m^n + \ldots + (u_k + v_k) \cdot m^k + \ldots + \\ + (u_1 + v_1 + 1) \cdot m + u'$$

Luego:

$$s = \underline{u_n} \ldots \underline{(u_k + v_k)} \ldots \underline{(u_1 + v_1 + 1)}\, \underline{u'}$$

Resultando la otra expresión clásica: Si $u_0 + v_0$ es mayor que m, (lo mismo para cualquier $u_i + v_i$) es igual a $\alpha \cdot m + u'$; escribo u' y "me llevo α" para la suma subsiguiente de la izquierda.

Ejemplo

Si se desean sumar, en base diez, los números representados por

1234 *y* 899, *se tendrá:*

$$1234 = 1 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10 + 4$$

y

$$899 = 8 \cdot 10^2 + 9 \cdot 10 + 9$$

Luego

$$\begin{aligned} 1234 + 899 &= 1 \cdot 10^3 + (2+8) \cdot 10^2 + (3+9) \cdot 10 + (4+9) \\ &= 1 \cdot 10^3 + (2+8) \cdot 10^2 + (3+9) \cdot 10 + (10+3) \\ &= 1 \cdot 10^3 + (2+8) \cdot 10^2 + (3+9+1) \cdot 10 + 3 \\ &= 1 \quad 10^3 + (2+8) \cdot 10^2 + (10+3) \cdot 10 + 3 \\ &= 1 \cdot 10^3 + (2+8) \cdot 10^2 + 1 \cdot 10^2 + 3 \cdot 10 + 3 \\ &= 1 \cdot 10^3 + (2+8+1) \cdot 10^2 + 3 \cdot 10 + 3 \\ &= 1 \cdot 10^3 + (10+1) \cdot 10^2 + 3 \cdot 10 + 3 \\ &= (1+1) \cdot 10^3 + 1 \cdot 10^2 + 3 \cdot 10 + 3 \\ &= 2 \cdot 10^3 + 1 \cdot 10^2 + 3 \cdot 10 + 3 \end{aligned}$$

Y en consecuencia:

$$1234 + 899 = 2133$$

Resultado al que se llega en la disposición práctica usual:

$$\begin{array}{r} 1234 \\ +\ \ 899 \\ \hline 2133 \end{array}$$

Multiplicación

Sin necesidad de detallar como antes cada paso, un planteo similar nos lleva a la clásica disposición operativa de la multiplicación.

Si

$$q = \underline{u_2u_1u_0}$$

y

$$\begin{aligned} r &= \underline{v_1v_0} \\ q &= u_2 \cdot m^2 + u_1 \cdot m + u_0 \\ r &= \qquad\qquad v_1 \cdot m + v_0 \end{aligned}$$

Luego:

$$p = q \cdot r = (u_2 \cdot m^2 + u_1 \cdot m + u_0) \cdot (v_1 \cdot m + v_0)$$

$$\begin{aligned} p = {} & u_2 \cdot v_1 \cdot m^3 + (u_2 \cdot v_0 + u_1 \cdot v_1) \cdot m^2 + \\ & + (u_1 \cdot v_0 + u_0 \cdot v_1) \cdot m + u_0 \cdot v_0 \end{aligned}$$

O sea:

$$p = \underline{(u_2 \cdot v_1)}\ \underline{(u_2 \cdot v_0 + u_1 \cdot v_1)}\ \underline{(u_1 \cdot v_0 + u_0 \cdot v_1)}\ \underline{(u_0 \cdot v_0)}$$

Resultado que coincide con el famoso mecanismo "escalera"

$$\begin{array}{rr} q = & \underline{u_2u_1u_0} \\ r = & \underline{v_1v_0} \\ \hline & u_2 \cdot v_0 \ \ u_1 \cdot v_0 \ \ u_0 \cdot v_0 \\ u_2 \cdot v_1 \ \ u_1 \cdot v_1 \ \ u_0 \cdot v_1 & \\ \hline p = \underline{(u_2 \cdot v_1)}\ \underline{(u_2 \cdot v_0 + u_1 \cdot v_1)} & \underline{(u_1 \cdot v_0 + u_0 \cdot v_1)}\ \underline{(u_0 \cdot v_0)} \end{array}$$

Donde vale la misma observación anterior si alguno de los números representados entre paréntesis es mayor o igual que m.

4. TABLAS DE ADICIÓN Y MULTIPLICACIÓN

Conociendo ya la disposición práctica de las dos operaciones fundamentales es cómodo para el mecanismo operatorio construir las tablas de tales operaciones, siguiendo el criterio expuesto en pág. 64.

Teniendo en cuenta que si se trabaja en base m, la cifra máxima con la que se debe operar corresponde a $m - 1$, tendremos así limitado el desarrollo a dar a cada tabla.

A título de ejemplo construiremos las tablas de adición y multiplicación en base **seis,** disponiendo entonces de las cifras ordenadas 0, 1, 2, 3, 4, 5, que representan en ese orden a los números menores que **seis,** cifrándose este último $10_{(seis}$.

Tabla de adición

Disponemos las expresiones cifradas del cero al cinco en una primera fila. Como segunda fila las expresiones cifradas de los números que resultan al sumar **uno** a cada uno de los anteriores y así sucesivamente hasta llegar a la sexta fila. Recordando el mecanismo operativo, si se desea cifrar el número siete, como es el siguiente de seis, es decir seis más uno, se tendrá $10 + 1 = 11$.

Resulta, con tal criterio la siguiente tabla de doble entrada:

0	1	2	3	4	5
1	2	3	4	5	10
2	3	4	5	10	11
3	4	5	10	11	12
4	5	10	11	12	13
5	10	11	12	13	14

Tabla de multiplicación

Disponemos en la primera fila los números del uno al cinco, descartando el cero, pues su producto por cualquier número es cero.

Como segunda fila escribimos el duplo de la primera o sea

$$2^{a} F = 1^{a} F + 1^{a} F$$

lo que se calcula mediante la tabla de adición ya construida.

Análogamente la tercera fila se obtiene triplicando la 1ª, o lo que es lo mismo:

$$3^{a} F = 1^{a} F + 2^{a} F$$

Y con idéntico criterio se obtienen la 4º y 5º filas.

1	2	3	4	5
2	4	10	12	14
3	10	13	20	23
4	12	20	24	32
5	14	23	32	41

Ejemplos

Construidas las tablas y demostrados los mecanismos operativos, podemos realizar cualquier cálculo en el sistema de base seis.

a) Sea sumar: $1034 + 4542 + 355$

Dispongamos en columna y efectuemos:

1034	$4 + 2 + 5 = 10 + 5 = 15$ *Se escribe 5 y pasa 1 a 2ª Col.*
4542	$1 + 3 + 4 + 5 = 4 + 4 + 5 = 12 + 5 = 23$
	Queda 3 y pasa 2
355	$2 + 0 + 5 + 3 = 2 + 5 + 3 = 11 + 3 = 14$
	Queda 4 y pasa 1
$\overline{10435}$	$1 + 1 + 4 + 0 = 2 + 4 = 10$

b) Sea multiplicar 345×123

345	
123	
$\overline{1523}$	$3 \times 5 = 23$; $(3 \times 4) + 2 = 20 + 2 = 22$; $(3 \times 3) + 2 = 13 + 2 = 15$
1134	$2 \times 5 = 14$; $(2 \times 4) + 1 = 12 + 1 = 13$; $(2 \times 3) + 1 = 10 + 1 = 11$
345	
$\overline{52203}$	

5. PASAJE ENTRE SISTEMAS

El problema que nos proponemos analizar es el de encontrar la expresión cifrada de un número en un sistema de base m, cuando se conoce su expresión cifrada en otra base n y recíprocamente.

Puesto que el sistema décimal es bien conocido, así como todas las operaciones en el mismo, desdoblaremos el problema general enunciado, en los siguientes casos:

a) Pasaje del sistema decimal a otro de base m.

b) Pasaje de un sistema de base m al decimal.

c) Caso general: pasaje de base m a base n.

a) **Decimal a base** m.

El teorema fundamental nos da la solución. En efecto, bastará realizar las divisiones reiteradas del número p dado, por m (operando en base 10).

Los restos son las cifras de p en base m.

Ejemplo

Sea p = *10435 en base diez. Expresarlo en base siete.*

$$\begin{array}{r|r|r|r|r|r}
10435 & 7 & & & & \\ \hline
\underline{5} & 1490 & 7 & & & \\ \hline
 & \underline{6} & 212 & 7 & & \\ \hline
 & & \underline{2} & 30 & 7 & \\ \hline
 & & & \underline{2} & 4 & 7 \\ \hline
 & & & & \underline{4} & 0
\end{array}$$

Luego:

$$10435_{(\text{Diez}} = 42265_{(\text{siete}}$$

b) **Base** m **a decimal**

Sea $p = \underline{u_n u_{n-1}} \ldots . \underline{u_1 u_0}_{(m}$

Luego:

$$p = u_n \cdot m^n + u_{n-1} \cdot m^{n-1} + \ldots . + u_1 \cdot m + u_0$$

Realizando todas las operaciones del segundo miembro en base diez, se obtendrá p en esa base, esto es, bastará calcular el valor numérico de la forma polinómica, cuando se reemplace m por su expresión en base diez.

Ejemplo

Sea $p = 42265_{(\text{siete}}$

$$p = 4 \times 7^4 + 2 \times 7^3 + 2 \times 7^2 + 6 \times 7 + 5_{(\text{diez}}$$

$$p = 9604 + 686 + 98 + 42 + 5_{(\text{diez}}$$

$$p = 10435_{(\text{Diez}}$$

c) **Base** m **a base** n

De acuerdo con los casos resueltos bastará realizar los siguientes pasajes:

1. — Base m a base diez.
2. — Base diez a base n .

Ejemplo

Sea $p = 42265_{(\text{siete}}$. *Expresarlo en base seis.*

1.— $42265_{(\text{Siete}} = 10435_{(\text{Diez}}$

2.—

$$\begin{array}{r|r|r|r|r|r|r}
10435 & 6 & & & & & \\ \hline
\underline{1} & 1739 & 6 & & & & \\ \cline{2-3}
 & \underline{1} & 289 & 6 & & & \\ \cline{3-4}
 & & \underline{1} & 48 & 6 & & \\ \cline{4-5}
 & & & \underline{0} & 8 & 6 & \\ \cline{5-6}
 & & & & \underline{2} & 1 & 6 \\ \cline{6-7}
 & & & & & \underline{1} & 0
\end{array}$$

Luego: $10435_{(\text{Diez}} = 120111_{(\text{seis}}$

O sea:

$$42265_{(\text{siete}} = 120111_{(\text{seis}}$$

Observación

De todo lo expuesto surge que el sistema de numeración más simple es el de base mínima dos, para construir el cual se necesitan las dos únicas cifras 0 y 1.

Las tablas de operación se reducen sencillamente a:

$$1 + 0 = 0 + 1 = 1$$
$$1 + 1 = 10$$

y

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

La elementalidad operatoria y esa única alternativa 0, 1 para sus cifras ha hecho que el sistema binario, pese al abundante número de cifras que requiere un número no muy grande, sea de fundamental aplicación en equipos electrónicos de cómputos, donde puede introducirse una correspondencia entre 0 y 1 con circuito abierto y cerrado, respectivamente.

EJERCICIOS

1. — *Verificar la adición realizada en la pág. 275 efectuando el pasaje al sistema decimal.*

2. — *La misma cuestión para la multiplicación de pág. 275.*

3. — *Expresar en el sistema decimal los números:*

$$a = 11_{(dos}$$
$$b = 111_{(dos}$$
$$c = 1111_{(dos}$$
$$d = 6460_{(siete}$$
$$3 = 69\,A\,\#\,4_{(doce}$$

4. — *Expresar los siguientes números cifrados en base seis, en base ocho.*

$$a = 4502$$
$$b = 3412$$
$$c = 543$$

5. — *Realizar el pasaje del ejercicio 4 sin utilizar el sistema decimal.*

6. — *Indicar si existe algún sistema de numeración y en tal caso determinar su base, en el cual:*

$$31_{(x} + 13_{(x} = 443_{(x}$$

7. — *Construir las tablas de adición y multiplicación en base cinco.*

8. — *Estudiar la sustracción en base cinco.*

9. — *Calcular en base cinco:* $x = (a - b - c) \cdot d$, *para*

$$a = 432, \quad b = 312, \quad c = 214 \text{ y } d = 103$$

10. — *Aplicando la operatoria del sistema decimal, deducir el mecanismo de la división en base cinco.*

CAPITULO XV

Homotecia en el plano

1. DEFINICIÓN Y PROPIEDADES ELEMENTALES

Definición

Dado un punto fijo O y un número real k distinto de cero, se llama homotecia de centro O y razón k a la transformación puntual que a todo punto M le hace corresponder otro punto M' tal que:

a) $M' \in OM$ b) $\overline{OM'} = k \cdot \overline{OM}$

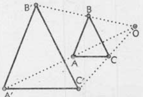
Notación

La homotecia de centro O y razón k se indica: $\mathcal{H}(O, k)$

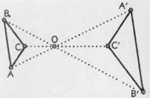
Definición

Dos figuras se llaman homotéticas si sus puntos se corresponden en una homotecia.

Ejemplos



$\mathcal{H}(O, 2) \cdot ABC = A'B'C'$



$\mathcal{H}(O, -2) \cdot ABC = A'B'C'$

Si $k > 0$, la homotecia se dice positiva. En tal caso las semirrectas OM y OM' son del mismo sentido y $M' \in \overrightarrow{OM}$.

Si $k < 0$ la homotecia se dice negativa. En tal caso las semirrectas OM y OM' son opuestas y $M' \in \overleftarrow{OM}$.

Si $k = 1$ la homotecia se reduce a la identidad.

Si $k = -1$, la homotecia equivale a una simetría de centro O.

Corolario

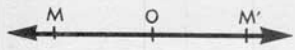
Si $|k| \neq 1$ **existe un solo punto unido, que es el centro** O.

Es inmediato, por la definición, que O es punto unido. En efecto: si su homólogo fuese O', debe verificarse $\overline{OO'} = k \cdot \overline{OO}$. Como $\overline{OO}$ es un segmento nulo resulta $\overline{OO'}$ segmento nulo y por lo tanto O' coincide con O.

Si $M \neq O$, de $\overline{OM'} = k \cdot \overline{OM}$ se tiene que $\dfrac{\overline{OM}}{1} = \dfrac{\overline{OM'}}{k}$

Luego $\dfrac{\overline{OM'} - \overline{OM}}{|k - 1|} = \overline{OM}$

O sea $\overline{MM'} = |k - 1| \cdot \overline{OM}$



Y como $|k| \neq 1$,

$|k - 1| \neq 0$,

Es decir: $\overline{MM'}$ no es nulo y por lo tanto M' es distinto de M. Luego el único punto unido es O.

Homotecia inversa

Dada la homotecia $\mathcal{H}(O, k)$ se verifica, para todo punto M, que su transformado $M' \in OM$ y que $\overline{OM'} = k \cdot \overline{OM}$. Esto puede expresarse diciendo que $\overline{OM} = \dfrac{1}{k} \cdot \overline{OM'}$ · lo cual, junto con la condición anterior de alineamiento, indica que M es el transformado de M' en la homotecia $\mathcal{H}\left(O, \dfrac{1}{k}\right)$. Luego:

Toda homotecia admite una transformación recíproca, que es la homotecia del mismo centro y de razón inversa.

Observación

En lo que sigue consideraremos el caso general en que k es distinto de 1.

2. TRANSFORMACIÓN DE RECTAS, SEMIRRECTAS Y SEGMENTOS.

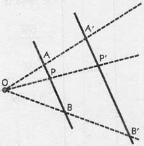
Teorema

Toda recta se transforma por una homotecia en otra recta paralela a ella.

H) AB y $\mathscr{H}(O, k)$

T) $\mathscr{H}(O, k) \cdot AB = A'B' \,/\, A'B' \parallel AB$

D) Si $\mathscr{H}(O, k) \cdot A = A'$ y $\mathscr{H}(O, k) \cdot B = B'$,



se tiene, por definición de homotecia:

$$\overline{OA'} = k\ \overline{OA} \text{ y}$$
$$\overline{OB'} = k\ \overline{OB}$$

O sea:

$$\frac{\overline{OA'}}{\overline{OA}} = k \quad \text{y} \quad \frac{\overline{OB'}}{\overline{OB}} = k$$

Luego:

$$\frac{\overline{OA'}}{\overline{OA}} = \frac{\overline{OB'}}{\overline{OB}}$$

Por lo tanto, por el recíproco del teorema de Tales, se cumple que: $A'B' \parallel AB$. Es necesario demostrar ahora que todo punto perteneciente a la recta AB se transforma por la homotecia dada en un punto de A'B'.

Sea $P \in AB$ y $\mathscr{H}(O, k) \cdot P = P'$. Luego:

$$\overline{OP'} = k \cdot \overline{OP} \ ; \text{ o sea } \frac{\overline{OP'}}{\overline{OP}} = k$$

Luego

$$\frac{\overline{OA'}}{\overline{OA}} = \frac{\overline{OP'}}{\overline{OP}}$$

Por el recíproco citado, resulta: $A'P' \parallel AP$. O sea $A'P' \parallel AB$.

Por la unicidad de la paralela $A'P' = A'B'$, o sea:

$$P' \in A'B'$$

Corolario

Si la recta dada pasa por el centro de homotecia, es unida.

En efecto, dada la recta OA, su homóloga en la homotecia es la recta determinada por los respectivos homólogos de A y de O. Pero O es punto unido y el homólogo A' de A pertenece a la recta OA por definición de homotecia. Luego $OA' = OA$.

Teorema

Toda semirrecta se transforma por una homotecia en otra semirrecta. Si la razón es positiva las semirrectas homólogas son del mismo sentido y si es negativa, son de sentido contrario.

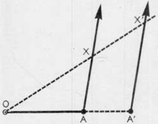
H) $\overrightarrow{AX}$ y $\mathcal{H}(O, k)$

1. — $k > 0$
2. — $k < 0$

T) $\mathcal{H}(O, k) \cdot \overrightarrow{AX} = \overrightarrow{A'X'}$

1. — $\overrightarrow{AX}$ y $\overrightarrow{A'X'}$ acordes
2. — $\overrightarrow{AX}$ y $\overrightarrow{A'X'}$ discordes

D) 1. — $k > 0$. Por el teorema anterior, la recta AX se transforma en una recta paralela. Luego los dos puntos homólogos de los de AX pertenecen a una recta paralela.



Si $\mathcal{H}(O, k) \cdot A = A'$, $A' \in \overrightarrow{OA}$ por ser $k > 0$

Si $\mathcal{H}(O, k) \cdot X = X'$, $X' \in \overrightarrow{OX}$

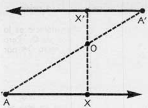
Luego, como las rectas OX y OA se cortan en O, cada una queda dividida por dicho punto en dos semirrectas opuestas y pertenecientes a semiplanos distintos con respecto a la otra recta.

Así $\overrightarrow{OX}$ pertenece a uno de los semiplanos con respecto a OA.

Si X' pertenece a $\overrightarrow{OX}$, como se ha visto, X y X' están en un mismo semiplano con respecto a OA.

Luego $\overrightarrow{AX}$ y $\overrightarrow{A'X'}$ pertenecen a un mismo semiplano con respecto a la recta OA, que es idéntica a la AA' que une sus orígenes y como además, pertenecen a rectas paralelas, son acordes.

2. — $k < 0$. Como en el caso anterior los homólogos de los puntos de AX pertenecen a una recta A'X' paralela a la primera.

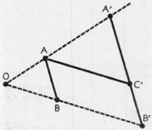


Si $\mathcal{H}(O, k) \cdot X = X'$, $\overrightarrow{OX}$ y $\overrightarrow{OX'}$ son opuestas por ser $k < 0$. O sea X y X' están en semiplanos distintos con respecto a cualquier recta, como AA', que pase por O y por lo tanto lo mismo ocurre con $\overrightarrow{AX}$ y $\overrightarrow{A'X'}$. O sea:

$\overrightarrow{AX}$ y $\overrightarrow{A'X'}$ son discordes.

Corolario

Toda homotecia $\mathcal{H}(O, k)$ transforma a dos puntos cualesquiera A y B en otros dos A' y B' tales que $\overline{A'B'} = k \cdot \overline{AB}$.



Por definición de segmento, los puntos del $\overline{AB}$ pertenecen a $\overrightarrow{AB}$ y a $\overrightarrow{BA}$. Luego, por el teorema anterior, sus homólogos pertenecen a $\overrightarrow{A'B'}$ y a $\overrightarrow{B'A'}$, homólogos, respectivamente, de las anteriores. Es decir pertenecen al $\overline{A'B'}$.

Además AB // A'B' por ser rectas homólogas en la homotecia.

Por otra parte $\dfrac{\overline{OA'}}{\overline{OA}} = k$ y $\dfrac{\overline{OB'}}{\overline{OB}} = k$ por definición de homotecia.

La paralela por A a OB corta a A'B' en C' y por teorema de Tales:

$$\frac{\overline{OA'}}{\overline{OA}} = \frac{\overline{A'B'}}{\overline{C'B'}}$$

Pero $\overline{C'B'} = \overline{AB}$, por ser lados opuestos de un paralelogramo. Luego:

$$\frac{\overline{OA'}}{\overline{OA}} = \frac{\overline{A'B'}}{\overline{AB}} \quad \text{es decir} \quad \frac{\overline{A'B'}}{\overline{AB}} = k$$

y por lo tanto:

$$\overline{A'B'} = k \cdot \overline{AB}$$

Recíproco

> **Si una transformación puntual transforma dos puntos cualesquiera A y B en otros dos puntos A' y B' tales que AB y A'B' sean paralelas y $\overline{A'B'} = k \cdot \overline{AB}$ (k distinto de 1), dicha transformación es una homotecia de razón k.**

Como AB y A'B' son paralelas, los cuatro puntos pertenecen a un mismo plano y por lo tanto las rectas AA' y BB' también. Luego se cortan o son paralelas.

Si fuesen paralelas, resultaría $\overline{A'B'} = \overline{AB}$, por ser segmentos de paralelas entre paralelas, o sea $k = 1$, contra lo supuesto.

Por lo tanto AA' y BB' se cortan en un punto O.

Por teorema de Tales $\dfrac{\overline{OA'}}{\overline{OA}} = \dfrac{\overline{OB'}}{\overline{OB}} = k'$, es decir

$$\overline{OA'} = k' \cdot \overline{OA} \quad \text{y} \quad \overline{OB'} = k' \cdot \overline{OB}$$

Como O, A y A' están alineados, y también lo están, O, B y B', resulta por definición de homotecia:

$$\text{A y A' son homólogos en } \mathcal{H}\,(O, k')$$
$$\text{B y B' son homólogos en } \mathcal{H}\,(O, k')$$

Luego por el corolario anterior:

$$\overline{A'B'} = k' \cdot \overline{AB}$$

Pero por la H) $\overline{A'B'} = k \cdot \overline{AB}$

Luego $k = k'$ por unicidad de la razón entre dos cantidades.

Es decir, la transformación dada es la homotecia $\mathcal{H}$ **(O, k)**

3. TRANSFORMACIÓN DE ÁNGULOS

Definición

> **Se llama transformación conforme a la que conserva los ángulos.**

Es decir, los ángulos homólogos, o sea, formados por pares de semirrectas respectivamente homólogas, son congruentes.

Teorema

> **La homotecia es una transformación conforme.**

H) $\mathcal{H}(O, k) \cdot \overrightarrow{AB} = \overrightarrow{A'B'}$ y $\mathcal{H}(O, k) \cdot \overrightarrow{AC} = \overrightarrow{A'C'}$

T) $\widehat{BAC} = \widehat{B'A'C'}$

D) Las semirrectas homólogas en una homotecia son paralelas y del mismo o distinto sentido según sea $k \gtrless 0$, como se demostró anteriormente. Luego:

$\widehat{BAC} = \widehat{B'A'C'}$ por tener sus lados respectivamente paralelos y del mismo sentido o respectivamente paralelos y de sentido contrario.

Corolarios

I. — Si dos rectas son perpendiculares, sus homólogas en una homotecia también lo son.

II. — Si dos figuras de un plano son congruentes, sus transformadas en una homotecia también lo son.

4. TRANSFORMACIÓN DE CIRCUNFERENCIAS

Teorema

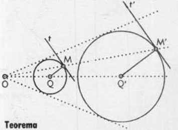
Toda homotecia $\mathcal{H}(O, k)$ transforma una circunferencia de radio r en otra circunferencia de radio $r' = k \cdot r$.

H) $C(Q, r)$ y $\mathcal{H}(O, k)$

T) $\mathcal{H}(O, k) \cdot C(Q, r) = C(Q', r') / r' = k \cdot r$

D) Si $\mathcal{H}(O, k) \cdot Q = Q'$, tomando un punto M cualquiera de la $C(Q, r)$ se tiene que:

$\mathcal{H}(O, k) \cdot M = M'$ y $\overline{Q'M'} = k \cdot \overline{QM}$ por teorema anterior



O sea $\overline{Q'M'} = k \cdot r$

Es decir $\forall M \in C(Q, r)$, la distancia de su homólogo a Q' es constante e igual a $k \cdot r$. Luego por definición de circunferencia, los homólogos de los puntos de la $C(Q, r)$ pertenecen a una circunferencia:

$C(Q', r') / r' = k \cdot r$

Teorema

Si dos circunferencias son homólogas en una homotecia, las respectivas tangentes en dos puntos homólogos son paralelas.

H) $\mathcal{H}(O, k) \cdot C(Q, r) = C(Q', r')$

$M \in C(Q, r)$, y $\mathcal{H}(O, k) \cdot M = M'$

t tangente a $C(Q, r)$ en M

t' tangente a $C(Q', r')$ en M'

T) $t \parallel t'$

D) Por propiedad de la tangente a una circunferencia:

$$t \perp QM \text{ en } M$$

Luego su homóloga en la homotecia debe pertenecer a M' y ser perpendicular a Q'M', pues la homotecia conserva la perpendicularidad. O sea: t' homóloga de t en la homotecia $\mathcal{H}(O, k)$.

Por lo tanto $t \parallel t'$ por propiedad de las rectas homólogos.

Observación

Dada una figura cualquiera y una homotecia siempre se puede determinar la figura homotética de la dada, sin más que aplicar la definición de homotecia. El problema inverso, por lo general, no tiene solución. Es decir, dadas dos figuras no existe necesariamente una homotecia que transforme a una en la otra, puesto que, como hemos visto, tienen que cumplirse ciertas condiciones esenciales de alineamiento, paralelismo, proporcionalidad, etc.

Sin embargo, si las dos figuras son circunferencias, esas condiciones se dan siempre. Es decir, dadas dos circunferencias existe siempre una homotecia que las vincula.

Precisamente, el objeto de los problemas siguientes es hallar esa homotecia y dar la manera de encontrar su centro y determinar su razón.

Para ello debemos recordar que, dado un segmento, existe siempre y es único el punto que lo divide aditiva o sustractivamente en una razón dada, respectivamente negativa o positiva.

Problema I

Dadas dos circunferencias de igual radio hallar, si existe, una homotecia que transforme una de ellas en la otra.

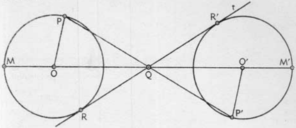
Sean las circunferencias $C(O, r)$ y $C(O', r') \,/\, r' = r$

Si existe una homotecia $\mathcal{H}(Q, k) \,/\, \mathcal{H}(Q, k) \cdot C(O, r) = C(O', r')$, debe ser:

$$r' = |k| \cdot r \quad \text{o sea} \quad \frac{r'}{r} = |k|$$

Pero $r' = r \Rightarrow k = |1|$. No puede ser $k = 1$, pues en tal caso la homotecia equivale a la identidad, según se ha visto y por lo tanto transformaría a cada circunferencia en sí misma.

Luego, si existe una homotecia $\mathcal{H}(Q, k)$ que transforme a la $C(O, r)$ en la $C(O', r')$ debe ser $k = -1$, es decir la homotecia será negativa.



Tomamos en $C(O, r)$ un punto arbitrario $P \notin OO'$ y trazamos en la otra circunferencia el radio $\overline{O'P'}$ de sentido contrario a $\overline{OP}$ y de sostenes paralelos. La recta PP' corta siempre al $\overline{OO'}$, en un punto Q.

Como los triángulos OPQ y O'P'Q' son congruentes por segundo criterio, resulta $|\overline{OQ}| = |\overline{O'Q'}|$ y de signo contrario por ser Q interior al $\overline{OO'}$. Es decir:

$$\overline{OQ} = -\overline{O'Q}$$

y como O, Q y O' están alineados, resulta:

O' es homólogo de O en la homotecia $\mathcal{H}(Q, -1)$.

Análogamente $|\overline{O'P'}| = |\overline{OP}|$ y de signo contrario por serlo sus sentidos, es decIr

$\overline{O'P'} = -\overline{OP}$, luego, por teorema anterior:

O' y P' son homólogos de O y P, respectivamente, en una homotecia de razón -1. Esa homotecia tiene por centro Q, pues según vimos:

$$\mathcal{H}(Q, -1) \cdot O = O'$$

y no puede ser otro, por la unicidad del punto que divide a $\overline{OO'}$ en la razón $k = -1$. Luego:

P' es homólogo de P en la homotecia $\mathcal{H}(Q, -1)$.

Si el punto considerado pertenece a $\overline{OO'}$, como M, basta considerar el radio $\overline{O'M'} \in OO'$ y de sentido contrario al $\overline{OM}$, es decir:

$$\overline{O'M'} = -\overline{OM}$$

Y repitiendo la última parte del razonamiento anterior, se tiene

M′ es homólogo de M en la homotecia $\mathcal{H}(Q, -1)$.

Luego existe la homotecia $\mathcal{H}(Q, -1)$ que transforma a la circunferencia $C(O, r)$ en la $C(O', r') \,/\, r = r'$.

Problema II

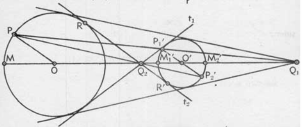
Dadas dos circunferencias no concéntricas de distinto radio, hallar, si existe, una homotecia que transforme una de ellas en la otra.

Las circunferencias pueden ser exteriores, tangentes exterior o interiormente, secantes o una interior a la otra. El procedimiento para hallar la homotecia que las vincule, como se verá, es el mismo en todos los casos, pues no depende del caso particular en que se encuentren las circunferencias dadas.

Sean $C(O, r)$ y $C(O', r') \,/\, O \neq O'$ y $r \neq r'$

Si existe una homotecia $\mathcal{H}(Q, k) \,/\, \mathcal{H}(Q, k) \cdot C(O, r) = C(O', r')$, debe ser:

$$r' = |k| \cdot r \quad \text{o sea:} \quad \frac{r'}{r} = |k|$$



Tomamos en $C(O, r)$ un punto arbitrario $P \notin OO'$ y trazamos en la otra circunferencia el diámetro $P_1'P_2'$ de sostén paralelo a OP. Luego uno de los radios, como el $O'P_1'$, es del mismo sentido que OP, y el otro es de sentido contrario.

Las rectas PP_1' y PP_2' cortan a OO' en Q_1 y Q_2, respectivamente, tales que Q_1 es exterior y Q_2 es interior al $\overline{OO'}$.

Por teorema de Tales se tiene:

$$\frac{\overline{O'Q_1}}{\overline{OQ_1}} = \frac{\overline{O'P_1'}}{\overline{OP}} = \frac{r'}{r}$$

$$\overline{O'Q_1} = \frac{r'}{r} \cdot \overline{OQ_1} \;/\; \frac{r'}{r} > 0$$

por ser $\overline{O'Q_1}$ y $\overline{OQ_1}$ del mismo sentido

Y como O , O' y Q_1 están alineados, resulta:

O' es homólogo de O en la homotecia $\mathcal{H}\left(Q_1, \frac{r'}{r}\right)$

Pero también $\overline{O'P_1'} = \frac{r'}{r} \cdot \overline{OP}$; luego, por teorema anterior:

O' y P_1' son homólogos de O y P, respectivamente, en una homotecia de razón $k = \frac{r'}{r}$.

Esta homotecia tiene como centro a Q_1 pues según vimos:

$\mathcal{H}\left(Q_1, \frac{r'}{r}\right) \cdot O = O'$ y no puede ser otro por la unicidad del punto que divide a $\overline{OO'}$ en la razón $k = \frac{r'}{r}$. Luego:

P_1' es homólogo de P en la homotecia $\mathcal{H}\left(Q_1, \frac{r'}{r}\right)$

Si el punto considerado pertenece a $\overline{OO'}$, como el M , basta considerar el radio $\overline{O'M'} \in \overline{OO'}$ y del mismo sentido que $\overline{OM}$. Resulta:

$$\frac{\overline{O'M'}}{\overline{OM}} = \frac{r'}{r} \text{ (razón positiva)}$$

Lo cual significa:

M' es homólogo de M en la $\mathcal{H}\left(Q_1, \frac{r'}{r}\right)$

Luego existe la homotecia $\mathcal{H}\left(Q_1, \frac{r'}{r}\right)$ que transforma a la C(O , r) en la C(O' , r').

Esta homotecia no es única. En efecto, por teorema de Tales:

$$\frac{\overline{O'Q_2}}{\overline{OQ_2}} = \frac{\overline{O'P_2'}}{\overline{OP}} = \frac{r'}{r}$$

La razón es negativa por $\overline{O'P_2'}$ y $\overline{OP}$ de distinto sentido. Luego:

$\overline{O'Q_2} = -\frac{r'}{r}\overline{OQ_2}$ y como O, O' y Q_2 están alineados, resulta:

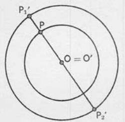
O' es homólogo de O en la $\mathcal{H}\left(Q_2, -\frac{r'}{r}\right)$

Siguiendo un razonamiento análogo al ya efectuado, se tiene:

Existe la homotecia $\mathcal{H}\left(Q_2, -\frac{r'}{r}\right)$ que transforma a la $C(O, r)$ en la $C(O', r')$.

Problema III

Dadas dos circunferencias concéntricas hallar, si existe, una homotecia que transforme una de ellas en la otra.



Sean $C(O, r)$ y $C(O', r')$ tales que $O = O'$ y $r \neq r'$.

Como en el caso anterior, si existe la homotecia, debe ser $k = \left|\frac{r'}{r}\right|$

Tomamos un punto cualquiera $P \in C(O,r)$ y trazamos la recta diametral que pase por P.

Dicha recta corta a $C(O', r')$ en P_1' y P_2'.

Se tiene:
$$\frac{\overline{O'P_1'}}{\overline{OP}} = \frac{r'}{r} \Rightarrow \overline{O'P_1'} = \frac{r'}{r}\overline{OP}$$
$$\frac{\overline{O'P_2'}}{\overline{OP}} = -\frac{r'}{r} \Rightarrow \overline{O'P_2'} = -\frac{r'}{r}\overline{OP}$$

O sea P_1' es homólogo de P en la homotecia $\mathcal{H}\left(O, \frac{r'}{r}\right)$

y P_2' es homólogo de P en la homotecia $\mathcal{H}\left(O, -\frac{r'}{r}\right)$

Luego: existen dos homotecias $\mathcal{H}\left(O, \frac{r'}{r}\right)$ y $\mathcal{H}\left(O, -\frac{r'}{r}\right)$ que transforman a la circunferencia $C(O, r)$ en la $C(C', r')$.

Resumen de los tres casos

Dadas dos circunferencias congruentes existe siempre una homotecia negativa ($k = -1$) que transforma una en la otra.

Dadas dos circunferencias de distinto radio existen dos homotecias, una negativa y otra positiva, de razón igual, en valor absoluto, al cociente de los radios.

Si las circunferencias son concéntricas, el centro de homotecia coincide con el centro común de las circunferencias.

Si las circunferencias no son concéntricas, el centro de homotecia pertenece a la recta determinada por los centros de dichas circunferencias.

Corolario

Si dos circunferencias admiten tangentes interiores comunes, éstas cortan a la recta de los centros en el centro de la homotecia negativa. Si existen tangentes exteriores comunes y éstas cortan a la recta de los centros, lo hacen en el centro de la homotecia positiva.

En efecto: si t_1 y t_2 son tangentes interiores comunes (ver figuras anteriores) cada una de ellas deja a las circunferencias en distintos semiplanos. Luego, los radios que pasan por los puntos de contacto de cada tangente con cada una de las circunferencias, además de pertenecer a rectas paralelas por ser perpendiculares a una misma recta, son de sentido contrario, es decir:

$$\frac{\overline{O'R'}}{\overline{OR}} = -\frac{r'}{r} \Rightarrow \overline{O'R'} = -\frac{r'}{r}\overline{OR}$$

O sea: $\mathcal{H}\left(Q_1, -\frac{r'}{r}\right) \cdot R = R'$ y por lo tanto $Q_1 \in RR'$ o bien $Q_1 \in t_1$.

Análogamente $Q_1 \in t_2$.

Luego: Q_1 es la intersección de las tangentes interiores comunes con la recta de los centros.

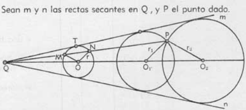
De la misma manera, se tiene:

Q_2 es la intersección de las tangentes exteriores comunes con la recta de los centros.

5. APLICACIONES

I.— *Construir una circunferencia que sea tangente a dos rectas secantes dadas y que pase por un punto dado no perteneciente a dichas rectas.*

Sean m y n las rectas secantes en Q, y P el punto dado.



Se traza una circunferencia $C(O, r) / O \in$ bisectriz del ángulo mn y E = distancias de O a m y n. Luego $C(O, r)$ es tangente a m y n.

La circunferencia pedida y la $C(O, r)$ serán homólogas en una homotecia positiva cuyo centro es la intersección de las tangentes exteriores comunes m y n.

Se traza PQ que corta a la $C(O, r)$ en M y N. Por P se traza la paralela a NO que corta a la bisectriz en O_1, y la paralela a MO que corta a la bisectriz en O_2.

Las circunferencias $C(O_1, \overline{O_1P})$ y $C(O_2, \overline{O_2P})$ son soluciones del problema.

En efecto, ambas pasan por P y demostraremos que son tangentes a m y n.

Consideremos la $C(O_1, \overline{O_1P})$.

$$\frac{\overline{O_1P}}{\overline{ON}} = \frac{r_1}{r} \Rightarrow \overline{O_1P} = \frac{r_1}{r} \cdot \overline{ON}$$

$r_1 \neq r$, pues si fuese $r_1 = r$ o sea $\overline{O_1P} = \overline{ON}$, y por ser de sostenes paralelos, serían paralelas NP y la bisectriz, contra lo establecido.

Luego la igualdad anterior expresa que O_1 y P son homólogos de O y de N, respectivamente, en una homotecia de razón $k \neq 1$ y cuyo centro es Q, intersección de NP con la bisectriz.

Resulta de inmediato que $C(O, r)$ y $C(O_1, \overline{O_1P})$ son homólogas en la $\mathscr{H}\left(Q, \frac{r_1}{r}\right)$.

Luego, si $\overline{OT}$ es el radio de sostén perpendicular a m en el punto de contacto, el radio homólogo, por ser paralelo a OT, es también perpendicular a m.

O sea, m es tangente a $C(O_1, \overline{O_1P})$

Análogamente se demuestra para n y para la otra circunferencia.

II. — *Construir una circunferencia que sea tangente a una circunferencia dada y a una recta dada en un punto dado de ésta.*

Sean la circunferencia $C(O, r)$, la recta m' y el punto $P' \in m'$.

La recta m' puede ser exterior, secante o tangente a la $C(O, r)$.

Consideraremos el caso en que m' es exterior.

Existen dos soluciones probables según que la circunferencia buscada sea tangente exterior o interiormente a la dada, pero en ambos casos dichas circunferencias deben pertenecer al semiplano con respecto a m' en el que se encuentra la circunferencia $C(O, r)$.

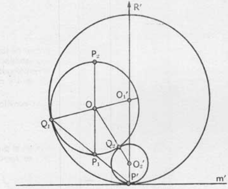
 Además, si deben ser tangentes a m' en P', sus respectivos centros O_1' y O_2' deben encontrarse sobre la perpendicular a m' que pase por P'. O sea, dichos centros pertenecerán a la semirrecta de origen P' trazada perpendicularmente a m' en el semiplano que contiene a $C(O , r)$.

Por otra parte, si la circunferencia buscada es tangente exterior (interiormente) a la $C(O , r)$, se sabe por propiedades de las circunferencias tangentes que existe una sola recta tangente interior (exterior) común a ambas que pasa por el punto de contacto de las mismas, punto que pertenece a su vez a la recta de los centros de las circunferencias.

Luego, por corolario anterior, dicho punto de contacto es el centro $Q_2(Q_1)$ de la homotecia negativa (positiva) que vincula a las circunferencias.

Por lo tanto, si se tienen Q_2 y Q_1, los puntos O_2' y O_1' estarán respectivamente sobre las rectas OQ_2 y OQ_1.

Resulta entonces la construcción siguiente:



a) En el semiplano con respecto a m' que contiene a $C(O , r)$, se traza $\overrightarrow{P'R'}$ / $P'R' \perp m'$.

b) Por O se traza la paralela a $P'R'$ que corta a $C(O , r)$ en P_1 y P_2. Sea $\overrightarrow{OP_2}$ la semirrecta acorde con $\overrightarrow{P'R'}$. Luego, $\overrightarrow{OP_1}$ y $\overrightarrow{P'R'}$ son discordes.

c) Se trazan P_1P' y P_2P', que cortan a $C(O , r)$ en Q_1 y Q_2 respectivamente.

d) Se trazan OQ_1 y OQ_2, que cortan a $P'R'$ en O_1' y O_2' respectivamente. Las circunferencias $C(O_1' , \overline{O_1'P'})$ y $C(O_2' , \overline{O_2'P'})$ son las circunferencias buscadas.

6. PRODUCTO DE DOS HOMOTECIAS

Sean dos homotecias $\mathcal{H}_1(O_1, k_1)$ y $\mathcal{H}_2(O_2, k_2)$ y un punto cualquiera M.

Si $\mathcal{H}_1(O_1, k_1) \cdot M = M_1$ y $\mathcal{H}_2(O_2, k_2) \cdot M_1 = M_2$,

estudiaremos la transformación $\mathcal{T}$ tal que: $\mathcal{T} \cdot M = M_2$

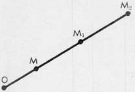
Se presentan dos casos según que los centros O_1 y O_2 coincidan o no.

Teorema

El producto de dos homotecias del mismo centro es otra homotecia del mismo centro y cuya razón es el producto de las razones de las homotecias dadas.

Sean las homotecias $\mathcal{H}_1(O, k_1)$ y $\mathcal{H}_2(O, k_2)$

Por definición de homotecia:



$$\begin{cases} \overline{OM_1} = k_1 \cdot \overline{OM} \\ M_1 \in OM \Rightarrow OM_1 = OM \end{cases}$$

$$y \begin{cases} \overline{OM_2} = k_2 \cdot \overline{OM_1} \\ M_2 \in OM_1 \Rightarrow OM_2 = OM_1 \end{cases}$$

O sea: $\overline{OM_2} = k_1 \cdot k_2 \cdot \overline{OM}$ y $OM_2 = OM$, es decir:

$$M_2 \in OM$$

Luego: M_2 es el transformado de M en una homotecia $\mathcal{H}(O, k_1 \cdot k_2)$.

O sea: $\mathcal{T} = \mathcal{H}_2 \cdot \mathcal{H}_1 = \mathcal{H}(O, k_1 \cdot k_2)$

Corolarios

I. — Si las homotecias $\mathcal{H}_1$ y $\mathcal{H}_2$ son inversas y sus centros coinciden, la transformación producto es la identidad.

En efecto, $k_1 \cdot k_2 = 1$

II. — El producto de dos homotecias del mismo centro es conmutativo.

En efecto, como k_1 y k_2 son números reales, $k_1 \cdot k_2 = k_2 \cdot k_1$

Luego:

$$\mathcal{T} = \mathcal{H}_2 \cdot \mathcal{H}_1 = \mathcal{H}_1 \cdot \mathcal{H}_2$$

Teorema

El producto de dos homotecias de distinto centro y razones no inversas es otra homotecia cuya razón es el producto de las razones dadas y cuyo centro está alineado con los centros de las homotecias dadas.

Sean dos puntos M y N y sus homólogos M_1 y N_1, respectivamente, en la homotecia $\mathcal{H}_1$, de centro O_1 y razón k_1. Luego:

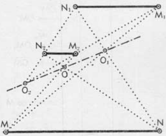
$$\overline{M_1N_1} = k_1 \cdot \overline{MN} \quad \text{y} \quad M_1N_1 \mathbin{/\!/} MN$$

Los homólogos de M_1 y N_1 en la homotecia $\mathcal{H}_2$ de centro O_2 y razón k_2, serán M_2 y N_2, respectivamente, tales que

$$\overline{M_2N_2} = k_2 \cdot \overline{M_1N_1} \quad \text{y} \quad M_2N_2 \mathbin{/\!/} M_1N_1$$

Por carácter transitivo de la igualdad de segmentos y del paralelismo de rectas, resulta:

$$\overline{M_2N_2} = k_1 \cdot k_2 \cdot \overline{MN} \quad \text{y} \quad M_2N_2 \mathbin{/\!/} MN$$



O sea M_2 y N_2 son homólogos de M y N en una homotecia de centro O y de razón $k = k_1 \cdot k_2$, tal que $k \neq 1$, pues las razones no son inversas.

Determinaremos el centro O.

Como la recta O_1O_2 pasa por el centro de la homotecia $\mathcal{H}_1$ es unida en esa transformación y por pasar por O_2, es unida en la homotecia $\mathcal{H}_2$

Es decir:

$$\mathcal{H}_1(O_1, k_1) \cdot O_1O_2 = O_1O_2 \text{ y}$$
$$\mathcal{H}_2(O_2, k_2) \cdot O_1O_2 = O_1O_2$$

Considerando la homotecia producto, se tiene:

$$\underbrace{\mathcal{H}_2(O_2, k_2) \cdot \mathcal{H}_1(O_1, k_1)}_{\mathcal{T} = \mathcal{H}(O, k)} \cdot O_1O_2 = O_1O_2$$

Lo cual expresa que O_1O_2 es unida en $\mathcal{H}$ de centro O y razón k, es decir es una recta que pasa por O. En efecto si no pasase por O, el homólogo de un punto cualquiera A de dicha recta, por ser ésta unida, debe pertenecer a la misma recta y además a la recta AO. Es decir el homólogo de A es el mismo punto, lo cual significa que A es unido. Esto es absurdo, pues se ha demostrado que el único punto unido en una homotecia es el centro.

Luego: O está alineado con O_1 y O_2.

Teorema

El producto de dos homotecias de distinto centro y razones inversas es una traslación.

Sean dos puntos M y N y sus homólogos M_1 y N_1 respectivamente en la $\mathcal{H}_1(O_1, k_1)$. Luego:

$$\overline{M_1N_1} = k_1 \cdot \overline{MN} \text{ y } M_1N_1 \parallel MN$$

Los homólogos de M_1 y N_1 en la $\mathcal{H}_2(O_2, k_2)$ serán M_2 y N_2, respectivamente, tales que

$$\overline{M_2N_2} = k_2 \cdot \overline{M_1N_1} \text{ y } M_2N_2 \parallel M_1N_1$$

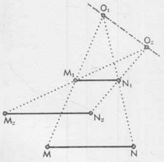
Por carácter transitivo de la igualdad de segmentos y del paralelismo de rectas, resulta:

$$\overline{M_2N_2} = k_1 \cdot k_2 \cdot \overline{MN} \text{ y } M_2N_2 \parallel MN$$

Pero $k_1 \cdot k_2 = 1$, pues las razones son inversas. Por lo tanto:

$$\overline{M_2N_2} = \overline{MN} \text{ y } M_2N_2 \parallel MN.$$

O sea $\overline{M_2N_2}$ y $\overline{MN}$ son homólogos en una traslación.



Como en el teorema anterior, se demuestra que siendo la recta de los centros unida en ambas homotecias, es unida también en la transformación producto, que en este caso es una traslación. Puesto que en toda traslación son unidas únicamente las rectas paralelas al vector de traslación, se tiene que:
La traslación producto es una traslación de vector paralelo a la recta de los centros de las homotecias dadas.

Corolario

Las homotecias de un plano no forman grupo.

EJERCICIOS

1. — *Dados una circunferencia y un punto perteneciente a una recta tangente a la misma, construir una circunferencia que sea tangente a ambas y pase por el punto. Discutir el número de soluciones posibles según que dicho punto coincida o no con el punto de contacto de la circunferencia y la recta dadas.*

2. — *Resolver el problema anterior en el caso en que la recta y la circunferencia dadas sean secantes.*

3. — *Dados una recta y un punto perteneciente a una circunferencia, construir una circunferencia que pase por el punto y sea tangente a la recta y a la circunferencia dadas.*

4. — *Construir un triángulo ABC conociendo el ángulo A, la razón* $\overline{AB}/\overline{AC} = k$ *y la mediana correspondiente al vértice A.*

5. — *Dado un triángulo ABC, la mediana* $\overline{AA'}$ *y un punto P de AA' se trazan por P las paralelas a los lados AB y AC que cortan a BC en Q y R, respectivamente. Demostrar que A' es el punto medio del segmento* $\overline{QR}$.

6. — *Sea un paralelogramo ABCD. Una recta que pasa por A corta a BC en E, a CD en F y a la diagonal BD en I. Demostrar que:*

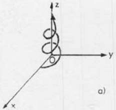
$$\overline{IA}^2 = \overline{IE} \cdot \overline{IF}$$

CAPITULO XVI

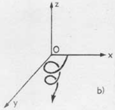
Aplicaciones vectoriales a la trigonometría

1. LAS DOS ORIENTACIONES DEL ESPACIO Y EL PRODUCTO VECTORIAL

Sea el espacio R^3 referido a una terna de origen O y ejes x, y, z, no necesariamente ortogonal. Dicha terna admite las siguientes representaciones usuales:



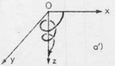
a)



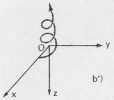
b)

En el caso a) decimos que la terna es positiva o derecha, y que el espacio está orientado positivamente. En b) está representada una terna negativa, y análogamente, el espacio tiene orientación negativa.

Consideremos ahora las ternas:



a')



b')

Las orientaciones de las ternas a') y b') son las mismas, respectivamente, que las representadas por a) y b). Para pasar de una terna positiva a una negativa o viceversa, es necesario deformar el triedro de referencia de modo tal que en una posición los tres ejes sean coplanares. En cambio, es posible pasar del caso a) al a') sin que ello ocurra.

Definición

Producto vectorial de dos vectores $\vec{A}$ y $\vec{B}$ es el vector indicado con el símbolo $\vec{A} \wedge \vec{B}$, caracterizado por las siguientes condiciones:

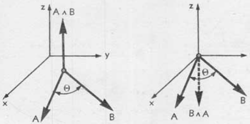
I) Su módulo es igual al producto de los módulos de los vectores dados por el seno del ángulo que determinan:

$$|\vec{A} \wedge \vec{B}| = |\vec{A}|\,|\vec{B}| \text{ sen } \Theta$$

II) Su dirección es normal al plano que determinan los vectores dados:

$$\textbf{dirección de } \vec{A} \wedge \vec{B} \perp \textbf{ plano } (\vec{A}, \vec{B})$$

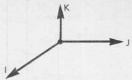
III) Su sentido es tal que la terna $\vec{A}, \vec{B}, \vec{A} \wedge \vec{B}$ tiene la misma orientación que la de referencia:



En los dos casos la orientación del espacio es positiva, y análogamente lo son las orientaciones de las ternas $\vec{A}, \vec{B}, \vec{A} \wedge \vec{B}$ y $\vec{B}, \vec{A}, \vec{B} \wedge \vec{A}$. Siendo los vectores $\vec{A} \wedge \vec{B}$ y $\vec{B} \wedge \vec{A}$, opuestos, ocurre que el producto vectorial no es conmutativo, y se lo llama por tal motivo, anticonmutativo, es decir:

$$\vec{A} \wedge \vec{B} = -\vec{B} \wedge \vec{A}$$

Sea la base ortonormal I, J, K; interesa determinar los seis productos vectoriales a que dan origen:



Aplicando en cada caso la definición, se tiene:

$I \wedge J = K$	$K \wedge K = I$	$K \wedge I = J$
$J \wedge I = -K$	$J \wedge J = -I$	$I \wedge K = -J$

2. DISTRIBUTIVIDAD DEL PRODUCTO VECTORIAL RESPECTO DE LA SUMA DE VECTORES

I) Producto mixto

Definición

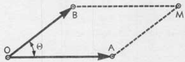
Se llama producto mixto de tres vectores $\vec{A}$, $\vec{B}$ y $\vec{C}$, al producto vectorial de los dos primeros, escalarmente por el tercero.

Usaremos la notación: $(\vec{A}\,\vec{B}\,\vec{C}) = (\vec{A} \wedge \vec{B}) \cdot \vec{C}$

II) Significado geométrico del módulo del producto vectorial

Sean los vectores $\vec{A}$ y $\vec{B}$. Por definición se tiene:

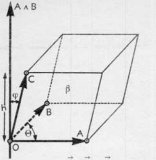
$$|\vec{A} \wedge \vec{B}| = |\vec{A}|\,|\vec{B}| \operatorname{sen} \Theta = 2 \cdot (\tfrac{1}{2} |\vec{A}|\,|\vec{B}| \operatorname{sen} \Theta) =$$
$$= 2 \cdot \text{Area}\,(A\overset{\triangle}{O}B) = \text{Area}\ A\overset{\square}{O}BM$$



Entonces:

El módulo del producto vectorial se identifica con el área del paralelogramo construido sobre los dos vectores dados.

III) Significado geométrico del producto mixto



Sean tres vectores $\vec{A}$, $\vec{B}$ y $\vec{C}$, que podemos suponer concurrentes en O, y no coplanares:

Por definición de producto escalar es:

$$(\vec{A} \wedge \vec{B}) \cdot \vec{C} = |\vec{A} \wedge \vec{B}|\,|\vec{C}| \cos \varphi$$

Teniendo en cuenta el significado del módulo del producto vectorial determinado en II), resulta, llamando β a la base del paralelepípedo cuyas aristas son los tres vectores dados:

$$(\vec{A} \wedge \vec{B}) \cdot \vec{C} = \text{Area}\,\beta \cdot |\vec{C}| \cos \varphi \qquad (1)$$

Considerando la perpendicular trazada por el extremo del vector $\vec{C}$, a la recta definida por $\vec{A} \wedge \vec{B}$, se obtiene la altura h del paralelepípedo, tal que

$$\text{med. } h = |\vec{C}| \cos \varphi \qquad (2)$$

Por sustitución de (2) en (1) es:

$$(\vec{A} \wedge \vec{B}) \cdot \vec{C} = \text{Area}\,\beta \cdot \text{med. } h = \text{med. } V$$

En consecuencia:

El producto mixto de tres vectores representa la medida del volumen del paralelepípedo cuyas aristas son dichos vectores.

IV) Propiedad invariante del producto mixto

Mediante consideraciones análogas a las del párrafo anterior, y teniendo en cuenta que las ternas, $\vec{A}$, $\vec{B}$, $\vec{C}$ y $\vec{B}$, $\vec{C}$, $\vec{A}$ son positivas, se llega al siguiente resultado:

$$(\vec{B} \wedge \vec{C}) \cdot \vec{A} = \text{med. } V$$

Por consiguiente, vale la igualdad:

$$(\vec{A} \wedge \vec{B}) \cdot \vec{C} = (\vec{B} \wedge \vec{C}) \cdot \vec{A} = (\vec{C} \wedge \vec{A}) \cdot \vec{B}$$

Es decir:

El doble producto mixto es invariante en las permutaciones cíclicas de sus elementos.

V) Distributividad del producto vectorial respecto de la suma de vectores

Se trata de demostrar la siguiente proposición:

$$(\vec{A}+\vec{B})\wedge\vec{C} = (\vec{A}\wedge\vec{C})+(\vec{B}\wedge\vec{C})$$

Para ello, consideramos el vector:

$$\vec{X} = (\vec{A}+\vec{B})\wedge\vec{C} - (\vec{A}\wedge\vec{C}) - (\vec{B}\wedge\vec{C}) \qquad (1)$$

Multiplicamos los dos miembros de (1) escalarmente por un vector $\vec{Y}\neq\vec{0}$ cualquiera, y teniendo en cuenta la distributividad del producto escalar respecto de la suma de vectores, se tiene:

$$\vec{X}\cdot\vec{Y} = [(\vec{A}+\vec{B})\wedge\vec{C}]\cdot\vec{Y} - (\vec{A}\wedge\vec{C})\cdot\vec{Y} - (\vec{B}\wedge\vec{C})\cdot\vec{Y}$$

Por la propiedad invariante del producto mixto, la igualdad anterior se transforma en:

$$\vec{X}\cdot\vec{Y} = (\vec{C}\wedge\vec{Y})\cdot(\vec{A}+\vec{B}) - (\vec{C}\wedge\vec{Y})\cdot\vec{A} - (\vec{C}\wedge\vec{Y})\cdot\vec{B}$$

Y por la misma distributividad del producto escalar respecto de la suma de vectores es:

$$\vec{X}\cdot\vec{Y} = (\vec{C}\wedge\vec{Y})\cdot[(\vec{A}+\vec{B}) - \vec{A} - \vec{B}]$$

Es decir:

$$\vec{X}\cdot\vec{Y} = (\vec{C}\wedge\vec{Y})\cdot\vec{0} = 0$$

Siendo nulo el producto escalar $\vec{X}\cdot\vec{Y}$ para todo $\vec{Y}$, resulta necesariamente $\vec{X}=\vec{0}$. Entonces, el vector definido en (1) es nulo, y por consiguiente:

$$(\vec{A}+\vec{B})\wedge\vec{C} = (\vec{A}\wedge\vec{C})+(\vec{B}\wedge\vec{C})$$

3. EXPRESIÓN CANÓNICA DEL PRODUCTO VECTORIAL

Sean los vectores de R^3:

$$\vec{A} = a_x I + a_y J + a_z K \qquad (1)$$

$$\vec{B} = b_x I + b_y J + b_z K \qquad (2)$$

Al efectuar el producto vectorial de $\vec{A}$ por $\vec{B}$, la distributividad del producto vectorial respecto de la suma de vectores nos autoriza a multiplicar ordenadamente cada término del primero por todos los términos del segundo, y se tiene:

$$\begin{aligned}\vec{A}\wedge\vec{B} &= a_xb_x\,(I\wedge I) + a_xb_y\,(I\wedge J) + a_xb_z\,(I\wedge K) + \\ &+ a_yb_x\,(J\wedge I) + a_yb_y\,(J\wedge J) + a_yb_z\,(J\wedge K) + \\ &+ a_zb_x\,(K\wedge I) + a_zb_y\,(K\wedge J) + a_zb_z\,(K\wedge K)\end{aligned}$$

Teniendo en cuenta los productos vectoriales de los versores fundamentales, es:

$$\vec{A} \wedge \vec{B} = a_x b_y K - a_x b_z J - a_y b_x K + a_y b_z I + a_z b_x J - a_z b_y I \qquad (3)$$

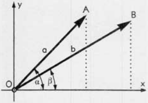
El segundo miembro de (3) es el desarrollo del determinante que tiene como primera fila a los versores fundamentales; como segunda y tercera, a las componentes de los vectores (1) y (2), respectivamente.

Entonces, resulta:

$$\vec{A} \wedge \vec{B} = \begin{vmatrix} I & J & K \\ a_x & a_y & a_z \\ b_x & b_y & b_z \end{vmatrix}$$

El determinante así obtenido, nos da la expresión canónica del producto vectorial.

4. COSENO DE LA SUMA Y DE LA DIFERENCIA DE DOS ÁNGULOS



Sean dos vectores $\vec{A}$ y $\vec{B}$, de módulos a y b, respectivamente, que podemos suponer aplicados en el origen de un sistema ortogonal.

El eje x forma con dichos vectores, los ángulos α y β. Sean: a_x y a_y las componentes de $\vec{A}$; y b_x y b_y, las de $\vec{B}$.

El ángulo de los vectores es $\alpha - \beta$.

Efectuamos el producto escalar de $\vec{A}$ y $\vec{B}$, de dos maneras:

$$\vec{A} \cdot \vec{B} = a_x b_x + a_y b_y$$

(1) en función de las componentes.

$$\vec{A} \cdot \vec{B} = a \cdot b \cdot \cos(\alpha - \beta)$$

(2) en función de los módulos y del ángulo comprendido.

De (1) y (2) resulta:

$$a \cdot b \cdot \cos(\alpha - \beta) = a_x b_x + a_y b_y$$

Trasponiendo los factores a y b:

$$\cos(\alpha - \beta) = \frac{a_x}{a} \cdot \frac{b_x}{b} + \frac{a_y}{a} \cdot \frac{b_y}{b}$$

Por definición de seno y coseno, resulta:

$$\mathbf{\cos(\alpha - \beta) = \cos\alpha \cdot \cos\beta + sen\,\alpha \cdot sen\,\beta}$$

Para obtener la fórmula relativa al coseno de la suma de dos ángulos, reducimos el problema al caso anterior, del siguiente modo:

Por coseno de la diferencia, se tiene:

$$\cos(\alpha + \beta) = \cos \alpha \cos(-\beta) + \operatorname{sen} \alpha \operatorname{sen}(-\beta)$$

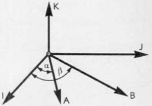
y reduciendo al primer cuadrante, resulta:

$$\mathbf{cos}(\alpha + \beta) = \mathbf{cos}\, \alpha \cdot \mathbf{cos}\, \beta - \mathbf{sen}\, \alpha \cdot \mathbf{sen}\, \beta$$

5. SENO DE LA DIFERENCIA Y DE LA SUMA DE DOS ÁNGULOS

Sean en R^2 los vectores:

$$\vec{A} = a_x I + a_y J$$
$$\vec{B} = b_x I + b_y J$$



Su producto vectorial es:

$$\vec{A} \wedge \vec{B} = \begin{vmatrix} I & J & K \\ a_x & a_y & 0 \\ b_x & b_y & 0 \end{vmatrix}$$

Al desarrollar subsiste sólo la componente respecto de K, y se tiene:

$$\vec{A} \wedge \vec{B} = (a_x b_y - a_y b_x) \cdot K$$

De acuerdo con la figura, este producto vectorial tiene el sentido de K, lo cual significa que su componente es positiva. Entonces:

$$|\vec{A} \wedge \vec{B}| = a_x b_y - a_y b_x \qquad (1)$$

Por otra parte, atendiendo a la definición de módulo del producto vectorial, es:

$$|\vec{A} \wedge \vec{B}| = a \cdot b \cdot \operatorname{sen}(\beta - \alpha) \qquad (2)$$

De (1) y (2) resulta:

$$a \cdot b \cdot \operatorname{sen}(\beta - \alpha) = a_x b_y - a_y b_x$$

multiplicando los dos miembros por -1, se tiene:

$$-a \cdot b \cdot \operatorname{sen}(\beta - \alpha) = a_y b_x - a_x b_y$$

Y por relaciones entre las funciones de ángulos simétricos, podemos escribir:

$$a \cdot b \cdot \operatorname{sen}(\alpha - \beta) = a_y b_x - a_x b_y$$

trasponiendo factores:

$$\operatorname{sen}(\alpha-\beta)=\frac{a_y}{a}\cdot\frac{b_x}{b}-\frac{a_x}{a}\cdot\frac{b_y}{b}$$

Por definición de seno y de coseno, resulta:

$$\mathbf{sen}\,(\alpha-\beta)=\mathbf{sen}\,\alpha\cdot\mathbf{cos}\,\beta-\mathbf{cos}\,\alpha\cdot\mathbf{sen}\,\beta$$

Siguiendo un criterio análogo al expuesto en el párrafo anterior, deducimos la fórmula relativa al seno de la suma de dos ángulos, previa transformación de la misma en diferencia:

$$\operatorname{sen}(\alpha+\beta)=\operatorname{sen}[\alpha-(-\beta)]$$

Por seno de la diferencia, se tiene:

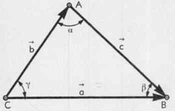
$$\operatorname{sen}(\alpha+\beta)=\operatorname{sen}\alpha\cos(-\beta)-\cos\alpha\cdot\operatorname{sen}(-\beta)$$

Por reducción al primer cuadrante, resulta:

$$\mathbf{sen}\,(\alpha+\beta)=\mathbf{sen}\,\alpha\cdot\mathbf{cos}\,\beta+\mathbf{cos}\,\alpha\cdot\mathbf{sen}\,\beta$$

6. TEOREMA DEL SENO

En todo triángulo, los lados son proporcionales a los senos de los ángulos opuestos.



Hipótesis) ABC triángulo

Tesis) $\dfrac{a}{\operatorname{sen}\alpha}=\dfrac{b}{\operatorname{sen}\beta}=\dfrac{c}{\operatorname{sen}\gamma}$

Demostración:

Sea el triángulo ABC representado por la figura adjunta, y cuyos lados son los vectores $\vec{a}$, $\vec{b}$ y $\vec{c}$ de módulos: a, b y c respectivamente.

Por suma de vectores, es: $\vec{a}=\vec{b}+\vec{c}$

multiplicamos vectorialmente los dos miembros de esta igualdad por $\vec{b}$:

$$\vec{a}\wedge\vec{b}=(\vec{b}+\vec{c})\wedge\vec{b}$$

por distributividad del producto vectorial respecto de la suma de vectores:

$$\vec{a}\wedge\vec{b}=\vec{b}\wedge\vec{b}+\vec{c}\wedge\vec{b}\qquad(1)$$

 pero $\vec{b}\wedge\vec{b}$ es el vector nulo, pues el ángulo que forman es nulo.

La igualdad (1) se reduce entonces a:

$$\vec{a} \wedge \vec{b} = \vec{c} \wedge \vec{b}$$

siendo iguales los vectores de ambos miembros, sus módulos también lo son:

$$|\vec{a} \wedge \vec{b}| = |\vec{c} \wedge \vec{b}|$$

Por definición de módulo del producto vectorial, tenemos:

$$a \cdot b \cdot \operatorname{sen} \gamma = c \cdot b \cdot \operatorname{sen} \alpha$$

cancelando el factor b :

$$a \cdot \operatorname{sen} \gamma = c \cdot \operatorname{sen} \alpha$$

por trasposición de factores resulta:

$$\frac{a}{\operatorname{sen} \alpha} = \frac{c}{\operatorname{sen} \gamma} \qquad (2)$$

Si se multiplican los dos miembros de la igualdad:

$$\vec{a} = \vec{b} + \vec{c}$$

vectorialmente por $\vec{c}$, se llega a un resultado análogo que vincula a los lados a y b con los senos de sus ángulos opuestos:

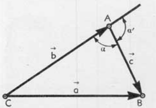
$$\frac{a}{\operatorname{sen} \alpha} = \frac{b}{\operatorname{sen} \beta} \qquad (3)$$

Aplicando la transitividad a las relaciones (2) y (3), resulta

$$\frac{a}{\operatorname{sen} \alpha} = \frac{b}{\operatorname{sen} \beta} = \frac{c}{\operatorname{sen} \gamma}$$

7. TEOREMA DEL COSENO

En todo triángulo, el cuadrado de cada lado es igual a la suma de los cuadrados de los otros dos, menos el doble producto de los mismos por el coseno del ángulo opuesto al primero.



Hipótesis) ABC triángulo

Tesis) $a^2 = b^2 + c^2 - 2\,bc \cos \alpha$

Demostración) Por suma de vectores es

$$\vec{a} = \vec{b} + \vec{c}$$

Elevando al cuadrado los dos miembros de la igualdad:

$$\vec{a}^{\,2} = (\vec{b} + \vec{c})^2$$

Por distributividad del producto escalar:

$$\vec{a}^2 = \vec{b}^2 + \vec{c}^2 + 2 \cdot \vec{c} \cdot \vec{b}$$

Por definición de producto escalar, se tiene:

$$a^2 = b^2 + c^2 + 2\, b \cdot c \cdot \cos\alpha' \qquad (1)$$

El ángulo formado por los vectores $\vec{b}$ y $\vec{c}$ es α', adyacente a α; esto significa que:

$$\cos\alpha' = \cos(180^\circ - \alpha) = -\cos\alpha \qquad (2)$$

El teorema queda demostrado al sustituir (2) en (1):

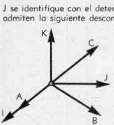
$$a^2 = b^2 + c^2 - 2 \cdot b \cdot c \cdot \cos\alpha$$

8. DOBLE PRODUCTO VECTORIAL

El producto vectorial de dos vectores, vectorialmente por un tercero, está dado por la fórmula:

$$(\vec{A} \wedge \vec{B}) \wedge \vec{C} = (\vec{A} \cdot \vec{C})\, \vec{B} - (\vec{B} \cdot \vec{C})\, \vec{A}$$

Sin restringir la generalidad, elegimos la terna de versores fundamentales de modo que I tenga la dirección de $\vec{A}$; y que el plano I, J se identifique con el determinado por $\vec{A}$ y $\vec{B}$. En tal caso, $\vec{A}$, $\vec{B}$ y $\vec{C}$ admiten la siguiente descomposición canónica:



$$\vec{A} = a_x I \qquad (1)$$

$$\vec{B} = b_x I + b_y J \qquad (2)$$

$$\vec{C} = c_x I + c_y J + c_z K \qquad (3)$$

De (1) y (2) se tiene:

$$\vec{A} \wedge \vec{B} = \begin{vmatrix} I & J & K \\ a_x & 0 & 0 \\ b_x & b_y & 0 \end{vmatrix} = a_x b_y K \qquad (4)$$

De (3) y (4) se deduce:

$$(\vec{A} \wedge \vec{B}) \wedge \vec{C} = (a_x b_y K) \wedge \vec{C} = a_x b_y (K \wedge \vec{C}) = a_x b_y \begin{vmatrix} I & J & K \\ 0 & 0 & 1 \\ c_x & c_y & c_z \end{vmatrix} =$$

$$= a_x b_y (-c_y I + c_x J) = -a_x b_y c_y I + a_x b_y c_x J \qquad (5)$$

Determinamos ahora:

$$(\vec{A} \cdot \vec{C})\, \vec{B} - (\vec{B} \cdot \vec{C})\, \vec{A} = a_x c_x (b_x I + b_y J) - (b_x c_x + b_y c_y)\, a_x I =$$

$$= -a_x b_y c_y I + a_x b_y c_x J \qquad (6)$$

De (5) y (6) resulta la fórmula

$$(\vec{A} \wedge \vec{B}) \wedge \vec{C} = (\vec{A} \cdot \vec{C})\,\vec{B} - (\vec{B} \cdot \vec{C})\,\vec{A}$$

9. PRODUCTO ESCALAR DE DOS PRODUCTOS VECTORIALES

Sea $\vec{A} \wedge \vec{B} = \vec{X}$ (1)

Entonces

$$(\vec{A} \wedge \vec{B}) \cdot (\vec{C} \wedge \vec{D}) = \vec{X} \cdot (\vec{C} \wedge \vec{D}) = (\vec{C} \wedge \vec{D}) \cdot \vec{X} = (\vec{C}\,\vec{D}\,\vec{X}) = (\vec{X}\,\vec{C}\,\vec{D}) =$$

$$= (\vec{X} \wedge \vec{C}) \cdot \vec{D} \quad (2)$$

De (1) y (2) resulta, luego de efectuar el doble producto vectorial:

$$(\vec{A} \wedge \vec{B}) \cdot (\vec{C} \wedge \vec{D}) = [(\vec{A} \wedge \vec{B}) \wedge \vec{C}] \cdot \vec{D} = [(\vec{A} \cdot \vec{C})\vec{B} - (\vec{B} \cdot \vec{C})\,\vec{A}] \cdot \vec{D}$$

Por distributividad del producto escalar, se tiene:

$$(\vec{A} \wedge \vec{B}) \cdot (\vec{C} \wedge \vec{D}) = (\vec{A} \cdot \vec{C})\,(\vec{B} \cdot \vec{D}) - (\vec{B} \cdot \vec{C})(\vec{A} \cdot \vec{D})$$

10. TEOREMA DEL COSENO PARA LOS LADOS DE UN TRIÁNGULO ESFÉRICO

Sea el triángulo esférico ABC determinado por los extremos de tres versores aplicados en el origen de un sistema.

Por producto escalar de dos productos vectoriales, tenemos:

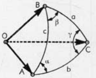
$$(\vec{A} \wedge \vec{B}) \cdot (\vec{A} \wedge \vec{C}) = (\vec{A} \cdot \vec{A})(\vec{B} \cdot \vec{C}) - (\vec{A} \cdot \vec{C})(\vec{B} \cdot \vec{A}) \quad (1)$$

Por producto escalar y módulo del producto vectorial es:

$$(\vec{A} \wedge \vec{B}) \cdot (\vec{A} \wedge \vec{C}) = |\vec{A} \wedge \vec{B}|\,|\vec{A} \wedge \vec{C}| \cos \alpha = \operatorname{sen} c \cdot \operatorname{sen} b \cdot \cos \alpha \quad (2)$$

siendo α el ángulo de los planos $\vec{A}$, $\vec{B}$ y $\vec{A}$, $\vec{C}$, es decir, el diedro de arista OA.

Por otra parte, el segundo miembro de (1) es:



$$(\vec{A} \cdot \vec{A})(\vec{B} \cdot \vec{C}) - (\vec{A} \cdot \vec{C})(\vec{B} \cdot \vec{A}) =$$
$$= \cos a - \cos b \cdot \cos c \quad (3)$$

De (2) y (3) resulta:

$$\cos a - \cos b \cdot \cos c = \operatorname{sen} b \cdot \operatorname{sen} c \cdot \cos \alpha$$

Es decir:

$$\cos a = \cos b \cdot \cos c + \operatorname{sen} b \cdot \operatorname{sen} c \cdot \cos \alpha$$

Entonces:

En todo triángulo esférico, el coseno de un lado es igual a la suma de los cosenos de los otros dos, más el producto de sus senos, por el coseno del ángulo opuesto al primero.

EJERCICIOS

1. — *En todo paralelogramo, la suma de los cuadrados de sus diagonales es igual a la suma de los cuadrados de sus lados.*

2. — *El polígono cuyos vértices son los puntos medios de los lados de un cuadrilátero, es un paralelogramo.*

3. — *Estudiar el significado geométrico de la igualdad:*

$$\vec{X} \cdot \vec{Y} = \vec{X} \cdot \vec{Z}$$

4. — *Demostrar que*

$$P_B\vec{A} = \frac{\vec{A} \cdot \vec{B}}{|\vec{B}|}$$

siendo $P_B \vec{A}$ *la proyección del vector* $\vec{A}$ *sobre* $\vec{B}$.

5. — *Los vectores* $\vec{A}$ *y* $\vec{B}$ *forman un ángulo de 60°, siendo el módulo de* $\vec{A}$ *igual a 5. Hallar el módulo de* $\vec{B}$ *para que sea* $\vec{A}$ *perpendicular a la diferencia* $\vec{A} - \vec{B}$.

6. — *Los vectores* $\vec{A}$ *y* $\vec{B}$ *forman un ángulo de 120° y el módulo de* $\vec{A}$ *es 3. Hallar el módulo de* $\vec{B}$ *para que se verifique la ortogonalidad de los vectores* $\vec{A} + \vec{B}$ *y* $\vec{B}$.

ÍNDICE ALFABÉTICO

Adición de números enteros 141
— — — naturales 131
— — polinomios 255
— en los sistemas de numeración 271, 272
Álgebra de Boole 119
Altura de una ecuación 162
Ángulo de dos vectores 249
— — paralelismo 221
Anillo 99
— conmutativo 99
— de enteros 259
— — polinomios 257
Anillos de integridad 102, 103
Aplicación 44, 54
— biyectiva 57
— inyectiva 57
— sobre 56
— suryectiva 56
— uno a uno 57
Asociativa, Ley externa 81
— — interna 68
Axioma 115, 116
— de paralelismo 216
Axiomática 115
— de Hilbert 180

Base canónica 236
— de un espacio vectorial 109
— — — sistema de numeración. 263
— media 248
— ortonormal 246
Beltrami 227
Bicondicional 9
Bolyai 215
Boole 119
Buena ordenación 53

Cambio de base 237
— — — en sistemas de numeración 275, 276, 277
Cancelativa, Ley 72
Cardinal 128, 134, 136, 154
Categoricidad 125
Cifras de un sistema 263
Clase de equivalencia 45
Clasificación de aplicaciones 44
Coeficiente 254
Colineación 197
Combinación lineal de vectores .. 108
Compatibilidad 121, 122, 217
Completicidad 124
Composición de aplicaciones 76
— — sustituciones 96
Compuesto 63
Condición necesaria y suficiente .. 8
Condicional 7
Conectivos lógicos 4
Congruencia 45, 215
Conjunción 4
Conjunto cerrado 64
— cociente 45
— de llegada 40
— — los números enteros . 139, 147
— — — naturales 137
— — partida 40
— definido por comprensión 21
— — — extensión 20
— finito 134, 152
— numerable 154, 156
— unitario 23
— universal o referencial 23
— vacío 22
Conjuntos coordinables 135, 151
— especiales 22
— disjuntos 29
Conmutativa, Ley 70
Consistencia 121
Contradicción 10
Contradominio 41
Coordenadas de un vector .. 110, 111
Correspondencia 54
Coseno de la suma y diferencia .. 304
Cuantificadores 14
Cuerpo 105
— conmutativo 105
Cupla 33, 41
Curvatura 227

Definición implícita 115
— por abstracción 50, 182
Definiciones 116, 181
Dependencia lineal 235
Desigualdad de Schwartz 244
Diagonal de un producto cartesiano 36
Diagramas de Venn 26
Diferencia de conjuntos 30
— simétrica 30

Dimensión de un espacio 179
— — — — vectorial 110
Dirección 50
Distancia 245
Distributiva, Ley externa 80
— — interna 71
Disyunción 5
Doble implicación 9
— producto vectorial 308
Dominio 41, 54
— de integridad 104

Ecuación vectorial de la recta ... 240
Elemento de un conjunto 19
— neutro 72
— regular 75
— simétrico 73
Elementos de Euclides 170, 171, 180
— negativos 98
— positivos 98
Endomorfismo 84
Entero racional, entero relativo o entero 139
Enteros positivo, negativo y nulo 140, 141
Equipolencia de vectores 239
Equipotencia 135
Equivalencia 45
— de sistemas axiomáticos 120
— teorema fundamental 49
Espacio abstracto 179
— físico 178, 231
— intuitivo 178
— multidimensional 179, 180
— vectorial de polinomios 254
Espacios vectoriales 107
Estructura 85, 89
— del conjunto de los números enteros 147, 148
— — — — — naturales ... 137
Estructuras geométricas 187, 201, 211
Euclides 169, 215
Expresión cifrada 268
— formal inversa 267, 268

Familia de partes de un conjunto 27
— libre de vectores 108
Formas polinómicas 267

Función 44, 54
— inversa 58
— proposicional 14
Fundamentación axiomática del número natural 128, 133
— del número natural por teoría de conjuntos 134

Gauss 217, 220
Geometría 200, 201
— absoluta 174, 216, 219
— afín 208
— analítica 217
— de Euclides 215
— — Lobatchefsky 222
— — posición 212, 213
— — Riemann 228
— elíptica 229, 230
— esférica 228
— hiperbólica 223, 230
— métrica euclidiana 209
— parabólica 230
— proyectiva 208
— — superior 212
Geometrías no euclidianas 215
Giros 189
Grado de un polinomio 254
Gráfico de una función 55, 58
— — — relación 42
Grupo 89
— conmutativo o abeliano 90
— finito 93
— fundamental 194, 195
— proyectivo 197
— simétrico a n variables .. 96, 97
Grupoide 97

Hilbert 180, 217
Hiperespacio 180
Hiperplano 180
Homeomorfismo 213
Homomorfismo 82, 259
Homotecia 191, 279
Hungtinton 119

Igualdad de conjuntos 25
— — cuplas 34
Imagen 41
Implicación 7

Implicaciones asociadas 11
Inclusión de conjuntos 24
Independencia 122
Indeterminada 253
Integridad 124
Intersección de conjuntos 28
Intervalo natural 151
Inversión en el plano 226
Isomorfismo 85

Ley asociativa 68, 81
— cancelativa 72
— conmutativa 70
— distributiva 71, 80
— estable 65
— externa 78
— inducida 67
— interna 63
— lógica 10
Leyes algebraicas 63
— de De Morgan 32
Lobatchefsky .. 215, 217, 221, 222

Matemática aplicada 117
— pura 116
Matrices columna 233
Método genético para la construcción de enteros 138
— matemático 115
Metodología de las estructuras geométricas 203, 210
Modelo 116
Módulo de la suma 245
— — un vector 243
Monoidé 97
Monomio 254
Movimientos geométricos 191
— — directos 189
— — inversos 190

Multiplicación de números enteros 143
— — — naturales 132
— en los sistemas de numeración 273
N - upla 35
Negación 6
No contradicción 116, 121
Norma de un vector 243

Número algebraico 160
— cardinal 153
— entero 50, 138
— natural 128
— racional 60
— trascendente 161, 163
Números cardinales .. 128, 134, 136
— ordinales 128

Operaciones en los sistemas de numeración 271
— entre conjuntos 27
— — números naturales ... 131, 132, 133, 136
Orden 51
— amplio 51
— estricto 52
— lineal 53
— parcial 52
— total 52
Ordenación perfecta 134
Ordinal 128, 136

Par ordenado 33, 40
Paralelismo 216, 220, 221
— hiperbólico 222, 226
Partición 48
Permutaciones 93
Plano afín 239, 242
Poincaré 223
Polinomio 253
Postulado V de Euclides ... 174, 216
Potencia de los racionales 158
— — — reales 159
— del conjunto de las funciones reales 164
— — — de los números algebraicos 162
— — continuo 160
Principio de inducción completa .. 130
— — Klein 203, 204
— — permanencia de las leyes formales 137
Producto cartesiano 35
— de homotecias 294
— — dos productos vectoriales . 309
— — polinomios 257

— escalar de dos vectores . 242, 243
— mixto 301, 302
— vectorial de dos vectores 300
Propiedad lineal 44
Proposición 4
Proyecciones 195
— de vector 110, 111
— — una cupla 34
Pseudoesfera 227

Raíz de un polinomio 260
Rango 41
Recorrido 41, 54
Rectas paralelas 241
Reflexividad 43
Relación a - reflexiva 43
— a - simétrica 44
— a - transitiva 44
— antisimétrica 44
— binaria 39
— conexa 44
— inversa 42
— n - aria 43
— no - reflexiva 43
— no - simétrica 44
— no - transitiva 44
— ternaria 39
Relaciones entre conjuntos 24
Riemann 228, 230
Rotaciones 189

Saccheri 175, 220
Saturación 124
Secciones 196
Seno de la suma y diferencia 305
Silogismo 14, 116
Simetría 44
— axial 190
— central 190
Simétrico 73
Sistema axiomático 117
— — de Peano 128
— binario 263, 277
— de Peano 128
Sistemas axiomáticos para el número natural 128, 133
— de numeración 263
Suma de polinomios 255

Subanillos 102
Subcuerpos 106
Subgrupo 97
Sustitución 259
— idéntica 95
Sustituciones 94
Sustracción de números enteros 145, 146

Tablas de adición y multiplicación 273
Tautología 10
Teorema de Pitágoras 247
— — las tres perpendiculares . . 249
— del coseno en triángulos esféricos 309
— — — — planos 307
— — seno 306
— fundamental de equivalencia . 49
— — la numeración 265
Teoremas 116
Tercero excluido 116
Término independiente 254
— primitivo 115
Tipos de conjuntos 20
Topología 212, 213
Tractoide 227
Tractriz 227
Transformación 54
— bicontinua 213
— conforme 284
— idéntica 192
Transformaciones equivalentes . . . 192
— geométricas 187, 188
— involutivas 193
— métricas 188
— proyectivas 195
Transitividad 44
Traslaciones 188
Tricotomía 44

Unión de conjuntos 29

Vector 108
— fijo 239
— libre 239
Vectores linealmente independientes 108
— ortogonales 246