

ALGEBRA

para física

Ernesto F. GANDOLFO RASO

01/09/2010

Tabla de contenido

Estructura algebraica	8
Principales estructuras algebraicas	8
Operación matemática	8
Operación interna	8
1) Operación unaria	9
2) Operaciones binarias	9
3) Operación externa	10
Magma o Grupoide	11
Definiciones	11
Más Definiciones	12
No asociatividad	12
Más ejemplos	13
Categoría de Magmas (Mag)	14
Semigrupo	15
Ejemplo	15
Monoide	16
Ejemplos	16
Concatenación de cadenas alfanuméricas	16
Multiplicación de números naturales	17
En la teoría de categorías	18
Bibliografía	18
Referencias	18
Grupo	19
Definición	19
Notación	20
Tipos de grupos	20
Ejemplos	21
Curiosidades	22
Grupo cíclico	22
Propiedades	23
Subgrupos	24
Grupo lineal	24
Grupo lineal del espacio euclídeo	24
Propiedades del grupo lineal	24
Grupo de Lie	25

Tipos de grupos de Lie	25
Homomorfismos e isomorfismos	25
El álgebra de Lie asociada a un grupo de Lie	25
Lista de algunos grupos de Lie reales y de sus álgebras de Lie	27
Lista de algunos grupos de Lie complejos y de sus álgebras de Lie	29
Álgebra de Lie	30
Definición	30
Ejemplos	31
Homomorfismos, subálgebras e ideales	31
Clasificación de las álgebras de Lie	32
Álgebra de Lie ortogonal generalizada	32
Super álgebra de Lie	34
E8	34
Descripción básica	35
Formas reales	35
Teoría de las representaciones	35
Representaciones	36
Construcciones	36
Geometría	36
En física	37
Diagrama de Dynkin	37
Sistema de raíces	37
Matriz de Cartan	38
Algunas cifras a partir del cálculo de E_8	39
Notas y referencias	39
Politopo E8	39
Referencias	40
Una teoría del todo excepcionalmente simple	42
Panorama global	43
Nuevas partículas	44
Recepción	44
Referencias	46
Grupo uniparamétrico	46
Grupo uniparamétrico global	46
Ejemplo	47
Grupos uniparamétricos locales	47

Grupos uniparamétricos en grupos de Lie.....	47
Grupos uniparamétricos en física.....	47
Teorema de Noether.....	48
Operadores unitarios en mecánica cuántica.....	48
Grupo abeliano	48
Notación	48
Ejemplos	49
Propiedades	49
Anillo	49
Ejemplo de un anillo	49
Definición formal	50
Elementos destacados en un anillo	51
Algunos tipos importantes de anillos	51
Subconjuntos notables	52
Subanillos e ideales	52
Unidades	53
Centro	53
Anillo conmutativo.....	53
Ejemplos.....	53
Cuerpo	54
Definición	54
Cuerpo de escalares	55
Subcuerpos e ideales	55
Propiedades de los cuerpos	56
Ejemplos de cuerpos	56
Algunos teoremas iniciales	58
Construyendo nuevos cuerpos de otros dados	58
Módulo	58
Definición	58
Ejemplos	59
Submódulos y homomorfismos	59
Tipos de módulos	60
Definición alternativa como representaciones	60
Generalizaciones	61
Referencias	61
Espacio vectorial	62

Definición de espacio vectorial	62
Observación	63
Definición de subespacio vectorial	63
Consecuencias	63
Primer ejemplo con demostración al detalle	64
Representación de espacios vectoriales	64
Propiedades del espacio vectorial.	67
Historia	67
Ejemplos	68
Espacios de coordenadas y de funciones	68
Ecuaciones lineales	69
Teoría de números algebraicos	69
Bases y dimensión	69
Aplicaciones lineales y matrices	70
Matrices	71
Vectores y valores propios	72
Construcciones básicas	72
Espacios vectoriales con estructura adicional	73
Espacios vectoriales normados y espacios prehilbertianos	73
Espacios vectoriales topológicos	73
Espacio de Banach	74
Definición	74
Ejemplos	74
Operadores lineales	75
Espacio dual	75
Relación con espacios de Hilbert	75
Derivada de Fréchet	76
Generalizaciones	77
Espacio de Hilbert	77
Introducción	77
Ejemplos	78
Espacios euclideos	78
Espacios de sucesiones	79
Espacios de Lebesgue	79
Espacios de Sobolev	80
Bases ortonormales	80

Operaciones en los espacios de Hilbert.....	81
Suma directa y producto tensorial.....	81
Complementos y proyecciones ortogonales.....	81
Reflexividad.....	82
Operadores en espacios de Hilbert.....	82
Operadores acotados.....	82
Operadores no acotados.....	83
Referencias.....	83
Citas.....	83
Referencias.....	84
Referencias históricas.....	84
Subespacio vectorial.....	84
Definición.....	84
Condición de existencia de subespacio.....	84
Operaciones con subespacios.....	85
Unión.....	85
Intersección.....	85
Suma.....	85
Dimensiones de subespacios.....	86
Referencias.....	86
Álgebra sobre un cuerpo.....	87
Definiciones.....	87
Características.....	87
Clases de álgebra y ejemplos.....	88
Álgebras asociativas.....	88
Álgebras no asociativas.....	89
Más clases de álgebra.....	89
Álgebra de Clifford.....	90
Definición formal.....	90
Representaciones de álgebras de Clifford.....	91
Representaciones matriciales de las álgebras reales de Clifford.....	92
El sistema "K" para nombrar matrices.....	92
Álgebra de Clifford real $R_{2,0}$	94
Álgebra de Clifford real $R_{1,1}$	95
Álgebra de Clifford real $R_{2,1}$	95
Álgebra de Clifford real $R_{0,2}$	96

Álgebra de Clifford real $R_{0,3}$	97
Álgebra de Clifford real $R_{3,0}$	98
Álgebra de Clifford real $R_{3,1}$	98
Álgebra geométrica	100
Sistema numérico	101
Definición	101
Ejemplos notables	101
Los conjuntos forman un sistema numérico	101
Los restos de módulo 2	103
Bibliografía	104

Estructura algebraica

En la matemática, una **estructura algebraica** es una n -tupla (a_1, a_2, \dots, a_n) , donde a_1 es un conjunto dado no vacío, y $\{a_2, \dots, a_n\}$ un conjunto de operaciones aplicables a los elementos de dicho conjunto.

Principales estructuras algebraicas

Las estructuras algebraicas se clasifican según las propiedades que cumplen las operaciones sobre el conjunto dado. En estructuras algebraicas más elaboradas, se definen además varias leyes de composición interna.

- Magma
- Semigrupo
- Monoide
- Grupo
- Grupo abeliano
- Anillo
- Pseudoanillo
- Cuerpo
- Módulo
- Espacio vectorial
- Álgebra
- Sistema numérico

Operación matemática

En matemática una **operación matemática** es la acción de un operador sobre los elementos de un conjunto. El operador toma los elementos iniciales y los relaciona con otro elemento de un conjunto final que puede ser de la misma naturaleza o no; esto se conoce técnicamente como ley de composición.

El conjunto de partida puede estar formado por elementos de un único tipo (las operaciones aritméticas actúan sólo sobre números) o de varios (el producto de un vector por un escalar engloba al conjunto unión de vectores y escalares que conforman un espacio vectorial).

Dependiendo de cómo sean los conjuntos implicados en la operación con respecto al conjunto considerado principal según nuestras intenciones podemos clasificar las operaciones en dos tipos: internas y externas.

Operación interna

Es la operación en la que, tanto en sus elementos iniciales como en su resultado, sólo interviene un conjunto A único.

$$f : A \times A \times A \times \dots \times A \rightarrow A$$

de n argumentos.

Que también puede expresarse:

$$(a_1, a_2, a_3, \dots, a_n) \xrightarrow{\circ} b$$

O también:

$$\circ(a_1, a_2, a_3, \dots, a_n) \rightarrow b$$

Por el número de términos de la operación podemos diferenciar:

1) Operación unaria

Operación unaria, con un solo parámetro:

$$f : A \rightarrow A$$

también suelen denominarse funciones. Vamos unos ejemplos:

Dado el conjunto de los números naturales \mathbf{N} , definimos la operación unaria incremento, como la operación que para cada número natural n calcula el siguiente:

$$in(n) = n + 1$$

Partiendo de los números enteros \mathbf{Z} , la operación opuesto determina para cada número entero e su opuesto;

$$op(e) = -e$$

2) Operaciones binarias

La operación binaria es un caso muy importante, cuando n es igual a dos, que se representa:

$$f : A \times A \rightarrow A$$

y también:

$$\begin{array}{l} a \circ b \xrightarrow{\circ} c \\ (a, b) \xrightarrow{\circ} c \\ \circ(a, b) \rightarrow c \end{array}$$

Ejemplos

En el conjunto de los números naturales, \mathbf{N} , la operación de adición: $+$, $(N, +)$, se expresa:

1. $(+ : \mathbf{N} \times \mathbf{N} \longrightarrow \mathbf{N})$
2. $a, b \in \mathbf{N}, \quad a + b \rightarrow c$
3. $a, b \in \mathbf{N}, \quad (a, b) \xrightarrow{+} c$

$$4. \quad a, b \in \mathbb{N}, \quad +(a, b) \rightarrow c$$

Como operaciones binarias, donde a y b son los sumandos y c el resultado de la suma.

3) Operación externa

Una ley de composición externa sobre un conjunto A con un conjunto B es una aplicación:

$$f : B \times A \longrightarrow A$$

esta aplicación se dice que es una operación externa.

Ejemplo: Dado el conjunto V_2 de los vectores en el plano y el conjunto de escalares \mathbb{R} de números reales, tenemos que el producto de un número real por un vector en el plano es un vector en el plano:

$$\cdot : \mathbb{R} \times V_2 \longrightarrow V_2$$

Dado el vector:

$$3i + 6j$$

Si lo multiplicamos por un escalar 3:

$$3 \cdot (3i + 6j) \longrightarrow (9i + 18j)$$

Podemos ver que los dos vectores son del plano:

$$(3i + 6j), (9i + 18j) \in V_2$$

Partiendo de los conjuntos A y B distintos, y una aplicación:

$$f : A \times A \longrightarrow B$$

se dice que también es una ley de composición externa. Por ejemplo el Producto escalar de dos vectores en el plano, da como resultado un número real, esto es:

$$\circ : V_2 \times V_2 \longrightarrow \mathbb{R}$$

Tomando los vectores del plano:

$$\begin{aligned} \vec{u} &= (x_1, y_1) \\ \vec{v} &= (x_2, y_2) \end{aligned}$$

Y siendo su producto escalar:

$$\vec{u} \circ \vec{v} = (x_1, y_1) \circ (x_2, y_2) = x_1 \cdot x_2 + y_1 \cdot y_2$$

Que da por resultado un número real, veamos un ejemplo numérico:

$$\begin{aligned}\vec{u} &= (3, 6) \\ \vec{v} &= (5, 2)\end{aligned}$$

Operando

$$\vec{u} \circ \vec{v} = (3, 6) \circ (5, 2) = 3 \cdot 5 + 6 \cdot 2 = 15 + 12 = 27$$

Magma o Grupoide

Un **Magma** (o grupoide) es una estructura algebraica de la forma (A, \circ) donde **A** es un conjunto **no vacío**, donde se ha definido una ley de composición interna binaria \circ .

$$A \circ A \rightarrow A$$

Siendo esta ley de composición una operación interna:

1.- Operación interna: para cualesquiera par ordenado de elementos del conjunto **A x A** operados con \circ , el resultado pertenece al conjunto **A**. Es decir:

$$\forall x, y \in A : \quad x \circ y \in A.$$

El término **magma** se debe a la asociación de matemáticos franceses que se hace llamar Nicolás Bourbaki. Durante algún tiempo compitió, para reflejar el mismo concepto, con la palabra **grupoide**, que tiene otros sentidos en matemática (ver artículo grupoide), por lo que no es aconsejable su uso como sinónimo de magma.

Definiciones

Los tipos de magmas comúnmente estudiados incluyen:

- **Cuasigrupos** : Magmas no vacíos donde la división es siempre posible.
- **Grafos**: Cuasigrupos con elementos neutros.
- **Semigrupos**: Magmas donde la operación es asociativa.
- **Monoides**: Semigrupos con elemento neutro.
- **Grupos**: Monoides con elementos simétricos, o equivalentemente, cuasigrupos asociativos (que son siempre loops).
- **Grupos abelianos**: Grupos donde la operación es conmutativa.

El término "magma" fue introducido por Bourbaki. Anteriormente se usaba el término "grupoide", y todavía se utiliza a veces. En esta enciclopedia, no obstante, reservamos el término grupoide para un concepto algebraico diferente.

Existe lo que podemos llamar un **magma libre** sobre cualquier conjunto **X** y que puede ser descrito en términos familiares en ciencias de la computación como el magma de los árboles binarios con operación dada por la yuxtaposición (ordenada) de los árboles por la raíz. Tiene por tanto un rol fundacional en sintaxis.

Más Definiciones

Un magma se denomina:

- Medial si satisface la identidad $xy.uz = xu.yz$ (i.e. $(x*y)*(u*z) = (x*u)*(y*z)$)
- Semimedial izquierdo si satisface la identidad $xx.yz = xy.xz$
- Semimedial derecho si satisface la identidad $yz.xx = yx.zx$
- Semimedial si es, a la vez, semimedial izquierdo y derecho.
- Distributivo izquierdo si satisface la identidad $x.yz = xy.xz$
- Distributivo derecho si satisface la identidad $yz.x = yx.zx$
- Autodistributivo si es, a la vez, distributivo izquierdo y derecho.
- Conmutativo si satisface $xy = yx$
- Idempotente si satisface $xx = x$
- Unipotente si satisface $xx = yy$
- Zeropotente si satisface $xx.y = yy.x = xx$
- Alternativa si satisface $xx.y = x.xy$ & $x.yy = xy.y$
- Un semigrupo si satisface $x.yz = xy.z$ (asociatividad).
- Un **semigrupo con zeros izquierdos** o **elementos cancelativos izquierdos** si satisface $x = xy$.
- Un **semigrupo con zeros derechos** o **elementos cancelativos derechos** si satisface $x = yx$.
- Un **semigrupo con multiplicación nula** si satisface $xy = uv$.
- Entrópico si es imagen homomórfica de un magma cancelativo.

No asociatividad

Una operación binaria $*$ en un conjunto S que no satisfaga la ley asociativa se llama **no-asociativa**. Simbólicamente,

$$(x * y) * z \neq x * (y * z) \quad \text{para algunos } x, y, z \in S$$

para tal operación el orden de la evaluación importa. La substracción y la división de números reales son ejemplos bien conocidos de operaciones no-asociativas:

$$\left. \begin{aligned} (x - y) - z &\neq x - (y - z) \\ (x/y)/z &\neq x/(y/z) \end{aligned} \right\} \text{ para algunos } x, y, z \in \mathbb{R}$$

En general, se deben utilizar paréntesis para indicar el orden de la evaluación si aparece una operación no-asociativa más de una vez en una expresión. Sin embargo, los matemáticos convienen en una orden particular de la evaluación para varias operaciones no-asociativas comunes. Esto tiene el estatus de una convención, no de una verdad matemática. Una operación izquierdo-asociable se evalúa convencionalmente de izquierda a derecha, es decir,

$$\left. \begin{aligned} x * y * z &= (x * y) * z \\ w * x * y * z &= ((w * x) * y) * z \\ \text{etc.} \end{aligned} \right\} \text{ para todo } w, x, y, z \in S$$

mientras que una operación derecho-asociable se evalúa convencionalmente de derecha a izquierda:

$$\left. \begin{array}{l} x * y * z = x * (y * z) \\ w * x * y * z = w * (x * (y * z)) \\ \text{etc.} \end{array} \right\} \text{ para todo } w, x, y, z \in S$$

Las operaciones izquierdo-asociables y derecho-asociables ocurren; los ejemplos se dan abajo.

Más ejemplos

Las operaciones izquierdo-asociables incluyen las siguientes.

- Substracción y división de números reales:

$$\begin{array}{ll} x - y - z = (x - y) - z & \text{para todo } x, y, z \in \mathbb{R}; \\ x/y/z = (x/y)/z & \text{para todo } x, y, z \in \mathbb{R} \text{ con } y \neq 0, z \neq 0. \end{array}$$

Las operaciones derecho-asociables incluyen la siguiente.

- Exponenciación de números reales:

$$x^{y^z} = x^{(y^z)}.$$

La razón por la que la exponenciación es derecho-asociable es que una operación izquierdo-asociable repetida del exponente sería menos útil. Múltiples apariciones se podrían reescribir con la multiplicación:

$$(x^y)^z = x^{(yz)}$$

- El operador de asignación en muchos lenguajes de programación es derecho-asociable.

Por ejemplo, en el lenguaje C

$$x = y = z; \text{ significa } x = (y = z); \text{ y no } (x = y) = z$$

Es decir la declaración asignaría el valor de z a ambos x e y .

Las operaciones no-asociativas para las cuales no se define ningún orden convencional de la evaluación incluyen el siguiente.

- Tomar el promedio de números reales:

$$\frac{(x + y)/2 + z}{2} \neq \frac{x + (y + z)/2}{2} \neq \frac{x + y + z}{3} \quad \text{para algunos } x, y, z \in \mathbb{R}.$$

- Tomar el complemento relativo de conjuntos:

$$(A \setminus B) \setminus C \neq A \setminus (B \setminus C) \quad \text{para algunos conjuntos } A, B, C.$$

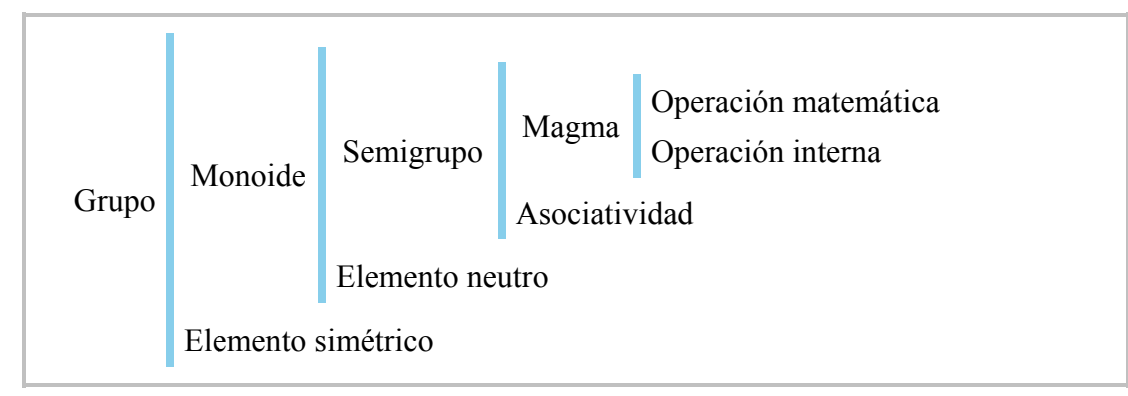
nota: invito a la comunidad matemática interesada a que por favor coloquen ejemplos de los diferentes magmas

Categoría de Magmas (Mag)

En matemática, la **categoría de magmas** (ver categoría, magma para definiciones), notada **Mag**, tiene por objetos conjuntos con una operación binaria, y morfismos dados por homomorfismos de las operaciones (en el sentido del álgebra universal).

La categoría *Mag* tiene producto directo por tanto el concepto de objeto (auto) magma tiene sentido.

Una propiedad muy importante es que un endomorfismo inyectivo puede ser extendido a un automorfismo de un magma extensión, simplemente el colímite de la sucesión constante del endomorfismo.



Semigrupo

Un **semigrupo** es una estructura algebraica de la forma (A, \circ) donde A es un conjunto donde se ha definido una ley de composición interna binaria \circ . Un semigrupo cumple las siguientes propiedades:

1.- Operación interna: para cualesquiera dos elementos del conjunto **A** operados bajo \circ , el resultado siempre pertenece al mismo semigrupo **A**. Es decir:

$$\forall x, y \in A : \quad x \circ y \in A.$$

2.- Asociatividad: para cualesquiera elementos del conjunto **A** no importa el orden en que se operen las parejas de elementos, mientras no se cambie el orden de los elementos (ver grupo abeliano), siempre dará el mismo resultado. Es decir:

$$\forall x, y, z \in A : \quad x \circ (y \circ z) = (x \circ y) \circ z.$$

Si además se cumple la propiedad conmutativa:

Conmutatividad: un conjunto **A** tiene la propiedad conmutativa respecto a la operación interna \circ si:

$$\forall a, b \in A : \quad a \circ b = b \circ a$$

Se dice que es un semigrupo conmutativo o abeliano.

Ejemplo

Un ejemplo de semigrupo conmutativo es el conjunto de los números naturales: \mathbb{N} con la operación suma: $+$. Que se representa: $(\mathbb{N}, +)$, podemos ver:

Que cumple la clausura, dado que la suma de dos números naturales es otro número natural:

$$\forall a, b \in \mathbb{N} : \quad a + b \in \mathbb{N}.$$

Que es asociativa:

$$\forall a, b, c \in \mathbb{N} : \quad (a + b) + c = a + (b + c).$$

Y conmutativa:

$$\forall a, b \in \mathbb{N} : \quad a + b = b + a.$$

Luego $(\mathbb{N}, +)$ es semigrupo conmutativo o abeliano.

Monoide

El **monoide** es una estructura algebraica (A, \circ) , donde A es un conjunto, y \circ una operación binaria que cumple:

1.- Operación interna: para cualesquiera dos elementos del conjunto A operados bajo \circ , el resultado siempre pertenece al mismo semigrupo A . Es decir:

$$\forall x, y \in A : \quad x \circ y \in A.$$

2.- Asociatividad: para cualesquiera elementos del conjunto A no importa el orden en que se operen las parejas de elementos, mientras no se cambie el orden de los elementos (ver grupo abeliano), siempre dará el mismo resultado. Es decir:

$$\forall x, y, z \in A : \quad x \circ (y \circ z) = (x \circ y) \circ z$$

3.- Con Elemento neutro para todo elemento x que pertenezca al conjunto A , existe un único elemento e de A , que cumple:

$$\forall x \in A : \quad \exists! e : \quad e \circ x = x \circ e = x$$

En esencia, un monoide es un semigrupo con elemento neutro.

Si además se cumple la propiedad conmutativa:

Conmutatividad: un conjunto A tiene la propiedad conmutativa respecto a la operación interna \circ si:

$$\forall a, b \in A : \quad a \circ b = b \circ a$$

Se dice que es un monoide conmutativo o abeliano.

Ejemplos

Concatenación de cadenas alfanuméricas

Definimos el conjunto A de las cadenas alfanuméricas, cada una de las cuales es una secuencia de letras y números de cualquier longitud, que representaremos:

$$\langle abcd \rangle$$
$$\langle aju73fr5 \rangle$$

La cadena vacía, la que no tiene ningún carácter, sería:

$$\langle \rangle$$

Definimos la operación \parallel de concatenación de cadenas de caracteres:

$$A \parallel A \rightarrow A$$

que podemos representar, de las siguientes formas:

- $\langle asd \rangle \parallel \langle rfv \rangle \rightarrow \langle asdrfv \rangle$
- $\langle 1234 \rangle \parallel \langle ju \rangle \rightarrow \langle 1234ju \rangle$

Podemos ver que (A, \parallel) tiene estructura algebraica de monoide:

1.- Es una operación interna: para cualesquiera dos cadenas su concatenación es una cadena alfanumérica:

$$\forall a, b \in A : a \parallel b \in A$$

2.- Es asociativa:

$$\forall a, b, c \in A : a \parallel (b \parallel c) = (a \parallel b) \parallel c$$

3.- Tiene elemento neutro: para todo elemento a cadena de caracteres, existe la cadena vacía $\langle \rangle$ de A , de modo:

$$\forall a \in A : \exists \langle \rangle : \langle \rangle \parallel a = a \parallel \langle \rangle = a$$

La concatenación de cadenas de caracteres no es conmutativa:

$$\forall a, b \in A : a \parallel b \neq b \parallel a$$

Por lo que (A, \parallel) tiene estructura algebraica de monoide, no conmutativo.

Multiplicación de números naturales

Partiendo del conjunto de los números naturales:

$$N = \{1, 2, 3, 4, \dots\}$$

y la operación multiplicación, podemos ver que: (N, \times) es un monoide

1.- Es una operación interna: para cualquiera dos números naturales su multiplicación es un número natural:

$$\forall a, b \in N : a \times b \in N$$

2.- Es asociativa:

$$\forall a, b, c \in N : \quad a \times (b \times c) = (a \times b) \times c$$

3.- Tiene elemento neutro: para todo elemento **a** número natural, existe el **1** en **N**, que cumple:

$$\forall a \in N : \quad \exists 1 : \quad 1 \times a = a \times 1 = a$$

4.- La multiplicación de números naturales es conmutativa:

$$\forall a, b \in A : \quad a \times b = b \times a$$

El conjunto de los números naturales, bajo la operación multiplicación: (N, \times) , tiene estructura algebraica de monoide conmutativo o abeliano.

En la teoría de categorías

Una categoría monoidal, es una categoría con una operación binaria que convierte a la categoría en un monoide. Dos ejemplos:

1. La categoría de conjuntos con la unión disjunta de conjuntos y el conjunto vacío como elemento neutro.
2. La categoría **Vect** \mathbb{K} de los espacios vectoriales sobre un campo \mathbb{K} junto con el producto tensorial de espacios vectoriales y a \mathbb{K} como el elemento neutro.

Bibliografía

1. Gutiérrez Gómez, Andrés; García Castro, Fernando (en español). *Álgebra lineal* (2 edición). Ediciones Pirámide, S.A.. ISBN 978-84-368-0174-3.

Referencias

- Adler, Irving (1970). *La Nueva Matemática*. Buenos Aires: Editorial Universitaria de Buenos Aires, Colección Ciencia Joven, 288 páginas, en rústica. Traducción del inglés: Jorge Jáuregui. Original: The New Mathematics, The John Day Company, New York.
- Birkhoff, Garrett; MacLane, Saunders (1963). *Álgebra Moderna*. Barcelona: Editorial Vicens-Vives.

Grupo

En álgebra abstracta, un **grupo** es un conjunto en el que se define una operación binaria (i.e. un magma), que satisface ciertos axiomas detallados más abajo. La rama de la matemática que estudia los grupos se llama teoría de grupos.

Definición

Sea una estructura algebraica formada por un conjunto A , sobre cuyos elementos se ha definido una operación o ley de composición interna binaria denotada por " \circ ". Se dice que la estructura (A, \circ) es un **grupo** con respecto a la operación \circ si satisface las siguientes propiedades:

1. Operación interna: para cualesquiera dos elementos del conjunto A operados bajo \circ , el resultado siempre pertenece al mismo semigrupo A . Es decir:

$$\forall x, y \in A : \quad x \circ y \in A$$

2. Asociatividad: para cualesquiera elementos del conjunto A no importa el orden en que se operen las parejas de elementos, mientras no se cambie el orden de los elementos (ver grupo abeliano), siempre dará el mismo resultado. Es decir:

$$\forall x, y, z \in A : \quad x \circ (y \circ z) = (x \circ y) \circ z$$

3. Con elemento neutro. Para todo elemento x que pertenezca al conjunto A , existe un único elemento e de A , que cumple:

$$\forall x \in A : \exists ! e : e \circ x = x \circ e = x$$

4. Con elemento simétrico respecto de la operación \circ , si se cumple:

$$\forall x \in A, \exists \bar{x} \in A : \bar{x} \circ x = x \circ \bar{x} = e$$

Si además se cumple la propiedad conmutativa:

1. Conmutatividad: un conjunto A tiene la propiedad conmutativa respecto a la operación interna \circ si:

$$\forall a, b \in A : a \circ b = b \circ a$$

Se dice que es un grupo conmutativo o abeliano.

Notación

Es frecuente utilizar a la hora de definir grupos dos notaciones:

- La notación multiplicativa.
 - Operación: $*$, llamada producto. También escrita como \cdot .
 - Elemento neutro: 1 .
 - Elemento inverso: x^{-1} .
 - Como en la multiplicación normal, el signo \cdot puede en muchas ocasiones no ser escrito, es decir: $a \cdot b = ab$.
- La notación aditiva.
 - Operación: $+$, llamada suma.
 - Elemento neutro: 0 .
 - Elemento opuesto de un elemento x del grupo: $-x$.

Históricamente la terminología multiplicativa precedió a la aditiva. La operación de grupo no es necesariamente una adición o una multiplicación en el sentido que nos resulta familiar en la aritmética elemental. Por ejemplo, una operación de grupo puede ser una sustitución o una rotación. Cualquier conjunto de elementos y una operación que a dos elementos asocie una tercera en el conjunto, puede ser un grupo si cumple con las condiciones o propiedades de grupo pedidas. Sus elementos no son siempre números en el sentido ordinario de la aritmética elemental. Asimismo en algunos casos puede ser más cómodo utilizar alguna de las dos notaciones y en otros resulta indiferente. Es posible que se utilicen indistintamente, siempre y cuando esto no mueva a confusión. Cuando se trata de las operaciones familiares de suma y multiplicación, es impropio usar una notación opuesta a la operación.

Tipos de grupos

- **Grupo abeliano (o conmutativo).** Se denomina grupo conmutativo o abeliano a aquel grupo que verifica la Propiedad conmutativa, es decir $a \cdot b = b \cdot a \forall a, b \in G$
 - **Grupo abeliano con torsión** Definición de torsión: Diremos que un elemento $a \in A$ posee **torsión** o, que es **de torsión**, si para algún $n \in \mathbb{N}$, $a^n = 1$. Si a es

de torsión, entonces el menor número natural n con la propiedad $a^n = 1$, coincide con el orden de a . Definición de grupo abeliano con torsión: Un grupo abeliano A se dice **con torsión** si es igual a 0 o si posee elementos no nulos de torsión.

- **Grupo abeliano de torsión.** Un grupo abeliano A se dice de torsión si todo elemento de A es de torsión.
- **Grupo finito.** Es un grupo con un número finito de elementos.
- **Grupo de Lie.** Es un grupo que además tiene estructura de variedad diferenciable.
- **Grupo cíclico.** Es un grupo conmutativo, finito o infinito, que puede ser generado por multiplicación reiterada de un sólo elemento.
- **Grupo libre.**
- **Grupos de Klein.**

Ejemplos

- La suma define estructura de grupo conmutativo en el conjunto de los números enteros (\mathbb{Z}), en el de los números racionales (\mathbb{Q}), en los números reales (\mathbb{R}) y en los números complejos (\mathbb{C}). Los vectores libres del espacio, con la suma de vectores, forman un grupo conmutativo. La suma de matrices define una estructura de grupo conmutativo en las matrices con coeficientes reales (digamos) con un número de columnas y filas prefijado. Las funciones reales de variable real, con la suma de funciones, también forman un grupo conmutativo, al igual que las sucesiones de números reales con la suma de sucesiones.
- El producto define estructura de grupo conmutativo en los números racionales no nulos, los números reales positivos, los números complejos de módulo 1, etc.
- Las matrices cuadradas de n columnas con coeficientes reales y determinante distinto de cero forman un grupo con el producto de matrices, grupo que no es conmutativo cuando $n > 1$.

Otros ejemplos de grupos no conmutativos se obtienen al considerar grupos de transformaciones, donde la operación es la composición de aplicaciones y el elemento neutro es la identidad:

- El grupo de los movimientos del espacio o grupo de isometría del espacio euclídeo, el grupo de las semejanzas del plano o el grupo de las afinidades de una recta (las aplicaciones de la forma $x \mapsto ax+b$ con a distinto de cero).
- El grupo de Galileo, formado por las transformaciones del espacio y el tiempo que conservan los sistemas de referencia inerciales).
- El grupo de Lorentz de la teoría de la relatividad, etc.

Todos estos últimos ejemplos lo son del concepto de Grupo de Lie, que son los grupos definidos por operaciones continuas sobre curvas superficies o variedades de dimensión mayor.

La importancia crucial de la teoría de grupos tanto en Física como en Matemática radica en que los isomorfismos de cualquier estructura, de cualquier teoría, forman siempre un grupo y que, en los casos más importantes, los grupos están clasificados: se conocen listas que agotan todos los que hay. La clasificación de los grupos de Lie, llevada a cabo esencialmente por Élie Cartan, es un punto culminante de la matemática europea, sólo comparable a la construcción de los 5 poliedros regulares realizada por la matemática griega. Al igual que ésta última es la determinación de todas las figuras geométricas simétricas posibles, la clasificación de grupos es la determinación de todas las posibles simetrías de cualquier estructura. Así, podemos conocer *a priori* los grupos de automorfismos de

cualquier teoría geométrica. Además, de acuerdo con el *Programa de Erlangen* de Felix Klein, este grupo de automorfismos reconstruye la correspondiente teoría geométrica.

Algo parecido sucede en Física, donde se ha descubierto que el grupo de simetrías del lagrangiano de un sistema determina propiedades fundamentales asociadas a las partículas elementales de dicho sistema. De hecho, aunque aún no conozcamos las teorías físicas por venir, la clasificación de grupos de Lie ya nos proporciona la lista de los posibles grupos de simetrías infinitesimales.

Curiosidades

Un grupo puede tener infinitos elementos, (como \mathbf{Z} con la suma, o los números reales no nulos con el producto) o por el contrario tener un número finito de éstos.

Dado un número natural n , los restos que se obtienen al dividir por n (es decir, los números $0, 1, \dots, n - 1$) forman un grupo, donde la suma $a + b$ es precisamente el resto al dividir la suma ordinaria por n . Este grupo se denota con $\mathbf{Z}/n\mathbf{Z}$ y se suele llamar grupo de enteros módulo n . Así, el grupo $\mathbf{Z}/12\mathbf{Z}$ es el que usamos para calcular con las horas de un reloj, y $\mathbf{Z}/24\mathbf{Z}$ si queremos distinguir las horas de la mañana de la tarde.

Además, en $\mathbf{Z}/n\mathbf{Z}$ el conjunto de los números primos relativos con n (denotado $(\mathbf{Z}/n\mathbf{Z})^*$) forma un grupo cuando la operación ab es el resto al dividir por n el producto usual. Sin embargo, se puede definir un grupo para otros números aunque no sean primos. Por ejemplo, el grupo $(\mathbf{Z}/12\mathbf{Z})^*$ el cual sólo tiene 4 elementos. ¿Por qué sólo 4 elementos? Porque puesto que para ser un grupo, cada elemento ha de tener un inverso. Si tomamos algún número que tenga algún factor común con 12, por ejemplo el 10, éste no puede ser multiplicado por otro número de forma que el resto de la división entre 12 sea 1. Es decir, 10 no tendría inverso. Así, sólo son elementos del grupo $(\mathbf{Z}/12\mathbf{Z})^*$ aquellos números co-primos con 12. Si n hubiese sido primo, todos los menores que él serían co-primos con él, excepto el cero, luego su grupo tendría $n - 1$ elementos.

Se dice que un grupo es **cíclico** si verifica estar generado por un solo elemento; es decir, supongamos que un conjunto A es grupo con respecto a una operación $*$. Si existe un elemento g en A tal que cualquier otro elemento de A se obtiene operando g o su inverso g^{-1} reiteradamente:

$$A = \{ \dots, g^{-r}, \dots, g^{-1}, g^0 = 1, g^1 = g, g^2, \dots, g^r, \dots \} = \{ g^r \mid r \in \mathbf{Z} \},$$

entonces se dice que $(A, *)$ es un grupo cíclico y que g es un generador de A , lo cual se denota por $A = \langle g \rangle$.

La clasificación de grupos cíclicos afirma que los finitos son isomorfos a $\mathbf{Z}/n\mathbf{Z}$, y los infinitos con \mathbf{Z} .

Grupo cíclico

En teoría de grupos, un **grupo cíclico** es un grupo que puede ser generado por un solo elemento; es decir, hay un elemento a del grupo G (llamado "generador" de G), tal que todo elemento de G puede ser expresado como una potencia de a . Si la operación del grupo se denota aditivamente, se dirá que todo elemento de G se puede expresar como na , para n entero.

En otras palabras, G es cíclico, con generador a , si $G = \{ a^n \mid n \in \mathbf{Z} \}$. Dado que un grupo generado por un elemento de G es, en sí mismo, un subgrupo de G , basta con demostrar que el único subgrupo de G que contiene a a es el mismo G para probar que éste es cíclico.

Por ejemplo, $G = \{ e, g^1, g^2, g^3, g^4, g^5 \}$ es cíclico. De hecho, G es esencialmente igual (esto es, isomorfo) al grupo $\{ 0, 1, 2, 3, 4, 5 \}$ bajo la operación de suma módulo 6. El isomorfismo se puede hallar fácilmente haciendo $g \rightarrow 1$.

Contrariamente a lo que sugiere la palabra "cíclico", es posible generar infinitos elementos y no formar nunca un ciclo real: es decir, que cada g^n sea distinto. Un tal grupo sería un **grupo cíclico infinito**, isomorfo al grupo \mathbf{Z} de los enteros bajo la adición.

Salvo isomorfismos, existe exactamente un grupo cíclico para cada cantidad finita de elementos, y exactamente un grupo cíclico infinito. Por lo anterior, los grupos cíclicos son de algún modo los más simples, y han sido completamente clasificados.

Por esto, los grupos cíclicos normalmente se denotan simplemente por el grupo "canónico" al que son isomorfos: si el grupo es de orden n , para n entero, dicho grupo es el grupo \mathbf{Z}_n de enteros $\{ 0, \dots, n-1 \}$ bajo la adición módulo n . Si es infinito, éste es, como cabe esperarse, \mathbf{Z} .

La notación \mathbf{Z}_n comúnmente es evitada por teoristas de los números, puesto que puede ser confundida con la notación usual para los números p -ádicos. Una alternativa es usar la notación de grupo cociente, $\mathbf{Z}/n\mathbf{Z}$; otra posible solución es denotar la operación multiplicativamente, y representar el grupo $C_n = \{ e, a^1, a^2, \dots, a^{n-1} \}$. Empero, estas dos notaciones no son tan populares como \mathbf{Z}_n .

Propiedades

Por lo dicho ya en la introducción, todo grupo cíclico es isomorfo a \mathbf{Z}_n , o bien, a \mathbf{Z} . Basta entonces con examinar dichos grupos para entender los grupos cíclicos en general. Dado un grupo cíclico G de orden n (donde n puede valer infinito), y dado $g \in G$, se tiene:

- G es abeliano; es decir, su operación es conmutativa: $ab = ba$ para cualesquiera a y $b \in G$. Esto es cierto, puesto que cualquier par de enteros a y b , $a + b \text{ mód } n = b + a \text{ mód } n$.
- Si $n < \infty$, entonces $g^n = e$, puesto que $n \text{ mód } n = 0$.
- Si $n = \infty$, entonces el grupo tiene exactamente dos generadores: 1 y -1 en \mathbf{Z} , y sus imágenes isomórficas en otros grupos cíclicos infinitos.
- Todo subgrupo de G es cíclico. De hecho, para n finito, todo subgrupo de G es isomorfo a un \mathbf{Z}_m , donde m es divisor de n ; y si n es infinito, todo subgrupo de G corresponderá a un subgrupo $m\mathbf{Z}$ de \mathbf{Z} (el cual es también isomorfo a \mathbf{Z}), bajo el isomorfismo entre G y \mathbf{Z} .

Los generadores de \mathbf{Z}_n son los enteros que son primos relativos con n . El número de tales generadores se designa por $\phi(n)$, donde ϕ designa la función ϕ de Euler. En general, si d es un divisor de n , el número de elementos de \mathbf{Z}_n de orden d es $\phi(d)$. El orden del elemento m es $n / \text{mcd}(m, n)$.

Si p es primo, el único grupo con p elementos (salvo isomorfismos) es \mathbf{Z}_p .

El producto directo de dos grupos cíclicos \mathbf{Z}_n y \mathbf{Z}_m es cíclico si y solo si m y n son primos entre sí; en tal caso, el grupo obtenido será isomorfo a \mathbf{Z}_{nm} . Por ejemplo, \mathbf{Z}_{12} es isomorfo a $\mathbf{Z}_3 \times \mathbf{Z}_4$, pero no a $\mathbf{Z}_6 \times \mathbf{Z}_2$.

El teorema fundamental de los grupos abelianos afirma que todo grupo abeliano finitamente generado es isomorfo al producto directo de un número finito de grupos cíclicos.

\mathbf{Z}_n y \mathbf{Z} son también anillos conmutativos. Si n es un número primo, \mathbf{Z}_n es un cuerpo finito, también denotado por \mathbf{F}_n o $\mathbf{GF}(n)$. Cualquier otro cuerpo con n elementos es isomorfo al ya descrito.

Subgrupos

Todos los subgrupos y grupos cocientes de un grupo cíclico son, a su vez, cíclicos. En particular, los subgrupos de \mathbf{Z} son de la forma $m\mathbf{Z}$ donde $m \geq 0$ es un número entero. Todos éstos son diferentes, y salvo por el grupo trivial (con $m=0$) son todos isomorfos a \mathbf{Z} . El retículo de subgrupos de \mathbf{Z} es isomorfo al dual del retículo de números naturales ordenados por divisibilidad. Todos los grupos cocientes de \mathbf{Z} son finitos, salvo por la excepción trivial $\mathbf{Z}/\{0\}$. Para todo divisor positivo d de n , el grupo $\mathbf{Z}/n\mathbf{Z}$ (isomorfo a \mathbf{Z}_n , y algunas veces incluso tomado como definición de éste) tiene exactamente un subgrupo de orden d , a saber, el generado por la clase residual de n/d ; no hay más subgrupos de $\mathbf{Z}/n\mathbf{Z}$. El retículo de subgrupos es entonces isomorfo al de divisores de n , ordenados por divisibilidad (el cual es isomorfo a su propio dual).

En particular, un grupo cíclico es simple si y solo si su orden (el número de sus elementos) es primo.

Dado un grupo cíclico C de orden n , con generador g , el tamaño del subgrupo generado por g^k para un entero k será el mínimo entero positivo m tal que mk es múltiplo de n ; fácilmente se puede demostrar que $m = n/\text{mcd}(k, n)$. El índice del subgrupo generado por g^k (esto es, el tamaño del grupo cociente $C/\langle g^k \rangle$) es, por lo tanto, $\text{mcd}(k, n)$.

Grupo lineal

El **grupo lineal** de un espacio vectorial E , denotado como $GL(E)$, es el grupo formado por todas los isomorfismos de ese espacio.

Grupo lineal del espacio euclídeo

Si consideramos el espacio euclídeo n -dimensional o \mathbf{R}^n como espacio vectorial su grupo lineal estará representado por todas las aplicaciones lineales que admiten inversa. Si escogemos una base cualquiera para ese espacio vectorial, cada aplicación lineal podría expresarse mediante una matriz. Entonces el grupo lineal vendrá representado por el conjunto de todas las matrices que representan aplicaciones lineales que admiten inversa, y por tanto, por matrices cuyo determinante es diferente de cero (ya que el álgebra lineal establece que una aplicación lineal invertible viene representada en una base por una matriz de determinante diferente de cero).

Propiedades del grupo lineal

En un espacio vectorial normado E el grupo lineal $GL(E)$ puede ser dotado de una topología inducida, y resulta ser un conjunto abierto dentro del conjunto de aplicaciones lineales o morfismos del espacio vectorial E .

Grupo de Lie

En matemática, un **grupo de Lie** (nombrado así por Sophus Lie) es una variedad diferenciable real o compleja que es también un grupo tal que las operaciones de grupo: multiplicación e inversión son funciones analíticas. Los grupos de Lie son importantes en análisis matemático, física y geometría porque sirven para describir la simetría de estructuras analíticas. Fueron introducidos por Sophus Lie en 1870 para estudiar simetrías de ecuaciones diferenciales.

Mientras que el espacio euclídeo \mathbf{R}^n es un grupo de Lie real (con la adición ordinaria de vectores como operación de grupo), ejemplos más típicos son grupos de matrices inversibles (multiplicación de matrices), por ejemplo el grupo $\mathbf{SO}(3)$ de todas las rotaciones en el espacio de 3 dimensiones. Vea abajo para una lista más completa de ejemplos.

Tipos de grupos de Lie

Se clasifican los grupos de Lie con respecto a sus propiedades algebraicas (simple, semisimple, resoluble, nilpotente, abeliano), su conexidad (conexo o no conexo) y su compacidad.

Homomorfismos e isomorfismos

Si G y H son grupos de Lie (reales o complejos ambos), entonces un homomorfismo de grupo-de-Lie- $f: G \rightarrow H$ es un homomorfismo de grupo que es también una función analítica. (Se puede demostrar que es equivalente a requerir solamente que sea función continua.) La composición de dos tales homomorfismos es otra vez un homomorfismo, y la clase de todos los grupos de Lie (reales o complejos), junto con estos morfismos, forma una categoría. Dos grupos de Lie se dicen *isomorfos* si existe un homomorfismo biyectivo entre ellos cuyo inverso es también un homomorfismo. Los grupos de Lie isomorfos no necesitan, para cualquier propósito práctico, ser distinguidos; se diferencian solamente en la notación de sus elementos.

El álgebra de Lie asociada a un grupo de Lie

A cada grupo de Lie, podemos asociar un álgebra de Lie que captura totalmente la estructura *local* del grupo. Esto se hace como sigue. Un campo vectorial en un grupo de Lie G se dice invariante por la izquierda si conmuta con la traslación izquierda, que significa lo siguiente. Defina $L_g[f](x) = f(gx)$ para cualquier función analítica $f: G \rightarrow \mathbf{F}$ y todo g, x en G (aquí \mathbf{F} es el cuerpo \mathbf{R} o \mathbf{C}). entonces el campo vectorial X es invariante por la izquierda si $XL_g = L_gX$ para todo g en G .

El conjunto de todos los campos vectoriales en una variedad analítica es un álgebra de Lie sobre \mathbf{F} . En un grupo de Lie, los campos vectoriales invariantes por la izquierda forman una subálgebra, el álgebra de Lie asociada a G , denotado generalmente por una \mathfrak{g} gótica (\mathfrak{g}). Esta álgebra de Lie \mathfrak{g} es finito-dimensional (tiene la misma dimensión que la variedad G) lo que la hace susceptible a las tentativas de clasificación. Clasificando \mathfrak{g} , uno puede también conseguir un acercamiento al grupo de Lie G . La teoría de representación de los grupos simples de Lie son el mejor y más importante ejemplo.

Cada elemento v del espacio tangente T_e en el elemento identidad e de G determina un campo vectorial izquierdo-invariante único cuyo valor en el elemento x de G es denotado xv ; el espacio

vectorial subyacente a \mathfrak{g} se puede por lo tanto identificar con T_e . la estructura del álgebra de Lie en T_e puede también ser descrita como sigue: la operación del conmutador

$$(x, y) \mapsto xyx^{-1}y^{-1}$$

en $G \times G$ envía (e, e) a e , así que su derivada da una operación bilineal en T_e . resulta que esta operación bilineal satisface los axiomas de un corchete de Lie, y es igual al que es definido a través de campos vectoriales invariantes por la izquierda.

Cada vector v en \mathfrak{g} determina una función $c: \mathbf{R} \rightarrow G$ cuya derivada en todo punto viene dado por el campo vectorial invariante por la izquierda correspondiente

$$c'(t) = c(t)v$$

y que tiene la propiedad

$$c(s+t) = c(s)c(t)$$

para todo s y t . La operación en el lado derecho es la multiplicación de grupo en G . La semejanza formal de esta fórmula con la que es válida para la función exponencial justifica la definición

$$\exp(v) = c(1)$$

esto se llama la *función exponencial*, y mapea el álgebra de Lie \mathfrak{g} en el grupo de Lie G . Proporciona un difeomorfismo entre una vecindad de 0 en \mathfrak{g} y una vecindad de e en G . Esta función exponencial es una generalización de la función exponencial para los números reales (puesto que \mathbf{R} es el álgebra de Lie del grupo de Lie de números reales positivos con la multiplicación usual), para los números complejos (puesto que \mathbf{C} es el álgebra de Lie del grupo de Lie de números complejos diferentes a cero con la multiplicación usual) y para las matrices (puesto que $M(n, \mathbf{R})$ con el conmutador regular es el álgebra de Lie del grupo de Lie $GL(n, \mathbf{R})$ de todas las matrices inversibles).

Porque la función exponencial es suryectiva en alguna vecindad N de e , es común llamar a los elementos del álgebra de Lie **generadores infinitesimales** del grupo G . De hecho, el subgrupo de G generado por N será el grupo entero G solamente cuando G sea conexo.

La función exponencial y el álgebra de Lie determinan la estructura de grupo local de cada grupo de Lie conexo, debido a la fórmula de Campbell-Hausdorff: existe una vecindad U del elemento cero de \mathfrak{g} , tal que para u, v en U se tiene

$$\exp(u)\exp(v) = \exp(u + v + 1/2 [u, v] + 1/12 [[u, v], v] - 1/12 [[u, v], u] - \dots)$$

donde los términos omitidos son conocidos e implican los corchetes de Lie de cuatro o más elementos. En caso de que u y v conmuten, esta fórmula se reduce a la ley exponencial familiar $\exp(v)\exp(u) = \exp(u+v)$.

Cada homomorfismo $f: G \rightarrow H$ de los grupos de Lie induce un homomorfismo entre las álgebra de Lie correspondientes \mathfrak{g} y \mathfrak{h} . la asociación $G \mapsto \mathfrak{g}$ es un funtor. La estructura global de un grupo de Lie no está totalmente determinada, en general, por su álgebra de Lie; vea la tabla abajo para los ejemplos de grupos de Lie diversos que comparten la misma álgebra de Lie. Podemos decir sin

embargo que un grupo de Lie conexo es simple, semisimple, resoluble, nilpotente, o abeliano si y solamente si su álgebra de Lie tiene la propiedad correspondiente.

Si requerimos que el grupo de Lie sea simplemente conexo, entonces la estructura global está determinada por su álgebra de Lie: para cada álgebra de Lie \mathfrak{g} finito dimensional sobre \mathbf{F} hay un único (módulo un isomorfismo) grupo de Lie G simplemente conexo con \mathfrak{g} como álgebra de Lie. Por otra parte cada homomorfismo entre las álgebras de Lie se eleva a un homomorfismo único entre los correspondientes grupos de Lie simplemente conexos.

Lista de algunos grupos de Lie reales y de sus álgebras de Lie

grupo de Lie	descripción	Comentarios	álgebra de Lie	descripción	dim/ \mathbf{R}
\mathbf{R}^n	espacio euclídeo con adición	abeliano, simplemente conexo, no compacto	\mathbf{R}^n	el corchete de Lie es cero	n
\mathbf{R}^\times	números reales no nulos con la multiplicación	abeliano, no conexo, no compacto	\mathbf{R}	el corchete de Lie es cero	1
\mathbf{R}^+	números reales positivos con la multiplicación	abeliano, simplemente conexo, no compacto	\mathbf{R}	el corchete de Lie es cero	1
$S^1 = \mathbf{R}/\mathbf{Z}$	números complejos de valor absoluto 1 con la multiplicación	abeliano, conexo, no simplemente conexo, compacto	\mathbf{R}	el corchete de Lie es cero	1
\mathbf{H}^\times	cuaterniones no nulos con la multiplicación	conexo, simplemente conexo, no compacto	\mathbf{H}	cuaterniones, con el corchete de Lie dado por el conmutador	4
S^3	cuaterniones de módulo 1 con la multiplicación, una 3-esfera	simplemente conexo, compacto, simple y semi-simple, isomorfo a $SU(2)$ y a $\text{Spin}(3)$	\mathbf{R}^3	3-vectores reales, con el corchete de Lie el producto vectorial; isomorfo a los cuaterniones con parte real cero, con el corchete de Lie dado por el conmutador también isomorfo a	3

				$\mathfrak{su}(2)$ y a $\mathfrak{so}(3)$	
$GL(n, \mathbb{R})$	grupo general lineal: matrices reales n -por- n invertibles	no conexo, no compacto	$M(n, \mathbb{R})$	matrices reales n -por- n , con el corchete de Lie dado por el conmutador	n^2
$GL^+(n, \mathbb{R})$	matrices reales n -por- n con determinante positivo	conexo, no compacto	$M(n, \mathbb{R})$	matrices reales n -por- n , con el corchete de Lie dado por el conmutador	n^2
$SL(n, \mathbb{R})$	grupo especial lineal: matrices reales n -por- n con determinante 1	conexo, no compacto y simple si $n > 1$	$\mathfrak{sl}(n, \mathbb{R})$	matrices reales n -por- n , con traza 0, con el corchete de Lie dado por el conmutador	$n^2 - 1$
$O(n, \mathbb{R})$	grupo ortogonal: matrices reales n -por- n ortogonales	no conexo, compacto	$\mathfrak{so}(3, \mathbb{R})$	matrices reales n -por- n , antisimétricas, con el corchete de Lie dado por el conmutador; $\mathfrak{so}(3, \mathbb{R})$ es isomorfo a $\mathfrak{su}(2, \mathbb{R})$ y a \mathbb{R}^3 con el producto vectorial	$n(n-1)/2$
$SO(n, \mathbb{R})$	grupo especial ortogonal: matrices reales n -por- n ortogonales con determinante 1	conexo, compacto, no simplemente conexo si $n > 1$, semisimple, si $n=3$ o $n \geq 5$ simple	$\mathfrak{so}(n, \mathbb{R})$	matrices reales n -por- n , antisimétricas, con el corchete de Lie dado por el conmutador	$n(n-1)/2$
$Spin(n)$	grupo de espinores	simplemente conexo, compacto, semisimple, si $n=3$ o $n \geq 5$ simple	$\mathfrak{so}(n, \mathbb{R})$	matrices reales n -por- n , antisimétricas, con el corchete de Lie dado por el conmutador	$n(n-1)/2$
$Sp(2n, \mathbb{R})$	grupo simplécticoreal: matrices simplécticas reales	no compacto, simple y semisimple	$\mathfrak{sp}(2n, \mathbb{R})$	matrices reales que satisfacen $JA + A^T J = 0$ donde J es la matriz anti-simétrica estándar	$n(2n + 1)$

$\mathbf{Sp}(n)$	grupo simpléctico: matrices unitarias n -por- n cuaterniónicas	compacto, simplemente conexo, simple y semisimple si $n > 0$	$\mathfrak{sp}(n)$	matrices cuaterniónicas cuadradas A satisfaciendo $A = -A^*$, con el corchete de Lie dado por el conmutador	$n(2n + 1)$	
$\mathbf{U}(n)$	grupo unitario: matrices complejas n -por- n unitarias	isomorfo a S^1 para $n=1$, no simplemente conexo para $n > 0$, compacto. Nota: este <i>no</i> es un grupo/álgebra de Lie complejo	$\mathfrak{u}(n)$	matrices complejas n -por- n , que cumplen $A = -A^*$, con el corchete de Lie dado por el conmutador	$n(n-1)/2$	n^2
$\mathbf{SU}(n)$	grupo especial unitario: matrices complejas n -por- n unitarias con determinante 1	simplemente conexo, compacto y si $n \geq 2$, simple y semisimple. Nota: este <i>no</i> es un grupo/álgebra de Lie complejo	$\mathfrak{su}(n)$	matrices complejas $n \times n$, que cumplen $A = -A^*$ con traza 0, con el corchete de Lie dado por el conmutador	$n^2 - 1$	

Lista de algunos grupos de Lie complejos y de sus álgebras de Lie

grupo de Lie	descripción	Comentarios	álgebra de Lie	descripción	dim/C
\mathbf{C}^n	espacio euclídeo con adición	abeliano, simplemente conexo, no compacto	\mathbf{C}^n	el corchete de Lie es cero	n
\mathbf{C}^\times	números complejos no nulos con la multiplicación	abeliano, conexo, no simplemente conexo, no compacto	\mathbf{C}	el corchete de Lie es cero	1
$\mathbf{GL}(n, \mathbf{C})$	grupo general lineal: matrices complejas n -por- n inversibles	simplemente conexo, no compacto	$\mathbf{M}(n, \mathbf{C})$	matrices complejas n -por- n , con el corchete de Lie dado por el conmutador	n^2
$\mathbf{SL}(n, \mathbf{C})$	grupo especial lineal complejo: matrices complejas n -por- n con determinante 1	simple y semisimple, simplemente conexo si $n > 1$, no compacto	$\mathfrak{sl}(n, \mathbf{C})$	matrices complejas n -por- n , con traza 0, con el corchete de Lie dado por el conmutador	$n^2 - 1$

$O(n, \mathbb{C})$	grupo ortogonal: matrices complejas n - por- n ortogonales	no conexo $n > 1$, compacto	$so(n, \mathbb{C})$	matrices complejas n - por- n , antisimétricas, con el corchete de Lie dado por el conmutador	$n(n-1)/2$
$SO(n, \mathbb{C})$	grupo especial ortogonal: matrices complejas n -por- n ortogonales con determinante 1	conexo, no compacto, no simplemente conexo si $n > 1$, si $n=3$ o $n \geq 5$ simple y semisimple	$so(n, \mathbb{C})$	matrices complejas n - por- n , antisimétricas, con el corchete de Lie dado por el conmutador	$n(n-1)/2$
$Sp(2n, \mathbb{C})$	grupo simpléctico: matrices simplécticas complejas	no compacto, simple y semisimple	$sp(2n, \mathbb{C})$	matrices complejas que satisfacen $JA + A^T J = 0$ donde J es la matriz anti-simétrica estándar	$n(2n + 1)$

Álgebra de Lie

En matemática, un **álgebra de Lie** es la estructura algebraica que describe un conjunto de transformaciones infinitesimales. Su uso principal reside en el estudio de objetos geométricos tales como grupos de Lie y variedades diferenciables. El término "álgebra de Lie" (referido a Sophus Lie) fue creado por Hermann Weyl en los años 30, para lo que se denominaba "grupo infinitesimal".

Definición

Un álgebra de Lie \mathbf{A} es un espacio vectorial sobre un cierto cuerpo \mathbf{F} junto con una operación binaria $[\cdot, \cdot] : \mathbf{A} \times \mathbf{A} \rightarrow \mathbf{A}$, llamada **corchete de Lie**, que satisface las propiedades siguientes:

- es bilineal, es decir, $[a x + b y, z] = a [x, z] + b [y, z]$ y $[z, a x + b y] = a [z, x] + b [z, y]$ para todo a, b en \mathbf{F} y todo x, y, z en \mathbf{A} .
- satisface la identidad de Jacobi, es decir, $[[x, y], z] + [[z, x], y] + [[y, z], x] = 0$ para todo x, y, z en \mathbf{A} .
- $[x, x] = 0$ para todo x en \mathbf{A} .

Observe que la primera propiedad y la tercera juntas implican $[x, y] = -[y, x]$ para todo x, y en \mathbf{A} ("anti-simetría") si el cuerpo \mathbf{F} es de característica diferente de dos. Observe también que la multiplicación representada por el corchete de Lie no es, en general, asociativa, es decir, $[[x, y], z]$ no necesariamente es igual a $[x, [y, z]]$.

Ejemplos

- Cada espacio vectorial se convierte en un álgebra de Lie abeliana trivial si definimos el corchete de Lie como idénticamente cero.
- El espacio euclídeo \mathbb{R}^3 se convierte en un álgebra de Lie con el corchete de Lie dado por el producto vectorial.
- Si se da un álgebra asociativa A con la multiplicación $*$, se puede dar un álgebra de Lie definiendo $[x, y] = x * y - y * x$. esta expresión se llama el *conmutador* de x e y .
- Inversamente, puede ser demostrado que cada álgebra de Lie se puede sumergir en otra que surja de un álgebra asociativa de esa manera.
- Otro ejemplo importante viene de la topología diferencial: los campos vectoriales en una variedad diferenciable forman un álgebra de Lie de dimension infinita. Estos campos vectoriales actúan como operadores diferenciales sobre las funciones diferenciables sobre la variedad. Dados dos campos vectoriales X e Y , el corchete de Lie $[X, Y]$ se define como:

$$[X, Y]f = (XY - YX)f$$

y puede comprobarse que este operador corresponde a un campo vectorial. Las generalizaciones adecuadas de la teoría de variedades al caso de dimensión infinita muestra que este álgebra de Lie es la asociada (ver siguiente punto) al grupo de Lie de los difeomorfismos de la variedad.

- En el caso de una variedad que sea un grupo de Lie G a su vez, un subespacio de los campos vectoriales queda inalterado por las transformaciones dadas por el propio grupo, en el sentido de que en cada punto g del mismo, el campo no es más que:

$$X(g) = dl_g(X(e))$$

Este subespacio es de dimensión finita (e igual a la del grupo), dado que se corresponde con el espacio tangente en la identidad. Además hereda la estructura de álgebra de Lie definida en el punto anterior, y se le denomina el **álgebra de Lie asociada al grupo G** .

- Como ejemplo concreto, consideremos el grupo de Lie $SL(n, \mathbb{R})$ de todas las matrices $n \times n$ con valores reales y determinante 1. El espacio tangente en la matriz identidad se puede identificar con el espacio de todas las matrices reales $n \times n$ con traza 0 y la estructura de álgebra de Lie que viene del grupo de Lie coincide con el que surge del conmutador de la multiplicación de matrices.

Homomorfismos, subálgebras e ideales

Un homomorfismo $\phi : \mathbf{A} \rightarrow \mathbf{B}$ entre las álgebra de Lie \mathbf{A} y \mathbf{B} sobre el mismo cuerpo de base \mathbf{F} es una función \mathbf{F} -lineal tal que $[\phi(x), \phi(y)] = \phi([x, y])$ para todo x y y en \mathbf{A} . La composición de tales homomorfismos es otra vez un homomorfismo, y las álgebras de Lie sobre el cuerpo \mathbf{F} , junto con estos morfismos, forman una categoría. Si tal homomorfismo es biyectivo, se llama un isomorfismo, y las dos álgebras de Lie \mathbf{A} y \mathbf{B} se llaman isomorfas. Para todos los efectos prácticos, las álgebras de Lie isomorfas son idénticas.

Una *subálgebra* del álgebra de Lie \mathbf{A} es un subespacio vectorial \mathbf{B} de \mathbf{A} tal que $[x, y] \in \mathbf{B}$ para todo $x, y \in \mathbf{B}$. i.e. $[\mathbf{B}, \mathbf{B}] \subseteq \mathbf{B}$. La subálgebra es entonces un álgebra de Lie.

Un *ideal* del álgebra de Lie \mathbf{A} es un subespacio vectorial \mathbf{I} de \mathbf{A} tales que $[a, y] \in \mathbf{I}$ para toda $a \in \mathbf{A}$ y $y \in \mathbf{I}$. i.e. $[\mathbf{A}, \mathbf{I}] \subseteq \mathbf{I}$. Todos los ideales son subálgebras. Si \mathbf{I} es un *ideal* de \mathbf{A} , entonces el espacio cociente \mathbf{A}/\mathbf{I} se convierte en una álgebra de Lie definiendo $[x + \mathbf{I}, y + \mathbf{I}] = [x, y] + \mathbf{I}$ para todo $x, y \in \mathbf{A}$. Los ideales son precisamente los núcleos de homomorfismos, y el teorema fundamental de homomorfismos es válido para las álgebras de Lie.

Clasificación de las álgebras de Lie

Las álgebras de Lie reales y complejas se puede clasificar hasta un cierto grado, y esta clasificación es un paso importante hacia la clasificación de los grupos de Lie. Cada álgebra de Lie real o compleja finito-dimensional se presenta como el álgebra de Lie de un único grupo de Lie simplemente conexo real o complejo (teorema de Ado), pero puede haber más de un grupo, aún más de un grupo conexo, dando lugar a la misma álgebra. Por ejemplo, los grupos $\mathbf{SO}(3)$ (matrices ortogonales 3×3 de determinante 1) y $\mathbf{SU}(2)$ (matrices unitarias 2×2 de determinante 1), ambos dan lugar a la misma álgebra de Lie, a saber \mathbf{R}^3 con el producto vectorial. Un álgebra de Lie es abeliana si el corchete de Lie se anula, es decir $[x, y] = 0$ para todo x y y . Más generalmente, un álgebra de Lie \mathbf{A} es *nilpotente* si la serie central descendente

$$\mathbf{A} \supseteq [\mathbf{A}, \mathbf{A}] \supseteq [[\mathbf{A}, \mathbf{A}], \mathbf{A}] \supseteq [[[\mathbf{A}, \mathbf{A}]], \mathbf{A}], \mathbf{A}] \supseteq \dots$$

acaba haciéndose cero. Por el teorema de Engel, un álgebra de Lie es *nilpotente* si y solo si para cada x en \mathbf{A} , la función $\text{ad}(x): \mathbf{A} \rightarrow \mathbf{A}$ definida por

$$\text{ad}(x)(y) = [x, y]$$

es nilpotente. Más generalmente aún, un álgebra de Lie \mathbf{A} es *soluble* si la serie derivada

$$\mathbf{A} \supseteq [\mathbf{A}, \mathbf{A}] \supseteq [[\mathbf{A}, \mathbf{A}], [\mathbf{A}, \mathbf{A}]] \supseteq [[[\mathbf{A}, \mathbf{A}]], [\mathbf{A}, \mathbf{A}]], [[\mathbf{A}, \mathbf{A}], [\mathbf{A}, \mathbf{A}]] \supseteq \dots$$

acaba haciéndose cero. Una subálgebra soluble maximal se llama una *subálgebra de Borel*.

Un álgebra de Lie \mathbf{A} se llama *semisimple* si el único ideal soluble de \mathbf{A} es trivial. Equivalente, \mathbf{A} es semisimple si y solamente si la *forma de Killing* $K(x, y) = \text{tr}(\text{ad}(x)\text{ad}(y))$ es no-degenerada; aquí tr denota el operador de traza. Cuando el cuerpo \mathbf{F} es de característica cero, \mathbf{A} es semi-simple si y solamente si cada representación es totalmente reducible, esto es, que para cada subespacio invariante de la representación hay un complemento invariante (teorema de Weyl). Un álgebra de Lie es *simple* si no tiene ningún ideal no trivial. En particular, un álgebra de Lie *simple* es *semi-simple*, y más generalmente, las álgebras de Lie *semi-simples* son suma directa de *simples*. Las álgebras de Lie complejas *semi-simples* se clasifican a través de sus *sistemas de raíz*.

Álgebra de Lie ortogonal generalizada

$\begin{pmatrix} \mathbf{A} & \mathbf{V} \\ -\mathbf{V}^t & 0 \end{pmatrix}$ pertenece a $\mathfrak{so}(\mathbf{n}+1)$ si \mathbf{A} pertenece a $\mathfrak{so}(\mathbf{n})$ y \mathbf{V} es un \mathbf{n} -vector (columna).

$\begin{pmatrix} \mathbf{A} & \mathbf{V} \\ \mathbf{V}^t & 0 \end{pmatrix}$ pertenece a $\mathfrak{so}(\mathbf{n}, \mathbf{m}+1)$ si \mathbf{A} pertenece a $\mathfrak{so}(\mathbf{n}, \mathbf{m})$ y \mathbf{V} es un $(\mathbf{n}+\mathbf{m})$ -vector. (incluyendo $\mathbf{m} = 0$, por supuesto). El álgebra de Lobachevski es $\mathfrak{so}(\mathbf{n}, 1)$ (no álgebra de Lorentz como es usual en la literatura, una confusión con su papel en el álgebra de Poincaré, aunque la expresión común es álgebra hiperbólica).

Notación Nueva!: $\begin{pmatrix} A & V \\ 0 & 0 \end{pmatrix}$ pertenece a $\mathfrak{so}(\mathbf{n}, \mathbf{m}, 1)$ si \mathbf{A} pertenece a $\mathfrak{so}(\mathbf{n}, \mathbf{m})$ y \mathbf{V} es un $(\mathbf{n}+\mathbf{m})$ -vector. El álgebra euclidiana es $\mathfrak{so}(\mathbf{n}, 0, 1)$!. El álgebra de Poincaré es $\mathfrak{so}(\mathbf{n}, 1, 1)$. En general, representa el álgebra de Lie del producto semidirecto de las traslaciones en el espacio $\mathbf{R}^{\mathbf{n}+\mathbf{m}}$ con $\mathfrak{so}(\mathbf{n}, \mathbf{m})$ que tiene a $\mathfrak{so}(\mathbf{n}, \mathbf{m})$ como su álgebra de Lie.

Notación Nueva: $\begin{pmatrix} A & V \\ 0 & 0 \end{pmatrix}$ pertenece a $\mathfrak{so}(\mathbf{n}, \mathbf{m}, \mathbf{l}+1)$ si \mathbf{A} pertenece a $\mathfrak{so}(\mathbf{n}, \mathbf{m}, \mathbf{l})$ y \mathbf{V} es un $(\mathbf{n}+\mathbf{m}+\mathbf{l})$ -vector.

En particular: $\begin{pmatrix} A & V & X \\ 0 & 0 & t \\ 0 & 0 & 0 \end{pmatrix}$ pertenece a $\mathfrak{so}(\mathbf{n}, \mathbf{m}, 2)$ si \mathbf{A} pertenece a $\mathfrak{so}(\mathbf{n}, \mathbf{m})$ y \mathbf{V} y \mathbf{X} son $(\mathbf{n}+\mathbf{m})$ -vectores. El álgebra de Galileo es $\mathfrak{so}(\mathbf{n}, 0, 2)$, asociado a un producto semidirecto iterado. (t es un "número", pero importante $\mathfrak{g}/[\mathfrak{g}, \mathfrak{g}]$ da t si $\mathbf{n} > 2$. así que el tiempo es la parte conmutativa del grupo de Galileo).

Para completar, damos aquí las ecuaciones de estructura. El álgebra de Galileo \mathfrak{g} es expandida por T , X_i , V_i y A_{ij} (tensor antisimétrico) conforme a:

- $[X_i, T] = 0$
- $[X_i, X_j] = 0$
- $[A_{ij}, T] = 0$
- $[V_i, V_j] = 0$
- $[A_{ij}, A_{kl}] = \delta_{ik} A_{jl} - \delta_{il} A_{jk} - \delta_{jk} A_{il} + \delta_{jl} A_{ik}$
- $[A_{ij}, X_k] = \delta_{ik} X_j - \delta_{jk} X_i$
- $[A_{ij}, V_k] = \delta_{ik} V_j - \delta_{jk} V_i$

- $[V_i, X_j] = 0$
- $[V_i, T] = X_i$

Super álgebra de Lie

En matemática, una **super álgebra de Lie** es la generalización de un álgebra de Lie. Las super álgebras de Lie son importantes en física teórica en donde se utilizan para describir la matemática de la supersimetría. En estas teorías, los elementos pares de la super álgebra corresponden a los bosones y los elementos impares a los fermiones. Una super álgebra de Lie es un álgebra sobre un cuerpo de característica 0 \mathbb{Z}_2 -graduado cuyo producto $[\cdot, \cdot]$, llamado el **super corchete de Lie** o el **super conmutador**, satisface

- $[x, y] = -(-1)^{|x||y|} [y, x]$
- $(-1)^{|z||x|} [x, [y, z]] + (-1)^{|x||y|} [y, [z, x]] + (-1)^{|y||z|} [z, [x, y]] = 0$

donde x, y , y z son *puros* en la \mathbb{Z}_2 -graduación. Aquí $|x|$ denota el grado de x (0 o 1).

Las super álgebras de Lie son una generalización natural de las álgebras de Lie normales para incluir una \mathbb{Z}_2 -graduación. De hecho, las condiciones antedichas en el super corchete son exactamente aquellas en el corchete normal de Lie con las modificaciones hechas para la graduación. La última condición a veces se llama la **super identidad de Jacobi**.

El subálgebra par de una super álgebra de Lie forma un álgebra de Lie (normal) puesto que todos los signos desaparecen, y el super corchete se reduce a un corchete normal de Lie.

E8

En matemática, **E₈** es el nombre de un grupo de Lie (el más grande) *simple* y *excepcional* y del álgebra de Lie que le está asociada. Su álgebra de Lie es formulada con la notación **e₈**.

La estructura E_8 fue descubierta en 1887 por el matemático noruego Sophus Lie para estudiar las simetrías.

Es también el nombre dado al correspondiente sistema de generadores y al grupo de Weyl-Coxeter y a algunos grupos de Chevalley simples y finitos. Aunque el sistema E_8 fue previsto por Lie, fue Wilhelm Killing (entre 1888-1890) quien le dio la denominación e interpretación más precisa con que actualmente es identificado.

El nombre E_8 se debe a las clasificaciones de las álgebras de Lie simples y complejas de Wilhelm Killing y Élie Cartan, las cuales comprenden cuatro familias infinitas llamadas A_n, B_n, C_n, D_n y cinco casi excepcionales, llamadas E_6, E_7, E_8, F_4, G_2 .

El grupo E_8 es el más grande y el más complicado de estos casos excepcionales y frecuentemente el último caso de la demostración de varios teoremas.

Descripción básica

E_8 posee un rango 8 y 248 dimensiones (como espacio vectorial) y su centro es trivial. Los generadores son, entonces, vectores de dimensión 8 (serán observados más adelante en el presente artículo).

El grupo de Weyl de E_8 , es del orden 696729600. E_8 y el único grupo de Lie simple en el cual la representación no banal de mínima dimensión es la llamada *adjoint action* (acción adjunta), la cual actúa sobre el álgebra E_8 misma.

Existe un álgebra de Lie E_n para todo número entero $n \geq 3$, y es de infinitas dimensiones si n es mayor de 8.

Formas reales

El grupo de Lie *complejo* E_8 , de dimensiones complejas 248 (por lo tanto de dimensión real 496), puede ser considerado como un grupo simple de 496 dimensiones (reales), el cual está simplemente conexo, posee como máximo un subgrupo compacto de la forma compacta de E_8 y posee un grupo externo de automorfismos de dimensión 2, generado por la conjugación compleja.

Así como existe el grupo de Lie complejo, existen tres formas *reales* de E_8 , todas de 248 dimensiones, del siguiente modo:

- Una forma *compacta* (aquella a la cual el nombre se refiere a falta de otras informaciones), que es *simplemente conexa* y posee un grupo externo de automorfismos banales. $E_{8(-248)}$
- Una *split form* o forma desplegada, que posee como máximo un subgrupo compacto en el cual se tiene muy en cuenta al spin: $Spin(16) / (Z / 2Z)$, grupo fundamental de orden 2, y un no-algebraico doble recubrimiento y posee un grupo externo de automorfismos.
- Una tercera forma, que posee como máximo subgrupo compacto $E_7 \times SU(2) / (-I \times -I)$, grupo fundamental de orden 2, y un no-algebraico doble recubrimiento así como posee un grupo externo de automorfismos banales. Su notación es $E_{8(-24)}$

Teoría de las representaciones

Los coeficientes de las fórmulas de los caracteres para las representaciones *irreducibles* infinito-dimensionales dependen de algunas matrices cuadradas de polinomios: los polinomios de Lusztig-Vogan, análogos a los polinomios de Kazhdan-Lusztig, introducidos por George Lusztig y David Vogan (1983). El valor de estos polinomios calculados en 1 da los coeficientes de las matrices relativas a la representación estándar (cuyos caracteres son fáciles de describir merced a las representaciones irreducibles).

Estas matrices fueron calculadas tras cuatro años con la colaboración de un equipo denominado *Atlas of Lie groups and Representations* que reunió a 18 matemáticos e informáticos dirigidos por Jeffrey Adams y con gran parte de la programación hecha por Fokko du Cloux y Marc van Leeuwen.

Representaciones

\mathfrak{e}_8 se distingue de las otras álgebras de Lie de dimensión completa por el hecho de que su más pequeña representación no-trivial es la llamada representación adjunta.

La representación fundamental de E_8 es de dimensión 248.

Construcciones

Se puede construir la forma compacta del grupo E_8 como el grupo de automorfismos del álgebra de Lie \mathfrak{e}_8 correspondiente. Esta álgebra posee $\mathfrak{so}(16)$ como subálgebra de dimensión 120 y se puede hacer uso de ella para descomponer la representación adjunta como

$$\mathfrak{e}_8 = \mathfrak{so}(16) \oplus S_{16}^+$$

ó S_{16}^+ es una de las dos representaciones espinoriales, de tipo Majorana-Weyl del grupo $\text{Spin}(16)$ donde $\mathfrak{so}(16)$ es el álgebra de Lie.

Si se denomina J_{ij} a un juego de generadores por $\mathfrak{so}(16)$ y Q_a a los 128 componentes de S_{16}^+ entonces se puede escribir explícitamente las relaciones definitorias \mathfrak{e}_8 como

$$[J_{ij}, J_{kl}] = \delta_{jk}J_{il} - \delta_{jl}J_{ik} - \delta_{ik}J_{jl} + \delta_{il}J_{jk}$$

de modo que

$$[J_{ij}, Q_a] = \frac{1}{4} (\gamma_i \gamma_j - \gamma_j \gamma_i)_{ab} Q_b, \text{ que corresponde a la acción natural } \mathfrak{so}(16) \text{ sobre el espinador } S_{16}^+. \text{ El conmutador restante (que resulta ser un conmutador aunque no un anticonmutador) está definido entre los componentes del espinador como}$$
$$[Q_a, Q_b] = \gamma_{ac}^{[i} \gamma_{cb}^{j]} J_{ij}.$$

A partir de estas definiciones se puede observar que la identidad de Jacobi está cumplida.

Geometría

La forma real compacta de E_8 puede ser observada como el grupo de isosimetría de una variedad riemanniana de dimensión 128 denominada *plan proyectivo octoniónico*.

Este nombre procede de que tal plan puede construirse utilizando un álgebra que está construida como producto tensorial de los octoniones y con ellos mismos. Este tipo de construcción ha sido analizada detalladamente por Hans Freudenthal y Jacques Tits en su construcción del cuadro mágico o cuadrado mágico.

En física

En el marco de las teorías de la gran unificación y teorías del todo —principalmente en física de las partículas—, El grupo E_8 es a veces considerado como grupo de arqueo y referencia en la medida que contiene de una manera natural una serie de otros grupos de gran unificación muy considerados. Esto se puede observar bajo la sucesión de inclusiones

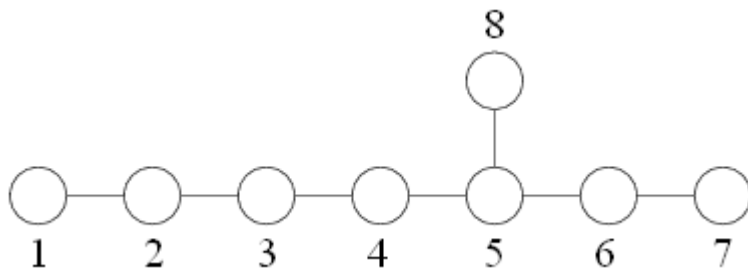
$$E_8 \leftarrow SO(10) \leftarrow SU(5) \leftarrow SU(3) \times SU(2) \times U(1)$$

Por lo demás, el grupo E_8 aparece frecuentemente en teoría de las cuerdas y en supergravedad. En la teoría de las cuerdas heteróticas una formulación hace aparecer $E_8 \times E_8$ (bajo forma compacta) como grupo de Gauge.

De otra parte, en cuanto que la supergravedad maximal está considerada como compactificada o resabiada sobre un toro de dimensión 8 entonces la teoría resultante en dimensión tres posee una simetría global E_8 (es decir: la forma desplegada o maximalmente no-compactada). Esto ha sugerido que una versión discreta, cuya notación es $E_8(\mathbb{Z})$, de este grupo sería una simetría, la cual estaría considerada en el contexto de la U-dualidad, de la teoría M.

En noviembre de 2007, un investigador estadounidense, Antony Garrett Lisi, publicó en el sitio de publicaciones ArXiv un artículo muy discutido referido a una teoría unificatoria de las 4 fuerzas elementales (Una teoría del todo excepcionalmente simple) basada en E_8 .

Diagrama de Dynkin



Sistema de raíces

Desde la base formada por las raíces simples $\mathfrak{so}(16)$, el sistema de raíces de E_8 está formado por un lado de todas las permutaciones de

$$(\pm 1, \pm 1, 0, 0, 0, 0, 0, 0)$$

que constituye el sistema de raíces de $\mathfrak{so}(16)$ y poseedor de $4 \times \binom{8}{2} = 112$ elementos (esto hace añadir nuevamente 8 generadores de Cartan para obtener 120 que es la la dimensión de $\mathfrak{so}(16)$).

Además se debe añadir a esto las 128 ponderaciones de la representación espinorial S_{16}^+ de $\mathfrak{so}(16)$. Siempre con la misma base, estos son representados por los vectores

$$\left(\pm\frac{1}{2}, \pm\frac{1}{2}, \pm\frac{1}{2}, \pm\frac{1}{2}, \pm\frac{1}{2}, \pm\frac{1}{2}, \pm\frac{1}{2}, \pm\frac{1}{2}\right)$$

de modo que la suma de todas las coordenadas sea pareja. Así éstas son del número $\frac{1}{2} \times 2^8 = 128$

Se obtienen entonces $112 + 128 = 240$ raíces, todas múltiplos de 1. Por abuso de lenguaje se ha considerado también en ocasiones al vector nulo como una raíz nula asociada al subálgebra de Cartan. Como E_8 es de rango 8, la raíz nula es entonces de multiplicidad 8. De este modo se describe bien a los 248 generadores del álgebra \mathfrak{e}_8 .

Matriz de Cartan

$$\begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & -1 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 2 \end{pmatrix}$$

Decodificación del grupo E_8

El 19 de marzo de 2007 el Instituto estadounidense de matemáticas (AIM) ha anunciado que los investigadores europeos y estadounidenses luego de cuatro años de trabajo han llegado a decodificar el E_8 , una de las estructuras matemáticas más complejas y grandes.

El núcleo del grupo de investigadores está constituido por siete matemáticos, cinco estadounidenses y dos franceses: Jeffrey Adams de la Universidad de Maryland, Dan Barbasch de Universidad Cornell, John Stembridge de la Universidad de Michigan, Peter Trapa de la Universidad de Utah, Marc van Leeuwen de la Universidad de Poitiers, David Vogan del MIT y Fokko du Cloux de la Universidad de Lyon.¹

Entre los objetos subyacentes en los grupos de Lie, se encuentra toda suerte de figuras geométricas como por ejemplo esferas, conos y cilindros del espacio tridimensional. Sin embargo las cuestiones se hacen más complejas (como si se potenciaran) cuando se las observa en más de tres dimensiones. «Comprender y clasificar las estructuras E_8 ha sido crítico para comprender los fenómenos en numerosos dominios de las matemáticas incluyendo el álgebra, la geometría, la física, la teoría de los números así como en la química», ha comentado Peter Sarnak, profesor de matemáticas en la Universidad de Princeton y presidente del comité científico del AIM.

Estos cálculos requieren de nuevas técnicas matemáticas y de más capacidad de cálculo en los ordenadores. Por ejemplo para llegar al cálculo de G_8 una sola operación ha necesitado 77 horas en un supercomputador dotado de 200 Gbytes de memoria RAM, y ha producido un resultado del orden de 60 Gbytes por lo que esta magnitud puede ser comparada a 60 veces a la requerida para el

genoma humano (el conjunto de datos del genoma representa un volumen de 1 Gbyte). El equipo de investigadores busca encontrar un supercomputador capaz de efectuar los cálculos requeridos; Noam Elkies, un matemático de la Universidad Harvard ha puesto en evidencia un modo de fraccionar el proyecto en elementos más simples. Cada elemento produce un subconjunto del resultado y su reunión permite hallar la solución completa. Así, en verano de 2006 tres integrantes del equipo de investigadores, entre ellos Fokko du Cloux, han descompuesto el programa en numerosos elementos. Los cálculos han sido realizados en una computadora de la Universidad de Washington.

El resultado del cálculo de E_8 si fuera escrito sobre papel cubriría un área similar a la de la isla de Manhattan.

Algunas cifras a partir del cálculo de E_8

Algunas nociones respecto a la magnitud del resultado final¹ :

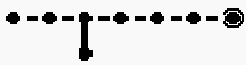
- El resultado de E_8 es una matriz de 453.060 filas y columnas.
- La matriz comporta 205.263.363.600 elementos,
- Si cada elemento de esta matriz estuviera escrito sobre una superficie de 2,5 cm², la matriz tendría la extensión de un cuadrado de 10 km de lado.
- Número de polinomios distintos : 1.181.642.979,
- Número de coeficientes entre los polinomios distintos : 13.721.641.221,
- Más grande coeficiente : 11.808.808,
- Polinomio de mayor coeficiente : $152 q^{22} + 3472 q^{21} + 38\,791 q^{20} + 293\,021 q^{19} + 1\,370\,892 q^{18} + 4\,067\,059 q^{17} + 7\,964\,012 q^{16} + 11\,159\,003 q^{15} + 11\,808\,808 q^{14} + 9\,859\,915 q^{13} + 6\,778\,956 q^{12} + 3\,964\,369 q^{11} + 2\,015\,441 q^{10} + 906\,567 q^9 + 363\,611 q^8 + 129\,820 q^7 + 41\,239 q^6 + 11\,426 q^5 + 2\,677 q^4 + 492 q^3 + 61 q^2 + 3 q$,
- Valor del polinomio $q = 1$: 60 779 787,
- Polinomio con el mayor valor (cuando $q=1$) descubierto hasta el presente (mayo de 2007) : $1\,583 q^{22} + 18\,668 q^{21} + 127\,878 q^{20} + 604\,872 q^{19} + 2\,040\,844 q^{18} + 4\,880\,797 q^{17} + 8\,470\,080 q^{16} + 11\,143\,777 q^{15} + 11\,467\,297 q^{14} + 9\,503\,114 q^{13} + 6\,554\,446 q^{12} + 3\,862\,269 q^{11} + 1\,979\,443 q^{10} + 896\,537 q^9 + 361\,489 q^8 + 129\,510 q^7 + 41\,211 q^6 + 11\,425 q^5 + 2\,677 q^4 + 492 q^3 + 61 q^2 + 3 q$,
- Valor para un polinomio $q = 1$: 62 098 473.

Notas y referencias

1. ^a ^b AIM math: Representations of E_8

Politopo E_8

Politopo E_8
Grafo vértice-arista

Tipo	Uniforme 8-politopo
Familia	Semirregular E-politopo Semirregular
Símbolo de Schläfli	$t_0\{3^{4,2,1}\}$
diagrama de Coxeter-Dynkin	
7-caras	19440 total: 2160 heptacruces 17280 7-simples
6-caras	207360 6-simples
5-caras	483840 5-simples
4-caras	483840 pentacorones
Celdas	241920 tetraedros
Caras	60480 triangulos
Vértices	6720
Vértices	240
Figura de vértice	Politopo E7: $\{3^{3,2,1}\}$
Grupo de simetría	$E_8, [3^{4,2,1}]$
Propiedadess	Convexo

El **politopo E8** es un politopo E-semirregular posible de dimensiones. Fue Gosset, quien lo describió 1900 como una *figura 8*-queriendo decir por sus facetas son politopos y 17280 simples. Su matemáticas del grupo E8. por H. S. M. Coxeter como Coxeter-Dynkin bifurcante, de la secuencia de 4 nodos. la familia de los 255 (2^8-1) convexos en ocho dimensiones, creado a partir de facetas que son politopos uniformes y figuras de vértice, definidas por todas las permutaciones de los diagramas anillados de Coxeter-Dynkin.

politopo semirregular. Es el finito con el mayor número descubierto por Thorold en un artículo publicado en *oica semirregular*, "semirregular" que todas regulares: 2160 7-ortotopos construcción se basa en las También fue denominado **4₂₁** por su diagrama de con un solo anillo al final Es uno de los miembros de politopos uniformes

Referencias

- T. Gosset: *On the Regular and Semi-Regular Figures in Space of n Dimensions*, Messenger of Mathematics, Macmillan, 1900

- A. Boole Stott: *Geometrical deduction of semiregular from regular polytopes and space fillings*, Verhandelingen of the Koninklijke academy van Wetenschappen width unit Ámsterdam, Eerste Sectie 11,1, Ámsterdam, 1910
- **Kaleidoscopes: Selected Writings of H.S.M. Coxeter**, editado por F. Arthur Sherk, Peter McMullen, Anthony C. Thompson y Asia Ivic Weiss, Wiley-Interscience Publication, 1995, ISBN 978-0-471-01003-6 [1]
 - (Artículo 24) H.S.M. Coxeter, *Regular and Semi-Regular Polytopes III*, [Math. Zeit. 200 (1988) 3-45] ver p347 (figura 3.8c) por Peter McMullen: (30-gonal node-edge graph of 4_{21})

Una teoría del todo excepcionalmente simple

Zoo de partículas

Una partícula más allá del Modelo Estándar en los límites de la física teórica y la física de partículas. En la imagen se muestran algunas partículas supersimétricas y sus propiedades de masa y spin.

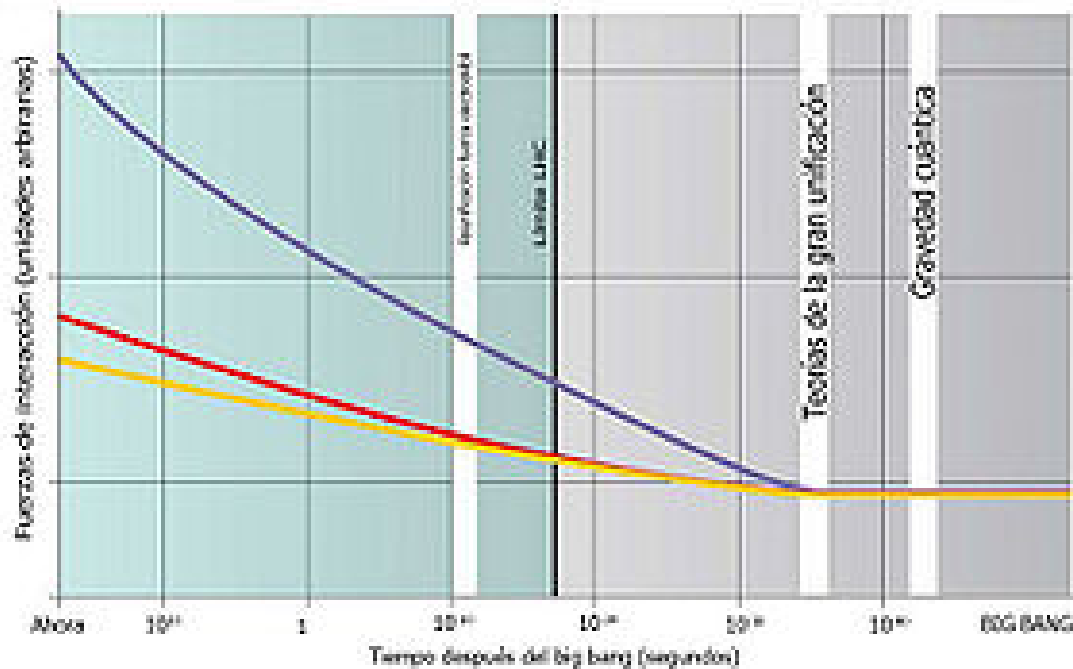


Zoo de partículas en la supersimetría.

Tres fuerzas a partir de una.

Las fuerzas que conocemos hoy tienen diferentes potencias. Pero si se pudiera dar marcha atrás en el tiempo hasta el Big Bang o simular las condiciones dentro de un acelerador de partículas se podría ver como todas parten con una potencia similar y se transforman en una superfuerza.

- Fuerza fuerte**
Mantiene el núcleo atómico junto
Bosón: 8 Gluones
Rango: 10^{-16} m
- Fuerza electromagnética**
Mantiene a los átomos juntos
causa el magnetismo
Bosón: Fotón
Rango: infinito
- Fuerza débil**
Causa radioactividad
Decaimiento Beta
Bosones: W^+ , W^- , Z^0
Rango: 10^{-18} m



Convergencia de las tres fuerzas. Se marca la energía máxima del LHC.

Una teoría del todo excepcionalmente simple¹

(*An Exceptionally Simple Theory of Everything* en inglés) es el título de un artículo de física teórica enviado a arXiv library el 6 de noviembre de 2007 por Antony Garrett Lisi. El artículo es aún más sorprendente por cuanto su autor no pertenece al mundo habitual de la física académica, sino que se dedica la mayor parte del año a la práctica del surf en Hawái.² Su Teoría del todo afirma que puede unificar todos los campos del modelo estándar con la gravedad utilizando una red de 248 puntos (red de geometría E_8). Aún no se ha sometido a una revisión por pares ni publicada en ninguna revista científica académica; no obstante, ha producido un gran revuelo y reacciones variadas, al tiempo que ha atraído el interés del público por el mismo y por su autor. Lisi advierte que la teoría está incompleta y que "terminará siendo la correcta o bien una especulación errónea."³ Así pues, a diferencia de la mayoría de las teorías de cuerdas, es verificable en un futuro próximo, cuando el Gran Colisionador de Hadrones comience a estar operativo. El título es una paronomasia matemática sobre la clasificación de la geometría E_8 , como grupo simple y como grupo excepcional.

paronomasia.

(Del lat. *paronomasia*, y este del gr. *παρονομασία*).

1. f. Semejanza entre dos o más vocablos que no se diferencian sino por la vocal acentuada en cada uno de ellos; p. ej., *azar* y *azor*; *lago*, *lego* y *Lugo*; *jácara* y *jícara*.
2. f. Semejanza de distinta clase que entre sí tienen otros vocablos; p. ej., *adaptar* y *adoptar*; *acera* y *acero*. *Marte* y *mártir*.
3. f. Conjunto de dos o más vocablos que forman **paronomasia**.
4. f. *Ret.* Figura consistente en colocar próximos en la frase dos vocablos semejantes en el sonido pero diferentes en el significado, como *puerta* y *puerto*; *secreto de dos* y *secreto de Dios*.

Panorama global

De acuerdo con Lisi, las matemáticas que logran describir el universo se expresarían en una hermosa estructura matemática unificada, concisa y elegante y al mismo tiempo consistente con la experiencia. En la teoría de campo, todas las propiedades observables de las partículas fundamentales se pueden comprender como resultado de operaciones que actúan en un campo cuya base es el conjunto de estados cuánticos permitidos. Las matemáticas de tales campos se rigen por ciertas reglas (es decir, las relaciones de conmutación que definen cómo se permite que interactúen las partículas) y además se debe especificar un principio matemático, conocido como el principio de acción, que rige la forma en que los estados pueden evolucionar con el tiempo. Previamente, la teoría cuántica de campo había sido capaz de identificar las propiedades del modelo estándar de las partículas elementales en correspondencia con las matemáticas de los bien conocidos grupos de Lie, específicamente el $SU(3)$ para la Fuerza nuclear fuerte y la $SU(2) \times U(1)$ para la fuerza electrodébil. Además, las matemáticas de la relatividad general son equivalentes a las del grupo de Lorentz, $SO(3,1)$.

El trabajo de Lisi identifica un mecanismo por el cual las matemáticas de todas las fuerzas a las que nos hemos referido antes y sus partículas fundamentales asociadas quedan incluidas dentro del marco matemático de las matemáticas E_8 , que es el mayor de los grupos de Lie simples. También especifica una acción para la estructura resultante que, si fuera correcta, proporcionaría el marco para la coevolución de las interacciones cuánticas y gravitacionales, proporcionando una solución para el problema de la gravedad cuántica. Puesto que la acción que especifica contiene las relaciones

normales tanto de la mecánica cuántica como de la relatividad, este aspecto de la teoría es intrínsecamente consistente con ambos reinos de la física establecida en los límites donde cada una de ellas es aplicable por separado. Además, una consecuencia natural de la ensayabilidad en E_8 es que tendría que haber exactamente tres familias de fermiones. La presencia de las tres familias está bien establecida experimentalmente, pero el Modelo Estándar no nos proporciona una explicación de por qué hay exactamente tres.

Esta inclusión de Lisi no admite parámetros libres. Predice necesariamente como consecuencia de esta inclusión y de la estructura de E_8 el número exacto de las partículas fundamentales, todas sus propiedades, sus masas, las fuerzas entre ellas, la naturaleza del espacio-tiempo y la constante cosmológica. Se fuerza a que las propiedades de la mecánica cuántica sean ciertas por construcción, mientras que las masas tendrían que ser determinables, en principio, por medición del valor esperado de los estados fundamentales del componente de Higgs de este campo. No obstante, los cálculos que se requieren para efectuar esto son extremadamente complicados y no han sido intentados antes de la publicación. Además, la unificación de Lisi es probable que no sea la única posible. El autor unificó los términos de la mecánica cuántica dentro de E_8 de un modo que minimiza la mezcla entre estados. Es probable que se puedan construir otras inclusiones "menos elegantes" que unirían la mecánica cuántica y la relatividad dentro de E_8 pero que dieran lugar a predicciones diferentes para las masas de las partículas. Lisi advierte que su teoría es incompleta. "La teoría es muy joven y aún se encuentra en desarrollo. Ahora mismo, asignaría una probabilidad baja (pero no insignificante) para esta predicción."⁴ "Este es un tipo de teoría del todo o nada, puesto que acabará siendo totalmente correcta o espectacularmente errónea. Soy el primero en admitir que esto es un buen intento. Pero no está dicha la última palabra hasta que el LHC termine de hablar."³

Nuevas partículas

En la teoría de Lisi, existirían 20 elementos a partir de los 248 elementos base del grupo de Lie E_8 que no corresponde con partículas o fuerzas conocidas. Esto requeriría la existencia de nuevas interacciones y partículas, aunque el número exacto de nuevas partículas dependería de la mezcla de estos estados básicos con los de las partículas convencionales conocidas (tal mezcla se define exactamente por la estructura de E_8 pero aún no ha sido determinada). Los nuevos campos incluyen dos nuevos números cuánticos en el modelo de Pati-Salam, un nuevo escalar de Higgs, así como nuevos campos que mezclan los leptones y los quarks y tiene fuerzas que varían dependiendo de la familia de fermiones. Por todo esto, la teoría también predice la descomposición del protón. Para ser consistente con las observaciones previas, Lisi sugiere que las masas de algunas de las partículas extra resultantes serían necesariamente demasiado grandes para haber sido observadas por los actuales aceleradores de partículas. La masa de al menos una de estas partículas estaría teóricamente dentro del rango detectable del LHC que ya se halla en servicio.^{1 5}

Recepción

En su blog, el físico Peter Woit escribe: "Me alegro de ver a alguien que persigue estas ideas, incluso si no se plantea soluciones a los problemas subyacentes." Woit describió los ataques personales a Lisi al poco de aparecer su artículo como deprimentes. "Garret es un investigador serio y competente que ha seguido una carrera no convencional y recientemente obtuvo una beca por el instituto para cuestiones fundamentales." (FQXI)⁶

Sabine Hossenfelder del Instituto "Perímetro" de Física Teórica Perimeter Institute for Theoretical Physics, que recientemente invitó a Lisi a una reunión internacional sobre gravedad cuántica de

bucles y a la cual Lisi agradece en su artículo el haber sido una correspondiente útil, hace hincapié en las limitaciones del trabajo:

Dado su estado actual,

- El modelo de Garrett no conduce naturalmente a la unificación de las interacciones del modelo estándar con la gravedad (Él tuvo que elegir la acción entre dos; en su publicación sólo se describe uno de los modos posibles, siendo esto explicado por el mismo Lisi),
- No nos permite comprender la gravedad cuántica (puesto que no nos dice nada sobre la cuantificación);
- No explica los parámetros del modelo estándar (porque no hay aún ningún mecanismo para la ruptura de la simetría);
- No explica la constante cosmológica o su valor (como se dice más arriba, para afirmar que tenga que existir, sería necesario mostrar que no habría otra forma de hacerlo sin que hubiera una);
- No explica la jerarquía del problema (Y no veo forma de hacerlo);
- No explica por qué vivimos en un espacio-tiempo con tres dimensiones espaciales y una dimensión tipo-tiempo.⁷

Estas limitaciones, que han sido ampliamente relacionadas con las asunciones adicionales que el modelo requiere respecto de la acción para dar las ecuaciones correctas del movimiento, están equilibradas en su visión, en el lado positivo, por el modo en que los grupos de Lie se usan para unificar los bosones con los fermiones. La investigadora también tiene preocupaciones técnicas por la falta de constantes de acoplamiento en el artículo, que de este modo parece basarse en sacar una longitud de escala característica de la nada. No obstante, finalmente afirma la revisora "Pienso que el artículo de Garret tiene el potencial de convertirse en una contribución muy especial, y su enfoque merece más examen."⁸

Marcus du Sautoy de la Universidad de Oxford dice: "Parece que le faltan muchas cosas"⁹ y un teórico de cuerdas Luboš Motl dice que "Cualquier investigador senior entusiasmado por la física sería capaz de ver que solo es una larga secuencia de malentendidos infantiles."¹⁰ Motl argumenta que es imposible tener una teoría con simetrías internas y externas unificadas en cualquier forma no trivial. Motl afirma que el artículo de Lisi viola el teorema de Coleman-Mandula, aunque Lisi asevera explícitamente que los presupuestos del teorema no son aplicables a su trabajo.¹¹

El físico Lee Smolin del Perimeter Institute for Theoretical Physics, un crítico con la teoría de cuerdas, describió el trabajo como "uno de los modelos de unificación más convincentes que he visto en muchos, muchos años."⁴

El profesor emérito David Finkelstein del Instituto de tecnología de Georgia dice "Pienso que todo esto debe ser más que una coincidencia y creo que está tocando algo profundo."⁵

Uno de los teóricos más importantes en gravedad cuántica Carlo Rovelli comentó "Cuando comencé a leer el artículo era escéptico. Cuando terminé, me pregunté porqué no se me había ocurrido la idea antes." ¹²

Referencias

1. ↑ ^{a b} A. Garrett Lisi, An Exceptionally Simple Theory of Everything (PDF format), Cornell University Library, Enviado el 6 Nov 2007
2. ↑ Personalidad de Lisi en New Scientist, [1], New Scientist, acceso 17/11/2007
3. ↑ ^{a b} «Is mathematical pattern the theory of everything? - fundamentals - 15 November 2007 - New Scientist». Consultado el 18-11-2007.
4. ↑ ^{a b} Surfer dude stuns physicists with theory of everything - Telegraph
5. ↑ ^{a b} Is mathematical pattern the theory of everything? - fundamentals - 15 November 2007 - New Scientist
6. ↑ Not Even Wrong » Blog Archive » An Exceptionally Simple Theory of Everything?
7. ↑ Backreaction: A Theoretically Simple Exception of Everything
8. ↑ Backreaction: A Theoretically Simple Exception of Everything
9. ↑ FOXNews.com - Laid-Back Surfer Dude May Be Next Einstein - Science News | Science & Technology | Technology News
10. ↑ The Reference Frame: Garrett Lisi: An exceptionally simple theory of everything
11. ↑ Backreaction: A Theoretically Simple Exception of Everything
12. ↑ A "theory of everything" causes trouble with the physicists, *Le Monde*, 19 November, 2007. (French)

Grupo uniparamétrico

En matemáticas, un **grupo uniparamétrico** o **subgrupo uniparamétrico** es un subconjunto de un grupo de Lie de dimensión uno. De hecho un grupo uniparamétrico puede ser representado por una colección $\{\varphi_t \in G | t \in I \subset \mathbb{R}\}$ de "operadores" o elementos de un grupo (G, \cdot) , que vienen dados por un homomorfismo local de grupo continuo $\varphi: \mathbb{R} \rightarrow G$, de la recta real \mathbb{R} , considerada como grupo aditivo) a otro grupo topológico G . Un homomorfismo local como el anterior se define por las siguientes condiciones:

1. $\varphi_0 = e_G$
2. $\exists(-t_0, t_0) \subset I_0 \subset I : (\forall s, t \in I_0 : (\varphi_{s+t} = \varphi_s \cdot \varphi_t))$

Grupo uniparamétrico global

Cuando la aplicación que define el subgrupo se puede extender a toda la recta real, es decir, cuando en la definición anterior puede extenderse de modo que $I_0 = \mathbb{R}$, entonces la extensión de φ es un homeomorfismo ordinario y entonces el grupo uniparamétrico no sólo es un subconjunto de un grupo continuo de dimensión uno, sino que toda la colección $\{\varphi_t\}$ es en sí misma un grupo continuo unidimensional.

Un grupo uniparamétrico global puede ser identificado con un grupo de Lie unidimensional.

Ejemplo

La aplicación dada por:

$$\varphi : \mathbb{R} \rightarrow U(1) \subset \mathbb{C} \quad \varphi_s = \exp(2\pi si)$$

Donde $U(1)$ denota el conjunto de números complejos de módulo unidad, que topológicamente puede ser interpretado como el círculo unidad del plano euclídeo; constituye un grupo uniparamétrico local, no trivial y la aplicación φ es un epimorfismo de grupos. En este caso el grupo paramétrico unidimensional es además un grupo de Lie.

Grupos uniparamétricos locales

En matemáticas y sobre todo en física surge la necesidad de considerar grupos de simetría alrededor del operador identidad φ_0 en ese caso usamos morfismos locales que no necesariamente pueden extenderse a morfismos globales.

Grupos uniparamétricos en grupos de Lie

Un caso especialmente extraño son los grupos uniparamétricos son aquellos que aún siendo grupos unidimensionales son densos en un grupo de Lie de dimensión mayor que uno. En ese caso surge la complicación técnica es que $\varphi(\mathbb{R})$ como subespacio de (G, \cdot) tiene una topología más gruesa que la de la recta real ordinaria, al ser φ inyectivo.

Un ejemplo de esto es la aplicación de la recta real sobre el toro:

$$\varphi : \mathbb{R} \rightarrow S^1 \times S^1 \quad \varphi_s = (e^{(2\pi r_0)si}, e^{2\pi si})$$

Donde r_0 es un número irracional. El grupo uniparamétrico identificado con el conjunto imagen de la aplicación anterior se enrolla y se enrolla sobre el toro indefinidamente sin intersectarse a sí mismo formando un conjunto denso en el toro que se distingue del toro por tres razones:

- Tiene una parametrización definida,
- El homomorfismo de grupos puede no ser inyectivo, y
- La topología inducida puede no ser la estándar de la recta real.

Grupos uniparamétricos en física

Puede probarse que el conjunto de grupos uniparamétricos locales que mantienen la simetría o invariancia de un cierto problema físico está generado por un elemento de un álgebra de Lie.

Teorema de Noether

El teorema de Noether permite construir integrales de movimiento o leyes de conservación a partir de elementos del álgebra de Lie que genera todos los grupos uniparamétricos que son simetrías locales del problema físico.

Operadores unitarios en mecánica cuántica

Tales grupos uniparamétricos son de importancia básica en la teoría de los grupos de Lie, para quienes cada elemento del álgebra de Lie asociada define tal homomorfismo, la función exponencial. En el caso de grupos matriciales viene dado por la exponencial de matrices.

Otro caso importante se ve en el análisis funcional, con G siendo el grupo de los operadores unitarios en un espacio de Hilbert.

Grupo abeliano

Dada una estructura algebraica sobre un conjunto A , y con una operación o ley de composición interna binaria: " \circ ". Se dice que la estructura (A, \circ) es un **Grupo abeliano** con respecto a la operación \circ si:

1. (A, \circ) tiene estructura algebraica Grupo
2. (A, \circ) tiene la Propiedad conmutativa

Los grupos abelianos son así llamados en honor al matemático noruego Niels Henrik Abel. Los grupos que no son conmutativos se denominan **no abelianos** (también *no conmutativos*, con menos frecuencia).

Notación

Hay dos notaciones principales para los grupos abelianos: aditiva y multiplicativa, descritas a continuación.

Notación	Operación	Elemento neutro	Potencias	Elementos inversos	Suma directa / producto directo
Adición	$a + b$	0	a^n	$-a$	$G \oplus H$
Multiplicación	$a * b$ ó ab	e ó 1	a^n	a^{-1} ó $1/a$	$G \times H$

La notación multiplicativa no es otra que la notación usual para los grupos, mientras que la aditiva es la notación usual para módulos. Cuando se trabaja sólo con grupos abelianos, usualmente se usa la notación aditiva.

Ejemplos

Todo grupo cíclico G es abeliano, pues si $x, y \in G = \langle a \rangle$, $x = a^m$ y $y = a^n$ para algunos m, n enteros, con lo cual, $xy = a^m a^n = a^{m+n} = a^{n+m} = a^n a^m = yx$. En particular, el grupo \mathbf{Z} de enteros bajo la suma es abeliano, al igual que el grupo de enteros módulo n , \mathbf{Z}_n .

Los números reales forman un grupo abeliano con la adición, al igual que los reales no nulos con la multiplicación.

Todo anillo es un grupo abeliano con respecto a su adición. En un anillo conmutativo, los elementos invertibles forman un grupo abeliano bajo la multiplicación.

Todo subgrupo de un grupo abeliano es normal, y por lo tanto, para todo subgrupo hay un grupo cociente. Subgrupos, grupos cocientes, y sumas directas de grupos abelianos son también abelianos.

Propiedades

- Si n es un número natural y x un elemento de un grupo abeliano G (con notación aditiva), se puede definir $nx = x + x + \dots + x$ (n sumandos), y $(-n)x = -(nx)$, con lo que G se vuelve un módulo sobre el anillo \mathbf{Z} de los enteros. De hecho, los módulos sobre \mathbf{Z} no son otros que los grupos abelianos.
- Si $f, g : G \rightarrow H$ son dos homomorfismos entre grupos abelianos, su suma (definida por $(f+g)(x) = f(x) + g(x)$) es también un homomorfismo; esto no se cumple en general para grupos no abelianos. Con esta operación, el conjunto de homomorfismos entre G y H se vuelve, entonces, un grupo abeliano en sí mismo.

Anillo

En álgebra, un **anillo** es una estructura algebraica formada por un conjunto (A) , y dos operaciones: suma y producto; de modo que $(A, +)$ es un grupo conmutativo con elemento neutro (que designamos 0), y el producto es asociativo, posee neutro, llamado unidad (que designamos 1), y tiene la propiedad distributiva respecto de la suma. Si además el producto es conmutativo hablaremos de un anillo conmutativo.

Ejemplo de un anillo

El ejemplo más intuitivo de un anillo es el conjunto de los números enteros:

... -4, -3, -2, -1, 0, 1, 2, 3, 4, ...

junto con las operaciones binarias de la suma y la multiplicación. La razón por la cual estas tres cosas forman un anillo, es porque cumplen con las siguientes propiedades:

1. Los números enteros están cerrados bajo la suma: dados dos números enteros a y b , se cumple que $a + b$ es un número entero.
2. La suma es asociativa: dados tres números enteros a , b y c , se cumple que $(a + b) + c = a + (b + c)$.
3. Existe un elemento neutro para la suma: para todo número entero a , $a + 0 = 0 + a = a$.
4. Existe un elemento simétrico para la suma: para todo número entero a , siempre existe algún número entero b , tal que $a + b = 0$.
5. La suma es conmutativa: dados dos números enteros a y b , se cumple que $a + b = b + a$.
6. Los números enteros están cerrados bajo la multiplicación: dados dos números enteros a y b , se cumple que $a \times b$ es un número entero.
7. La multiplicación es asociativa: dados tres números enteros a , b y c , se cumple que $(a \times b) \times c = a \times (b \times c)$.
8. Existe un elemento neutro para la multiplicación: para todo número entero a , $a \times 1 = a$.
9. La multiplicación es distributiva respecto de la suma: $a \times (b + c) = (a \times b) + (a \times c)$.

Definición formal

Sea A un conjunto no vacío perteneciente al conjunto, y sean \star y \circ dos operaciones binarias. Se dice que el conjunto (A, \star, \circ) es un **anillo** si se cumplen las siguientes propiedades:

- | | |
|---|--|
| 1. A es cerrado bajo la operación \star . | $\forall a, b \in A, a \star b \in A$ |
| 2. La operación \star es asociativa. | $\forall a, b, c \in A, (a \star b) \star c = a \star (b \star c)$ |
| 3. La operación \star tiene a n como elemento neutro. | $\forall a \in A, a \star n = n \star a = a$ |
| 4. Existe un elemento simétrico para \star . | $\forall a \in A, \exists b \in A, a \star b = b \star a = n$ |

Estas cuatro condiciones definen un grupo. Una quinta condición define un grupo abeliano:

- | | |
|---|---|
| 5. La operación \star es conmutativa. | $\forall a, b \in A, a \star b = b \star a$ |
|---|---|

Para definir un anillo, es necesario agregar tres condiciones más que hablan acerca de la segunda operación binaria:

- | | |
|---|---|
| 6. A es cerrado bajo la operación \circ . | $\forall a, b \in A, a \circ b \in A$ |
| 7. La operación \circ es asociativa. | $\forall a, b, c \in A, (a \circ b) \circ c = a \circ (b \circ c)$ |
| 8. La operación \circ es distributiva respecto de \star . | $\forall a, b, c \in A, \begin{cases} a \circ (b \star c) = (a \circ b) \star (a \circ c) \\ (a \star b) \circ c = (a \circ c) \star (b \circ c) \end{cases}$ |

Y agregando una novena condición, se define un anillo conmutativo:

- | | |
|---|---|
| 9. La operación \circ es conmutativa. | $\forall a, b \in A, a \circ b = b \circ a$ |
|---|---|

Elementos destacados en un anillo

- **Elemento cero:** denotado por 0. Es el neutro para la suma.
- **Elemento unitario:** si un elemento, que denotamos 1, cumple $1 \cdot a = a \cdot 1 = a$ para todo elemento a del anillo, se llama elemento unitario.

El elemento cero y el elemento unitario sólo coinciden en el caso de que el anillo sea trivial ($\{0\}$), debido a la propiedad distributiva.

- **Inverso multiplicativo:** si estamos en un anillo que posea un elemento unitario, b es **inverso multiplicativo por la izquierda** (o sencillamente **inverso por la izquierda**) de a si $b \cdot a = 1$. Así mismo, c es inverso multiplicativo por la derecha (o sencillamente inverso por la derecha) de a si $a \cdot c = 1$. Un elemento a^{-1} se dirá que es inverso multiplicativo (o sencillamente inverso) de a si a^{-1} es inverso por la izquierda de a e inverso por la derecha de a , es decir, $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Si existe el inverso de un elemento, entonces es único (lo que justifica llamarlo **el** inverso).

- **Elemento inversible**, o **elemento invertible** o **unidad**: es todo aquel elemento que posee inverso multiplicativo.
- **Divisor del cero:** un elemento $a \neq 0$ es divisor del cero por la izquierda, si existe algún b distinto de 0, tal que $a \cdot b = 0$. Lo es por la derecha si existe un c distinto de 0 tal que $c \cdot a = 0$. Se dirá que a es divisor del cero, si lo es tanto por la derecha como por la izquierda.
- **Elemento regular:** un elemento $a \neq 0$ de un anillo es regular si no es divisor de cero. Todo elemento invertible es regular.
- **Elemento idempotente:** es cualquier elemento e del anillo que al multiplicarse por sí mismo no varía, es decir, tal que $e \cdot e = e$ (esto se suele escribir como $e^2 = e$). El cero es siempre idempotente en un anillo, y si el anillo es unitario, también el 1 es idempotente.
- **Elemento nilpotente** (o **nihilpotente**): es cualquier elemento x del anillo para el que existe un número natural n de forma que $x^n = 0$ (donde x^n se define por recurrencia: $x^0 = 1$, $x^n = x \cdot x^{n-1}$). El 0 es siempre un nilpotente de cualquier anillo. Todo elemento nilpotente es divisor de cero.

Algunos tipos importantes de anillos

- **Anillo conmutativo:** aquel en el que el producto es conmutativo, esto es, $a \cdot b = b \cdot a$ para todos a y b (no debe confundirse con **anillo abeliano**).
- **Anillo unitario:** aquel que posee un elemento unitario y además, éste es distinto del neutro de la suma.
- **Anillo de división:** es el anillo en el cual todo elemento, a excepción del 0, tiene inverso.

- **Anillo con leyes de simplificación:** aquel en el que se cumplen las leyes de simplificación. Si un anillo no tiene divisores del cero, se cumplen las leyes de simplificación, y el recíproco también es cierto.
- **Dominio de integridad:** si un anillo no posee divisores del cero, es un dominio de integridad (a menudo se suele exigir que además se trate de anillos conmutativos y unitarios, pero esta exigencia no es aceptada por todos los autores).
- **Cuerpo:** se trata de un anillo de división conmutativo.
- **Anillo abeliano:** es un anillo en el que todo elemento idempotente pertenece al centro del anillo, es decir, todo elemento idempotente conmuta con cualquier elemento del anillo.

Subconjuntos notables

Subanillos e ideales

Un **subanillo** S de un anillo $R = (A, +, \cdot)$ es un subconjunto $S \subset R$ que cumple que es cerrado para la suma y la multiplicación en el anillo, esto es, si $a, b \in S$, entonces $a + b \in S$ y $a \cdot b \in S$. Si $1 \in R$ (es decir, si el anillo es unitario), entonces se exigirá además que $1 \in S$. Nótese que en este caso, cuando el anillo es unitario, $\{0\}$ no será subanillo de R , y sí lo será si R no es unitario.

Un subanillo S es propio cuando no coincide con todo el anillo, es decir, si $R \neq S$.

Resulta pues que un subanillo es un anillo dentro de otro anillo (para las mismas operaciones). En particular, $(S, +)$ es un subgrupo de $(R, +)$.

Pero en la Teoría de Anillos hay un tipo de subconjunto más notable aun que el de subanillo, el de ideal.

Un subconjunto $I \subset R$ es **ideal por la izquierda** de un anillo $(A, +, \cdot)$ si $(I, +)$ es subgrupo de $(R, +)$ y dados cualesquiera $r \in R$ y $x \in I$ se tiene que $r \cdot x \in I$.

Un subconjunto $I \subset R$ es **ideal por la derecha** de un anillo $(A, +, \cdot)$ si $(I, +)$ es subgrupo de $(R, +)$ y dados cualesquiera $r \in R$ y $x \in I$ se tiene que $x \cdot r \in I$.

Cuando un subconjunto I es ideal por la derecha e ideal por la izquierda se dice que es un **ideal bilátero (del anillo)**, o simplemente que es un **ideal (del anillo)**.

La propiedad conmutativa nos asegura que en todo anillo conmutativo todo ideal por la izquierda es ideal por la derecha, y todo ideal por la derecha es ideal por la izquierda, esto es, todos los ideales (por la izquierda o por la derecha) de un anillo conmutativo son ideales biláteros.

Un ideal I (por la izquierda, por la derecha o bilátero) se dice que es propio si es distinto de todo el anillo, esto es, $I \neq R$.

Unidades

Al conjunto de elementos invertibles de un anillo unitario $(R, +, \cdot, 1_R)$ se le llama **conjunto de unidades (del anillo)**, y se le denota por $U(R)$.

Si I es ideal (por la izquierda, por la derecha o bilátero) propio de un anillo unitario $U(R)$, entonces $I \cap U(R) = \emptyset$, esto es, ningún ideal propio tiene elementos invertibles. En particular, ningún ideal (por la izquierda, por la derecha o bilátero) propio tiene por elemento al 1, lo que impide a los ideales ser subanillos de anillos unitarios.

Centro

El centro de un anillo $(R, +, \cdot)$ (denotado por $Z(R)$) es el conjunto de elementos que conmutan para el producto, es decir $Z(R) := \{r \in R : r \cdot s = s \cdot r, \forall s \in R\}$. El centro de un anillo viene a ser como "la parte conmutativa del anillo". Nótese que siempre se tiene que $0 \in Z(R)$. Los anillos conmutativos son aquellos que coinciden con su centro, i.e., $R = Z(R)$.

Anillo conmutativo

En teoría de anillos (una rama del álgebra abstracta), un **anillo conmutativo** es un anillo $(R, +, \cdot)$ en el que la operación de multiplicación \cdot es conmutativa; es decir, si para cualesquiera $a, b \in R$, $a \cdot b = b \cdot a$.

Si adicionalmente el anillo tiene un elemento unitario 1 tal que $1a = a = a1$ para todo a , entonces el anillo se denomina **anillo conmutativo unitario**.

La rama de la teoría de anillos que estudia los anillos conmutativos se denomina **álgebra conmutativa**.

Ejemplos

- El ejemplo más importante es tal vez el de los números enteros con las operaciones usuales de suma y multiplicación, ambas conmutativas. Este anillo usualmente se denota por \mathbf{Z} , por la palabra alemana *Zahlen* (números).
- Los números racionales, reales, y complejos forman anillos conmutativos con las operaciones usuales; más aún, son campos.
- Más generalmente, todo campo es un anillo conmutativo por definición.
- El mejor ejemplo de un anillo **no** conmutativo es el conjunto de matrices cuadradas de 2×2 con valores reales. Por ejemplo, la multiplicación matricial

Pseudoanillo

En matemáticas entendemos por **pseudoanillo** una Estructura algebraica de la forma

$$\mathbf{R} = \langle R, +, * \rangle$$

donde R es un conjunto, la base del pseudoanillo, $+$ y $*$ son operaciones binarias y existe 0 , un elemento del conjunto, el zero del pseudoanillo, tal que

$\langle R, + \rangle$ es un Grupo abeliano

$\langle R, +, * \rangle$ es un semianillo.

Las operaciones $+$ y $*$ se dicen respectivamente suma y producto del pseudoanillo.

Cuando el producto de un pseudoanillo posee una unidad, que notamos con 1 , es decir, cuando $\langle R, * \rangle$ es un monoide,

$\langle R, +, * \rangle$

es una estructura llamada anillo.

Si el producto de un pseudoanillo es conmutativo, la estructura se llama pseudoanillo abeliano.

Cuerpo

En álgebra abstracta, un **cuerpo** o **campo** es una estructura algebraica en la cual las operaciones de adición y multiplicación se pueden realizar y cumplen las propiedades asociativa, conmutativa y distributiva, además de la existencia de un inverso aditivo y de un inverso multiplicativo, los cuales permiten efectuar las operaciones de sustracción y división (excepto la división por cero); estas propiedades ya son familiares de la aritmética de números ordinarios.

Los cuerpos son objetos importantes de estudio en álgebra puesto que proporcionan la generalización apropiada de dominios de números tales como los conjuntos de números racionales, de los números reales, o de los números complejos. Los cuerpos eran llamados **dominios racionales**.

El concepto de un cuerpo se usa, por ejemplo, al definir el concepto de espacio vectorial y las transformaciones en estos objetos, dadas por matrices, dos objetos en el álgebra lineal cuyos componentes pueden ser elementos de un cuerpo arbitrario. La teoría de Galois estudia las relaciones de simetría en las ecuaciones algebraicas, desde la observación del comportamiento de sus raíces y las extensiones de cuerpos correspondientes y su relación con los automorfismos de cuerpos correspondientes.

Definición

Un cuerpo es un anillo de división conmutativo, es decir, un anillo conmutativo en el que todo elemento distinto de cero es invertible respecto del producto. Por tanto un cuerpo es un conjunto F en el que se han definido dos operaciones, $+$ y $$, llamadas *suma* y *multiplicación* respectivamente, que cumplen las siguientes propiedades:*

F es cerrado para la suma y la multiplicación

Para toda a, b en F , $a + b$ y $a * b$ pertenecen a F (o más formalmente, $+$ y $*$ son operaciones matemáticas en F);

Asociatividad de la suma y la multiplicación

Para toda a, b, c en F , $a + (b + c) = (a + b) + c$ y $a * (b * c) = (a * b) * c$.

Conmutatividad de la suma y la multiplicación

Para toda a, b en F , $a + b = b + a$ y $a * b = b * a$.

Existencia de un elemento neutro para la suma y la multiplicación

Existe un elemento 0 en F , tal que para todo a en F , $a + 0 = a$.

Existe un elemento 1 en F diferente a 0 , tal que para todo a en F , $a * 1 = a$.

Existencia de elemento opuesto y de inversos

Para cada a en F , existe un elemento $-a$ en F , tal que $a + (-a) = 0$.

Para cada $a \neq 0$ en F , existe un elemento a^{-1} en F , tal que $a * a^{-1} = 1$.

Distributividad de la multiplicación respecto de la suma

Para toda a, b, c , en F , $a * (b + c) = (a * b) + (a * c)$.

El requisito $a \neq 0$ asegura que el conjunto que contiene solamente un cero no sea un cuerpo, y de paso elimina la posibilidad de que en el cuerpo existan divisores de cero distintos de 0 . Directamente de los axiomas, se puede demostrar que $(F, +)$ y $(F - \{0\}, *)$ son grupos conmutativos y que por lo tanto (véase la teoría de grupos) el opuesto $-a$ y el inverso a^{-1} son determinados únicamente por a . Además, el inverso de un producto es igual al producto de los inversos:

$$(a * b)^{-1} = a^{-1} * b^{-1}$$

con tal que a y b sean diferentes de cero. Otras reglas útiles incluyen

$$-a = (-1) * a$$

y más generalmente

$$-(a * b) = (-a) * b = a * (-b)$$

así como

$$a * 0 = 0,$$

todas reglas familiares de la aritmética elemental.

Cuerpo de escalares

Se define así al conjunto de números que son elementos de un cuerpo algebraico, sea real o complejo.

Otra acepción: Campo escalar o Campo de escalares.

Subcuerpos e ideales

Sea $(K, +, \cdot)$ un cuerpo, y $E \subset K$. Se dice que E es **subcuerpo** de K o que K es extensión de E si se cumple que $(E, +, \cdot)$ es un cuerpo cuando las operaciones $(+)$ y (\cdot) se restringen a E . En

particular, E será entonces un subanillo de $(K, +, \cdot)$. Se tiene entonces que $(E, +)$ y $(E \setminus \{0\}, \cdot)$ son subgrupos respectivos de los grupos abelianos $(K, +)$ y $(K \setminus \{0\}, \cdot)$.

Como todo cuerpo es un anillo, podríamos preguntarnos por la forma que tengan sus ideales. Para empezar, como todo cuerpo es anillo conmutativo, todo ideal por la izquierda es ideal (bilátero) y todo ideal por la derecha es también ideal (bilátero). Así pues sólo hemos de estudiar los ideales del cuerpo.

Si I es ideal del cuerpo K , entonces todo elemento no nulo $a \in K$ ha de tener inverso, $a^{-1} \in K$, luego a es una unidad de K [esto es, $a \in U(K)$], y se tendrá que $I \cap U(K) \neq \emptyset$, es decir, $I = R$. De esta manera, los únicos ideales de un cuerpo son el propio cuerpo y el ideal nulo.

Propiedades de los cuerpos

- Todo cuerpo es dominio de integridad
- Si $(K, +, \cdot)$ es un cuerpo, entonces, $(K, +)$ y $(K \setminus \{0\}, \cdot)$ son grupos abelianos

Ejemplos de cuerpos

- Los números racionales $\mathbb{Q} = \{\frac{a}{b} | a, b \in \mathbb{Z}, b \neq 0\}$ donde está incluido el conjunto \mathbb{Z} de los números enteros.
- Los números reales \mathbb{R} .
- Los números complejos \mathbb{C} .
- El cuerpo más pequeño tiene solamente dos elementos: 0 y 1. Es denotado por \mathbb{F}_2 o \mathbb{Z}_2 puede a veces ser definido por las dos tablas

+	0	1		*	0	1
0	0	1		0	0	0
1	1	0		1	0	1

Tiene aplicaciones importantes en informática, especialmente en criptografía y teoría de la codificación.

- Más generalmente, para un número primo p , el conjunto de los *números enteros* módulo p es un cuerpo finito con los p elementos: esto se escribe a menudo como $\mathbb{Z}_p = \{0, 1, \dots, p-1\}$ donde las operaciones son definidas realizando la operación en \mathbb{Z} , dividiendo por p y tomando el resto, ver aritmética modular.
- Los números reales contienen varios subcuerpos interesantes: los números reales algebraicos, los números computables, y los números definibles.

- Los números complejos contienen el cuerpo de números algebraicos, la clausura algebraica de \mathbb{Q} .
- Los números racionales se pueden ampliar a los cuerpos de números p -ádicos para cada número primo p .
- Sean E y F dos cuerpos con E un **subcuerpo** de F (es decir, un subconjunto de F que contiene 0 y 1, cerrado bajo las operaciones $+$ y $*$ de F y con sus propias operaciones definidas por restricción). Sea x un elemento de F no en E . Entonces $E(x)$ se define como el subcuerpo más pequeño de F que contiene a E y a x . Por ejemplo, $\mathbb{Q}(i)$ es el subcuerpo de los números complejos \mathbb{C} que consisten en todos los números de la forma $a+bi$ donde a y b son números racionales.
- Para un cuerpo dado F , el conjunto $F(x)$ de funciones racionales en la variable X con coeficientes en F es un cuerpo; esto se define como el conjunto de cocientes de polinomios con coeficientes en F .
- Si F es cuerpo, y $p(X)$ es un polinomio irreducible en un anillo de polinomios $F[X]$, entonces el cociente $F[X]/\langle p(X) \rangle$ es un cuerpo con un subcuerpo isomorfo a F . Por ejemplo, $\frac{\mathbb{R}[x]}{\langle x^2 + 1 \rangle}$ es un cuerpo (de hecho, es isomorfo al cuerpo de los números complejos).
- Cuando F es un cuerpo, el conjunto $F((x))$ de series formales de Laurent sobre F es un cuerpo.
- Si V es una variedad algebraica sobre F , entonces las funciones racionales $V \rightarrow F$ forman un cuerpo, el cuerpo de funciones V .
- Si S es una superficie de Riemann, entonces las funciones meromorfas de $S \rightarrow \mathbb{C}$ forman un cuerpo.
- Si I es un conjunto de índices, U es un ultrafiltro sobre I , y F_i es un cuerpo para cada i en I , el ultraproducto de F_i (usando U) es un cuerpo.
- Los números hiperreales forman un cuerpo que contiene los reales, más los números infinitesimales e infinitos.
- Los números surreales forman un cuerpo que contiene los reales, a excepción del hecho de que son una clase propia, no un conjunto. El conjunto de todos los números surreales con el cumpleaños menor que un cierto cardinal inaccesible es un cuerpo.
- Los nimbers forman un cuerpo, otra vez a excepción del hecho de que son una clase propia. El conjunto de nimbers con el cumpleaños menor que 2^{\aleph_1} , los nimbers con el cumpleaños menor que cualquier cardinal infinito son todos ejemplos de cuerpos.

Algunos teoremas iniciales

- El conjunto de elementos diferentes de cero de un cuerpo F (denotado típicamente por F^\times) es un grupo abeliano bajo multiplicación. Cada subgrupo finito de F^\times es cíclico.
- La característica de cualquier cuerpo es cero o un número primo. (la característica se define como el número entero positivo más pequeño n tal que $n \cdot 1 = 0$, o cero si no existe tal n ; aquí $n \cdot 1$ significa n sumandos $1 + 1 + 1 + \dots + 1$.)
- Si $q > 1$ es una potencia de un número primo, entonces existe (salvo isomorfismo) exactamente un cuerpo finito con q elementos. Además, estos son los únicos cuerpos finitos posibles.
- Como anillo, un cuerpo no tiene ningún ideal excepto $\{0\}$ y sí mismo.
- Todo anillo de división finito es un cuerpo (teorema de Wedderburn)
- Para cada cuerpo F , existe (salvo isomorfismo) un cuerpo único G que contiene a F , es algebraico sobre F , y es algebraicamente cerrado. G se llama la clausura *algebraica* de F .

Construyendo nuevos cuerpos de otros dados

- Si un subconjunto E de un cuerpo $(F, +, *)$ junto con las operaciones $*, +$ restringido a E es en sí mismo un cuerpo, entonces se llama un *subcuerpo* de F . Tal subcuerpo tiene los mismos 0 y 1 que F .
- Dado un cuerpo F , el cuerpo polinómico $F(X)$ es el cuerpo de fracciones de polinomios en X con coeficientes en F , es decir, sus elementos son funciones racionales con coeficientes en F .
- Una extensión algebraica de un cuerpo F es el cuerpo más pequeño que contiene a F y una raíz de un polinomio irreducible $p(X)$ en $F[X]$. Alternativamente, es idéntico al anillo factor $F[X]/\langle p(X) \rangle$, donde $\langle p(X) \rangle$ es el ideal generado por $p(X)$.

Módulo

Definición

Específicamente, un **módulo izquierdo** sobre el anillo R consiste en un grupo abeliano $(M, +)$ y una operación $R \times M \rightarrow M$ (multiplicación escalar, generalmente escrita sólo por yuxtaposición, es decir como rx para r en R y x en M) tal que

Para todo r, s en R , x, y en M , tenemos

1. $(rs)x = r(sx)$
2. $(r+s)x = rx+sx$
3. $r(x+y) = rx+ry$
4. $1x = x$

Generalmente, escribimos simplemente "un R - módulo *izquierdo* M " o ${}_R M$.

Algunos autores^[cita requerida] omiten la condición 4 en la definición general de módulos izquierdos, y llaman a las estructuras definidas antes "módulos izquierdos unitales". En este artículo sin embargo, todos los módulos (y todos los anillos) se presuponen unitales. Por lo general, para módulos, en la mayoría de los textos se considera la condición 4, mientras que para anillos no se supone que exista elemento unidad, excepto que se diga lo contrario.

Un **R módulo derecho** M o M_R se define de forma semejante, sólo que el anillo actúa por la derecha, es decir tenemos una multiplicación escalar de la forma $M \times R \rightarrow M$, y los tres axiomas antedichos se escriben con los escalares r y s a la derecha de x e y .

Si R es conmutativo, entonces los R -módulos a la izquierda son lo mismo que R -módulos a la derecha y se llaman simplemente R -módulos.

Ejemplos

- Si K es un cuerpo, entonces los conceptos " K -espacio vectorial" y K -módulo son idénticos.
- Cada grupo abeliano M es un módulo sobre el anillo de los números enteros \mathbf{Z} si definimos $nx = x + x + \dots + x$ (n sumandos) para $n > 0$, $0x = 0$, y $(-n)x = -(nx)$ para $n < 0$.
- Si R es cualquier anillo y n un número natural, entonces el producto cartesiano R^n es un módulo izquierdo y derecho sobre R si utilizamos las operaciones componente a componente. El caso $n = 0$ da el trivial R -módulo $\{0\}$ que consiste solamente en el elemento identidad (aditiva).
- Si X es una variedad diferenciable, entonces las funciones diferenciables de X a los números reales forman un anillo R . El conjunto de todos los campos vectoriales diferenciables definidos en X forman un módulo sobre R , y lo mismo con los campos tensoriales y las formas diferenciales en X .
- Las *matrices* cuadradas n -por- n con entradas reales forman un anillo R , y el espacio euclidiano \mathbf{R}^n es un módulo izquierdo sobre este anillo si definimos la operación de módulo vía la multiplicación de matrices.
- Si R es cualquier anillo e I es cualquier ideal izquierdo en R , entonces I es un módulo izquierdo sobre R . Análogamente, por supuesto, los ideales derechos son módulos derechos.

Submódulos y homomorfismos

Suponga que M es un R -módulo izquierdo y N es un subgrupo de M . Entonces N es un **submódulo** (o R -submódulo, para ser más explícito) si, para cualquier n en N y cualquier r en R , el producto rn está en N (o el nr para un módulo derecho). Si M y N son R - módulos, entonces una función $f: M \rightarrow N$ es un **homomorfismo de R - módulos** si, para cualquier m, n en M y r, s en R ,

$$f(rm + sn) = rf(m) + sf(n).$$

Esto, como cualquier homomorfismo de objetos matemáticos, es precisamente una función que preserva la estructura de los objetos. Un homomorfismo biyectivo de módulos es un isomorfismo de módulos, y los dos módulos se llaman *isomorfos*. Dos módulos isomorfos son idénticos para todos los propósitos prácticos, diferenciándose solamente en la notación para sus elementos.

El núcleo de un homomorfismo de módulos $f: M \rightarrow N$ es el submódulo de M que consiste en todos los elementos que son enviados a cero por f . Los teoremas de isomorfía familiares de grupos abelianos y de espacios vectoriales son también válidos para R -módulos.

Los R -módulos izquierdos, junto con sus homomorfismos de módulo, forman una categoría, escrita como ${}_R\mathbf{Mod}$. Esta es una categoría abeliana.

Tipos de módulos

Finitamente generado. Un módulo M es finitamente generado si existe un número finito de elementos x_1, \dots, x_n en M tales que cada elemento de M es una combinación lineal de esos elementos con coeficientes del anillo escalar R .

Libre. Un módulo libre es un módulo que tiene una base, o equivalentemente, uno que es isomorfo a una suma directa de copias del anillo escalar R . Éstos son los módulos que se comportan parecido a los espacios vectoriales.

Proyectivo. Los módulos proyectivos son sumandos directos de módulos libres y comparten muchas de sus propiedades deseables.

Inyectivo. Los módulos inyectivos se definen dualmente a los módulos proyectivos.

Simple. Un módulo simple S es un módulo que no es $\{0\}$ cuyos únicos submódulos son $\{0\}$ y S . Los módulos simples a veces se llaman *irreducibles*.

Indescomponible. Un módulo indescomponible es un módulo diferente a cero que no se puede escribir como una suma directa de dos submódulos diferentes a cero. Cada módulo simple es indescomponible.

Fiel. Un módulo fiel M es uno donde la acción de cada r en R da una función inyectiva $M \rightarrow M$. Equivalente, el aniquilador de M es el ideal cero.

Noetheriano. Un módulo noetheriano es un módulo tal que cada submódulo es finitamente generado. Equivalente, cada cadena creciente de submódulos llega a ser estacionaria en finitos pasos.

Artiniano. Un módulo artiniano es un módulo en el cual cada cadena decreciente de submódulos llega a ser estacionaria en finitos pasos.

Definición alternativa como representaciones

Si M es un R -módulo izquierdo, entonces la *acción* de un elemento r en R se define como la función $M \rightarrow M$ que envía cada x al rx (o al xr en el caso de un módulo derecho), y es necesariamente un

endomorfismo de grupo del grupo abeliano $(M, +)$. El conjunto de todos los endomorfismos de grupo de M es denotado $\text{End}_{\mathbf{Z}}(M)$ y forma un anillo bajo la adición y composición, y enviando un elemento r del anillo R a su acción define realmente un homomorfismo de anillo de R a $\text{End}_{\mathbf{Z}}(M)$.

Tal del homomorfismo $R \rightarrow \text{End}_{\mathbf{Z}}(M)$ se llama una *representación* de R en el grupo abeliano M ; una manera alternativa y equivalente de definir R -módulos izquierdos es decir que un R -módulo izquierdo es un grupo abeliano M junto con una representación de R en él.

Una representación se llama *fiel* si y solamente si la función $R \rightarrow \text{End}_{\mathbf{Z}}(M)$ es inyectiva. En términos de módulos, esto significa que si r es un elemento de R tal que $rx = 0$ para todo x en M , entonces $r = 0$. Cada grupo abeliano es un módulo fiel sobre los números enteros o sobre una cierta aritmética modular $\mathbf{Z}/n\mathbf{Z}$.

Generalizaciones

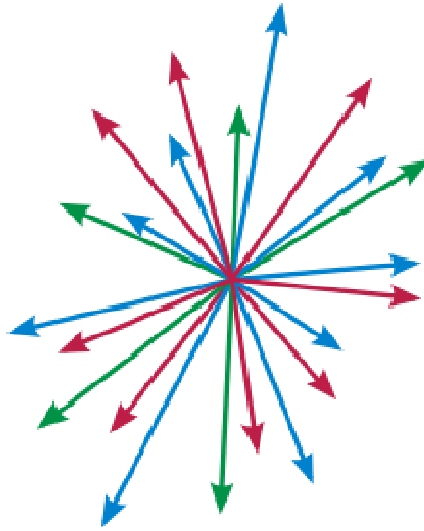
Cualquier anillo R se puede ver como categoría preaditiva con un solo objeto. Con esta comprensión, un R -módulo izquierdo es un funtor aditivo (covariante) de R a la categoría \mathbf{Ab} grupos abelianos. Los R -módulos derechos son funtores aditivos contravariantes. Esto sugiere que, si C es cualquier categoría preaditiva, un funtor aditivo covariante de C a \mathbf{Ab} sea considerado un módulo izquierdo generalizado sobre C ; estos funtores forman una categoría de funtores $C\text{-}\mathbf{Mod}$ que es la generalización natural de la categoría de módulos $R\text{-}\mathbf{Mod}$.

Los módulos sobre anillos conmutativos se pueden generalizar en una dirección distinta: tome un espacio anillado (X, \mathcal{O}_X) y considere los haces de \mathcal{O}_X -módulos. Éstos forman una categoría $\mathcal{O}_X\text{-}\mathbf{Mod}$. Si X tiene solamente un punto, entonces esto es una categoría de módulo en el viejo sentido sobre el anillo conmutativo $\mathcal{O}_X(X)$.

Referencias

- F.W. Anderson y K.R. Fuller: *Rings and Categories of Modules*, Graduate Texts in Mathematics, Vol. 13, 2da Ed., Springer-Verlag, New York, 1992

Espacio vectorial



Un **espacio vectorial** (o **espacio lineal**) es el objeto básico de estudio en la rama de la matemática llamada álgebra lineal. A los elementos de los espacios vectoriales se les llama vectores. Sobre los vectores pueden realizarse dos operaciones: la multiplicación por escalares y la adición (una asociación entre un par de objetos). Estas dos operaciones se tienen que ceñir a un conjunto de axiomas que generalizan las propiedades comunes de las tuplas de números reales así como de los vectores en el espacio euclídeo. Un concepto importante es el de *dimensión*.

Históricamente, las primeras ideas que condujeron a los espacios vectoriales modernos se remontan al siglo XVII: geometría analítica, matrices y sistemas de ecuaciones lineales. La primera formulación moderna y axiomática se debe a Giuseppe Peano, a finales del siglo XIX. Los siguientes avances en la teoría de espacios vectoriales provienen del análisis funcional, principalmente de los espacios de funciones. Los problemas de Análisis funcional requerían resolver problemas sobre la convergencia. Esto se hizo dotando a los espacios vectoriales de una adecuada topología, permitiendo tener en cuenta cuestiones de proximidad y continuidad. Estos espacios vectoriales topológicos, en particular los espacios de Banach y los espacios de Hilbert tienen una teoría más rica y elaborada.

Los espacios vectoriales tienen aplicaciones en otras ramas de la matemática, la ciencia y la ingeniería. Se utilizan en métodos como las series de Fourier, que se utiliza en las rutinas modernas de compresión de imágenes y sonido, o proporcionan el marco para resolver ecuaciones en derivadas parciales. Además, los espacios vectoriales proporcionan una forma abstracta libre de coordenadas de tratar con objetos geométricos y físicos, tales como tensores, que a su vez permiten estudiar las propiedades locales de variedades mediante técnicas de linealización.

Definición de espacio vectorial

Un espacio vectorial sobre un cuerpo \mathbf{K} (como el cuerpo de los números reales o los números complejos) es un conjunto \mathbf{V} no vacío, dotado de dos aplicaciones:

$$\begin{aligned} \text{Suma } + : V \times V &\longrightarrow V \\ (u, v) &\mapsto u + v \end{aligned}$$

operación interna tal que:

1) tenga la propiedad conmutativa, es decir

$$u + v = v + u, \forall u, v \in V$$

2) tenga la propiedad asociativa, es decir

$$u + (v + w) = (u + v) + w, \forall u, v, w \in V$$

3) tenga elemento neutro 0, es decir

$$\exists 0 \in V : u + 0 = u, \forall u \in V$$

4) tenga elemento opuesto, es decir

$$\forall u \in V, \exists -u \in V : u + (-u) = 0$$

$$\begin{aligned} \text{Producto } \cdot : K \times V &\longrightarrow V \\ (a, u) &\mapsto au \end{aligned}$$

operación externa tal que:

$$\text{a) } a(bu) = (ab)u, \forall a, b \in K, \forall u \in V$$

$$\text{b) } \exists 1 \in K, 1u = u, \forall u \in V$$

$$\text{c) } a(u + v) = au + av, \forall a \in K, \forall u, v \in V$$

$$\text{d) } (a + b)u = au + bu, \forall a, b \in K, \forall u \in V$$

Los elementos de K se llaman escalares.

Los elementos de V se llaman vectores.

Observación

Para demostrar que un conjunto V es un espacio vectorial:

- Si supiésemos que V es un grupo conmutativo o abeliano respecto la suma ya tendríamos resuelto 1,2,3 y 4.
- Si supiésemos que el producto es una acción por la izquierda de V tendríamos a y b.

Definición de subespacio vectorial

Sea V un espacio vectorial sobre K y $U \subset V$ no vacío, U es un subespacio vectorial de V si:

$$\bullet \quad \forall u, v \in U, u + v \in U$$

$$\bullet \quad \forall u \in U, \forall k \in K, ku \in U$$

Consecuencias

U hereda las operaciones de V como aplicaciones bien definidas, es decir que no escapan de U , y como consecuencia tenemos que U es un espacio vectorial sobre K .

Primer ejemplo con demostración al detalle

Queremos ver que \mathbb{R}^2 es un espacio vectorial sobre \mathbb{R}

Veamos pues que \mathbb{R}^2 juega el papel de V y \mathbb{R} el de K:

Los elementos de $V = \mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ son, de forma genérica, pares (x,y) de números reales.

defino la operación $u+v = (x_1, y_1) + (x_2, y_2) := (x_1+x_2, y_1+y_2) = (x_3, y_3)$ que pertenece a V, esto implica que la suma de vectores es interna y bien definida.

1) $u+v = (x_1, y_1) + (x_2, y_2) = (x_1+x_2, y_1+y_2) = (x_2+x_1, y_2+y_1) = (x_2, y_2) + (x_1, y_1) = v+u$, es decir $u+v=v+u$

2) $u+(v+w) = u + ((x_2, y_2) + (x_3, y_3)) = u + (x_2+x_3, y_2+y_3) = (x_1, y_1) + (x_2+x_3, y_2+y_3) = (x_1+(x_2+x_3), y_1+(y_2+y_3)) = (x_1+x_2+x_3, y_1+y_2+y_3)$, ahora véase que $(u+v)+w$ es lo mismo, es decir $u+(v+w)=(u+v)+w$.

3) $u+(0,0) = (x,y)+(0,0) = (x+0, y+0) = (x,y) = u$, es decir $(0,0)=0$ cero de V.

4) $u = (x,y)$, $u+(-x,-y) = (x,y)+(-x,-y) = (x-x, y-y) = (0,0) = 0$, es decir $-u:=(-x,-y)$ en general.

defino la operación $au = a(x,y) := (ax, ay) = (x_2, y_2)$ que pertenece a V, esto implica que la multiplicación de escalar por vector es interna y bien definida.

a) $a(bu) = a(b(x,y)) = a(bx, by) = (a(bx), a(by)) = ((ab)x, (ab)y) = (ab)(x,y) = (ab)u$, es decir: $a(bu)=(ab)u$.

b) $1u = 1(x,y) = (1x, 1y) = (x,y) = u$, es decir $1u=u$.

c) $a(u+v) = a((x_1, y_1)+(x_2, y_2)) = a(x_1+x_2, y_1+y_2) = (a(x_1+x_2), a(y_1+y_2)) = (ax_1+ax_2, ay_1+ay_2) = (ax_1, ay_1)+(ax_2, ay_2) = au+av$, es decir $a(u+v)=au+av$.

d) $(a+b)u = (a+b)(x,y) = ((a+b)x, (a+b)y) = (ax+bx, ay+by) = (ax, ay)+(bx, by) = au+bu$, es decir $(a+b)u=au+bu$.

Queda demostrado que es espacio vectorial.

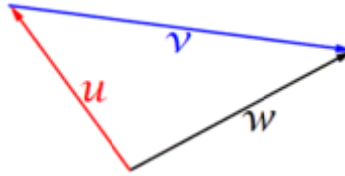
Representación de espacios vectoriales

Aunque hay quien no recomienda el uso de pinturas para evitar la confusión de conceptos y la inducción al error, sin investigación que lo corrobore, también es cierto que la memoria se estimula con mejores resultados. Para ello veamos las notas:

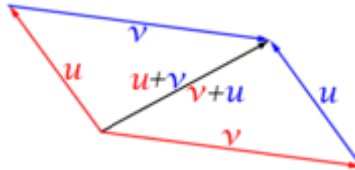
- Llamaremos vector la representación visual con el símbolo de flecha(un segmento y un triángulo en un extremo).
- La rectitud visual de una flecha o curvatura de la misma, no la hace diferente en símbolo.
- El que una flecha cierre en sí misma, indica la ausencia de efectos algebraicos.
- Encadenar vectores es unir el extremo que tiene un triángulo con el que no.

Examinemos cada uno de los casos que aparecen en la definición:

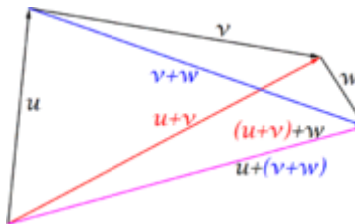
La definición suma de vectores en el orden $u+v$ produce otro vector, es como encadenar, siempre visualmente, un vector u y luego uno v. Diremos que $u+v$ se simplifica como un vector w.



1) Decir que $u+v=v+u$, es exigir que las dos sumas simplifiquen en el mismo vector, en negro. Véase que en física los vectores en rojo simulan la descomposición de fuerzas ejercidas por el vector negro en un punto, y se representa con un paralelogramo.



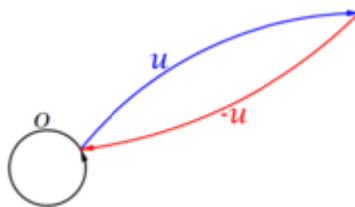
2) Decir que $u+(v+w)=(u+v)+w$, es exigir que las simplificaciones de sumas de vectores pueda ser optativa en cualquier cadena de sumas.



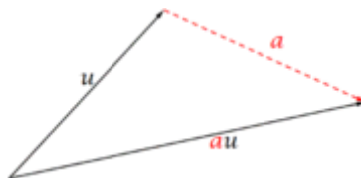
3) Decir que existe un vector 0 tal que $u+0=u$, equivale a exigir que exista un vector incapaz de efectuar, mediante la suma, modificación alguna a ninguno de los vectores.



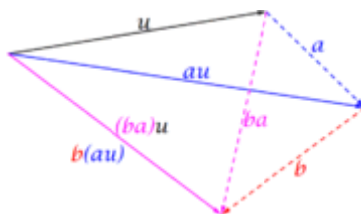
4) Decir que $u+(-u)=0$, es exigir la existencia de un elemento, $-u$, que sumado a u simplifique en el vector cero.



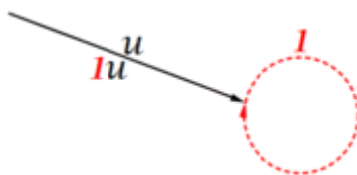
La definición producto $a \cdot u$ produce otro vector; es como modificar el extremo del vector u , siempre visualmente, donde encadenarían los siguientes vectores. Los escalares se representan con línea de trazos a modo, exclusivamente, de indicación. Por un la representación del producto en el caso $K = \mathbb{R}$ equivale a modificar, visualmente, el tamaño de la imagen del vector, y quedan siempre superpuestos, por otro lado las representaciones en el caso $K = \mathbb{C}$ equivale, además de modificar el tamaño, a rotaciones.



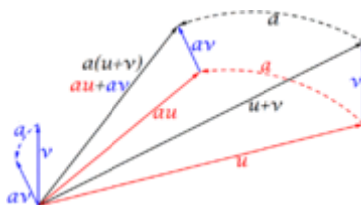
a) Decir que $a(bu)=(ab)u$, es exigir que los productos encadenados $a(b(u))$ pueden simplificarse como uno, $c=ab$, luego $(ab)u$ queda como cu .



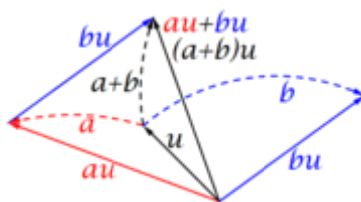
b) Decir que existe el escalar 1 tal que $1u=u$, equivale a decir exista un escalar incapaz de efectuar, mediante producto, modificación alguna a todos los vectores.



c) Decir que $a(u+v)=au+av$, es exigir la propiedad distributiva respecto la suma vectorial.



d) Decir que $(a+b)u=au+bu$, es exigir la propiedad distributiva respecto la suma escalar.



Notas

- El que h_a sea homotecia da cuenta del axioma 4 del producto por escalares ya que es lineal.
- El que f sea un morfismo de anillos significa que
 - $f(a+b)=f(a)+f(b)$, es decir que $h_{a+b}=h_a+h_b$, ó sea $(a+b)\vec{v}=a\vec{v}+b\vec{v}$ (axioma 10)

- $f(ab) = f(a) \circ f(b)$, es decir $h_{ab} = h_a \circ h_b$, ó sea $(a.b).\vec{x} = a.(b.\vec{x})$ (axioma 7)
 - $f(1) = I$, ó sea $h_1 = I$, donde 1 es el neutro de $(K,.)$ e I es la identidad, es decir la aplicación $I : \vec{x} \longrightarrow \vec{x}$ de V . La identidad es obviamente el neutro de $\text{End } V$. Esto se escribe $1.\vec{v} = \vec{v}$ para cualquier vector \vec{v} . (axioma 8)
- Se podría añadir $f(\vec{0}) = \vec{0}$, la aplicación nula de V , pero es una consecuencia de la tercera premisa.
 - El último punto ($f(1) = I$) equivale a afirmar que f no es la aplicación nula.

Propiedades del espacio vectorial.

Hay una serie de propiedades que se demuestran fácilmente a partir de los axiomas del espacio vectorial. Algunas de ellas se derivan de la teoría elemental de grupos, aplicada al grupo (aditivo) de vectores: por ejemplo, el vector nulo $\vec{0} \in V$, y el opuesto $-\mathbf{v}$ de un vector \mathbf{v} son únicos. Otras propiedades se pueden derivar de la propiedad distributiva, por ejemplo, la multiplicación por el escalar cero da el vector nulo y ningún otro escalar multiplicado por un vector da cero:

Propiedad	Significado
Unicidad del vector nulo	El vector nulo existe y es único.
Unicidad del opuesto de un vector	Cada vector (\mathbf{v}) tiene su opuesto ($-\mathbf{v}$) y éste es el único que cumple esta propiedad. Es decir: $\mathbf{v} + (-\mathbf{v}) = \vec{0}$.
Producto por el escalar cero	$0 \mathbf{v} = \vec{0}$. El 0 es el único escalar que cumple esta propiedad.
Producto de un escalar por el vector nulo	$a \vec{0} = \vec{0}$
Opuesto del producto de un vector por un escalar	$-(a \mathbf{v}) = (-a) \mathbf{v} = a (-\mathbf{v})$

Historia

Los espacios vectoriales se derivan de la geometría afín, a través de la introducción de coordenadas en el plano o el espacio tridimensional. Alrededor de 1636, los matemáticos franceses Descartes y Fermat fundaron las bases de la geometría analítica mediante la vinculación de las soluciones de una ecuación con dos variables a la determinación de una curva plana.¹ Para lograr una solución geométrica sin usar coordenadas, Bernhard Bolzano introdujo en 1804 ciertas operaciones sobre puntos, líneas y planos, que son predecesores de los vectores.² Este trabajo hizo uso del concepto de coordenadas baricéntricas de August Ferdinand Möbius de 1827.³ El origen de la definición de los vectores es la definición de Giusto Bellavitis de bipoint, que es un segmento orientado, uno de cuyos extremos es el origen y el otro un objetivo. Los vectores se reconsideraron con la presentación de los números complejos de Argand y Hamilton y la creación de los cuaterniones por este último (Hamilton fue además el que inventó el nombre de vector).⁴ Son elementos de \mathbf{R}^2 y \mathbf{R}^4 ; el tratamiento mediante combinaciones lineales se remonta a Laguerre en 1867, quien también definió los sistemas de ecuaciones lineales.

En 1857, Cayley introdujo la notación matricial, que permite una armonización y simplificación de las aplicaciones lineales. Casi al mismo tiempo, Grassmann estudió el cálculo baricéntrico iniciado por Möbius. Previó conjuntos de objetos abstractos dotados de operaciones.⁵ En su trabajo, los conceptos de independencia lineal y dimensión, así como de producto escalar están presentes. En realidad el trabajo de Grassmann de 1844 supera el marco de los espacios vectoriales, ya que teniendo en cuenta la multiplicación, también, lo llevó a lo que hoy en día se llaman álgebras. El matemático italiano Peano dio la primera definición moderna de espacios vectoriales y aplicaciones lineales en 1888.⁶

Un desarrollo importante de los espacios vectoriales se debe a la construcción de los espacios de funciones por Henri Lebesgue. Esto más tarde fue formalizado por Banach en su tesis doctoral de 1920⁷ y por Hilbert. En este momento, el álgebra y el nuevo campo del análisis funcional empezaron a interactuar, en particular con conceptos clave tales como los espacios de funciones p-integrables y los espacios de Hilbert. También en este tiempo, los primeros estudios sobre espacios vectoriales de infinitas dimensiones se realizaron.

Ejemplos

Espacios de coordenadas y de funciones

El primer ejemplo de un espacio vectorial sobre un cuerpo K es el propio cuerpo, equipado con la suma y multiplicación definida en el cuerpo. Esto se generaliza por el espacio vectorial conocido como el *espacio de coordenadas* representado generalmente como K^n , donde n es un entero. Sus elementos son n -tuplas

(a_1, a_2, \dots, a_n) , donde los a_i son elementos de K .

Las sucesiones infinitas de coordenadas, y, más generalmente, las funciones de cualquier conjunto fijo Ω en un cuerpo K también forman espacios vectoriales, mediante la suma y la multiplicación escalar puntual, es decir, la suma de dos funciones de f y g viene dada por

$$(f + g)(w) = f(w) + g(w)$$

y de igual modo para la multiplicación. Tales espacios de funciones se producen en muchas situaciones geométricas, cuando Ω es la recta real, un intervalo, o algún subconjunto de \mathbf{R}^n . Muchos conceptos en topología y análisis, tales como continuidad, integrabilidad o diferenciabilidad tienen un buen comportamiento respecto a la linealidad, es decir, sumas y múltiplos por un escalar de funciones que posean una determinada propiedad seguirán teniéndola. Por lo tanto, el conjunto de tales funciones son espacios vectoriales. Estos espacios se estudian con más detalle utilizando los métodos de análisis funcional, véase más abajo. Las desigualdades algebraicas también producen espacios vectoriales: el espacio vectorial $K[x]$ formado por funciones polinómicas, i.e.

$f(x) = r_n x^n + r_{n-1} x^{n-1} + \dots + r_1 x + r_0$, donde los coeficientes r_n, \dots, r_0 se encuentran en K . Las series de potencias son similares, salvo que se permiten infinitos términos.

Ecuaciones lineales

Los sistemas de ecuaciones lineales homogéneas están estrechamente vinculados a los espacios vectoriales. Por ejemplo, las soluciones de

$$\begin{aligned}a + 3b + c &= 0 \\ 4a + 2b + 2c &= 0\end{aligned}$$

vienen dadas por tripletas de la forma a , $b = a/2$, y $c = -5a/2$ para un a arbitrario. Forman un espacio vectorial: las sumas y múltiplos de esas tripletas sigue cumpliendo las ecuaciones, por lo que son soluciones, también. Las matrices se pueden utilizar para condensar múltiples ecuaciones lineales en una sola ecuación, con el ejemplo anterior,

$$A\mathbf{x} = \mathbf{0},$$

donde A es la matriz:

$$\begin{bmatrix} 1 & 4 \\ 3 & 2 \\ 1 & 2 \end{bmatrix},$$

, \mathbf{x} es el vector (a, b, c) , y $\mathbf{0} = (0, 0)$ es el vector nulo. De forma similar, las soluciones de *ecuaciones diferenciales lineales* homogéneas forman espacios vectoriales. Por ejemplo, las soluciones de la ecuación

$$f''(x) + 2f'(x) + f(x) = 0$$

son de la forma $f(x) = a \cdot e^{-x} + bx \cdot e^{-x}$, donde a y b son constantes arbitrarias, y $e = 2.718...$

Teoría de números algebraicos

Una situación común en la teoría de números algebraicos es un cuerpo K que contiene un subcuerpo E . Por las operaciones de multiplicación y adición de K , K se convierte en un E -espacio vectorial, es decir, una extensión de E . Por ejemplo, los números complejos son un espacio vectorial sobre \mathbf{R} . Otro ejemplo es $\mathbf{Q}(z)$, el cuerpo más pequeño que contiene los números racionales y algún número complejo z .

Bases y dimensión

Las *bases* revelan la estructura de los espacios vectoriales de una manera concisa. Una base es el menor conjunto (finito o infinito) $B = \{\mathbf{v}_i\}_{i \in I}$ de vectores que generan todo el espacio. Esto significa que cualquier vector \mathbf{v} puede ser expresado como una suma (llamada *combinación lineal*) de elementos de la base

$$a_1\mathbf{v}_{i1} + a_2\mathbf{v}_{i2} + \dots + a_n\mathbf{v}_{in},$$

donde los a_k son escalares y \mathbf{v}_{ik} ($k = 1, \dots, n$) elementos de la base B . La minimalidad, por otro lado, se hace formal por el concepto de independencia lineal. Un conjunto de vectores se dice que es linealmente independiente si ninguno de sus elementos puede ser expresado como una combinación lineal de los restantes. Equivalentemente, una ecuación

$$a_1 \mathbf{v}_{i1} + a_2 \mathbf{v}_{i2} + \dots + a_n \mathbf{v}_{in} = 0$$

sólo se consigue si todos los escalares a_1, \dots, a_n son iguales a cero. Por definición cada vector puede ser expresado como una suma finita de los elementos de la base. Debido a la independencia lineal este tipo de representación es única. Los espacios vectoriales a veces se introducen desde este punto de vista.

Todo espacio vectorial tiene una base. Este hecho se basa en el lema de Zorn, una formulación equivalente del axioma de elección. Habida cuenta de los otros axiomas de la teoría de conjuntos de Zermelo-Fraenkel, la existencia de bases es equivalente al axioma de elección. El ultrafilter lemma, que es más débil que el axioma de elección, implica que todas las bases de un espacio vectorial tienen el mismo "tamaño", es decir, cardinalidad. A ésta, se le llama la *dimensión* del espacio vectorial, representada por $\dim V$. Si el espacio es generado por un número finito de vectores, todo lo anterior puede demostrarse sin necesidad de acudir a la teoría de conjuntos.

La dimensión de un espacio de coordenadas F^n es n , pues cualquier vector (x_1, x_2, \dots, x_n) puede expresarse de forma única como combinación lineal de n vectores (llamados vectores coordenadas) $\mathbf{e}_1 = (1, 0, \dots, 0)$, $\mathbf{e}_2 = (0, 1, 0, \dots, 0)$, a $\mathbf{e}_n = (0, 0, \dots, 0, 1)$, es decir, la suma

$$x_1 \mathbf{e}_1 + x_2 \mathbf{e}_2 + \dots + x_n \mathbf{e}_n,$$

La dimensión de los espacios de funciones, como por ejemplo el espacio de funciones definidas en algún intervalo acotado o no, es infinita. Bajo unas adecuadas asunciones de regularidad de los coeficientes involucrados, la dimensión del espacio de soluciones de una ecuación diferencial ordinaria homogénea es igual al grado de la ecuación. Por ejemplo, la ecuación anterior tiene grado 2. El espacio de soluciones está generado por e^x y xe^x (que son linealmente independientes en \mathbf{R}), por lo que la dimensión de este espacio es dos. El grado de una extensión como por ejemplo $\mathbf{Q}(z)$ sobre \mathbf{Q} depende de si z es o no algebraico, i.e. satisface una cierta ecuación polinomial

$$q_n z^n + q_{n-1} z^{n-1} + \dots + q_0 = 0, \text{ con coeficientes racionales } q_n, \dots, q_0.$$

Si es algebraico, la dimensión es finita. Es más, es igual al grado del polinomio mínimo del que z es raíz. Por ejemplo, el conjunto de los números complejos es un espacio vectorial bidimensional sobre los números reales, generado por 1 y la unidad imaginaria i . Ésta última cumple $i^2 + 1 = 0$, una ecuación de grado dos. Si z no es algebraico, la dimensión es infinita. Así, para $z = \pi$ no existe dicha ecuación, pues π es trascendente.

Aplicaciones lineales y matrices

Como ocurre con muchas entidades algebraicas, la relación entre dos espacios vectoriales se expresa por las aplicaciones entre ellos. En el contexto de los espacios vectoriales, el concepto correspondiente se denomina *aplicación lineal* o *transformación lineal*. Se tratan de funciones $f: V \rightarrow W$ que son compatibles con la estructura relevante, i.e., preservan la suma de vectores y el producto por un escalar:

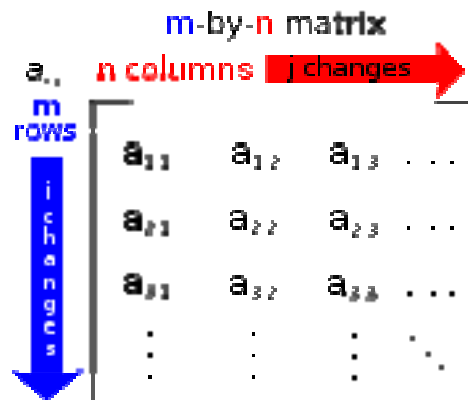
$$f(\mathbf{v} + \mathbf{w}) = f(\mathbf{v}) + f(\mathbf{w}) \text{ y } f(a \cdot \mathbf{v}) = a \cdot f(\mathbf{v}).$$

Un *isomorfismo* es aquella aplicación lineal $f: V \rightarrow W$ para la cual existe una inversa $g: W \rightarrow V$. Si existe un isomorfismo entre V y W , los dos espacios se dice que son *isomorfos*, siendo esencialmente idénticos como espacios vectoriales, ya que a cualquier identidad en V le corresponde, a través de f , otra similar en W , y viceversa a través de g .

Dados dos espacios vectoriales V y W , las aplicaciones lineales de V en W forman un espacio vectorial representado como $\text{Hom}_F(V, W)$ o como $L(V, W)$.

Una vez se elige una base de V , las aplicaciones lineales $f: V \rightarrow W$ están completamente determinadas por las imágenes de los vectores de la base, ya que cualquier elemento de V se expresa de forma única como una combinación lineal de éstos. Si los dos espacios tienen la misma dimensión se puede elegir una biyección entre dos bases fijas de V y W . La aplicación que aplica cualquier elemento de la base de V en el correspondiente elemento de la base de W , es, por su propia definición, un isomorfismo. Luego todo espacio vectorial está completamente determinado (salvo isomorfismos) por su dimensión, un simple número. En particular, cualquier espacio vectorial de dimensión n sobre F es isomorfo a F^n .

Matrices



Una matriz típica.

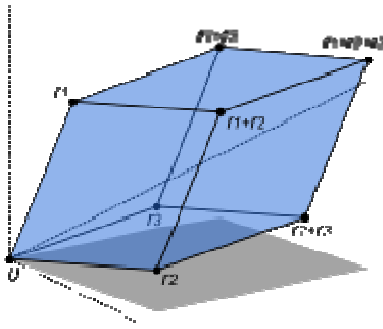
Las *matrices* son un concepto útil para representar las aplicaciones lineales. Se escriben como una tabla rectangular de escalares, es decir, elementos de algún cuerpo K . Cualquier matriz m -por- n A da lugar a una aplicación lineal de K^n a K^m , por la siguiente fórmula:

$$\mathbf{x} = (x_1, x_2, \dots, x_n) \mapsto \left(\sum_{i=1}^m x_i a_{i1}, \sum_{i=1}^m x_i a_{i2}, \dots, \sum_{i=1}^m x_i a_{in} \right),$$

o mediante el producto de la matriz A con el vector de coordenadas \mathbf{x} :

$$\mathbf{x} \mapsto A\mathbf{x}.$$

Además, después de la elección de bases de V y W , *cualquier* aplicación lineal $f: V \rightarrow W$ se representa de forma única por una matriz a través de esta fórmula.



El volumen de este paralelepípedo es el valor absoluto del determinante de la matriz 3-por-3 formada por los vectores r_1 , r_2 , y r_3 .

El determinante $\det(A)$ de una matriz cuadrada A es un escalar que nos dice si la correspondiente aplicación lineal es o no un isomorfismo: para serlo la condición necesaria y suficiente es que el determinante no sea cero.

Vectores y valores propios

Un caso especialmente importante de aplicación lineal son los endomorfismos, es decir, aplicaciones $f: V \rightarrow V$. En este caso, los vectores \mathbf{v} pueden compararse con sus imágenes por f , $f(\mathbf{v})$. Cualquier vector \mathbf{v} satisfaciendo $f(\mathbf{v}) = \lambda \cdot \mathbf{v}$, donde λ es un escalar, se dice que es un *vector propio* de f con *valor propio* λ .^{nb 1} Equivalentemente, \mathbf{v} es un elemento del núcleo de la diferencia $f - \lambda \cdot \text{Id}$ (la aplicación identidad $V \rightarrow V$). En el caso finito-dimensional, esto puede ser reformulado utilizando determinantes como: f tiene el valor propio λ sii

$$\det(f - \lambda \cdot \text{Id}) = 0.$$

Al desarrollar el determinante, la expresión del lado izquierdo resulta ser una función polinómica en λ , llamada polinomio característico de f . Si el cuerpo F es lo suficientemente grande como para contener un cero de este polinomio (que siempre ocurrirá si F es algebraicamente cerrado, por ejemplo \mathbb{C}) la aplicación lineal tendrá al menos un vector propio. El espacio vectorial V puede o no tener una base formada por vectores propios. Este fenómeno se rige por la forma canónica de Jordan del endomorfismo. El teorema espectral describe el caso infinito-dimensional; para lograr este objetivo, son necesarios los mecanismos de análisis funcional, consulte más abajo.

Construcciones básicas

Además de lo expuesto en los ejemplos anteriores, hay una serie de construcciones que nos proporcionan espacios vectoriales a partir de otros. Además de las definiciones concretas que figuran a continuación, también se caracterizan por propiedades universales, que determina un objeto X especificando las aplicaciones lineales de X a cualquier otro espacio vectorial.

Espacios vectoriales con estructura adicional

Desde el punto de vista del álgebra lineal, los espacios vectoriales se comprenden completamente en la medida en que cualquier espacio vectorial se caracteriza, salvo isomorfismos, por su dimensión. Sin embargo, los espacios vectoriales *ad hoc* no ofrecen un marco para hacer frente a la cuestión fundamental para el análisis de si una sucesión de funciones converge a otra función. Asimismo, el álgebra lineal no está adaptada *per se* para hacer frente a series infinitas, ya que la suma solo permite un número finito de términos para sumar. Las necesidades del análisis funcional requieren considerar nuevas estructuras.

Espacios vectoriales normados y espacios prehilbertianos

La "medición" de vectores es una necesidad frecuente, ya sea especificando una norma, $|| \cdot ||$, que mide las longitudes de los vectores, o por un producto escalar, $\langle \cdot, \cdot \rangle$, que permite medir además los ángulos entre los vectores. En particular se cumple la fórmula:

$$\langle \mathbf{x}, \mathbf{y} \rangle = \cos(\angle(\mathbf{x}, \mathbf{y})) \cdot \|\mathbf{x}\| \cdot \|\mathbf{y}\|$$

Esta última implica que las longitudes de los vectores se puede definir también, mediante la definición de la correspondiente norma $\|\mathbf{x}\| := \sqrt{\langle \mathbf{x}, \mathbf{x} \rangle}$.

Dos vectores \mathbf{x} e \mathbf{y} satisfaciendo que su producto escalar es cero se dice que son ortogonales.

Los espacios vectoriales dotados de estas operaciones se conocen respectivamente como *espacios vectoriales normados* y *espacios prehilbertianos*.

Ejemplos

Los espacios de coordenadas K^n pueden equiparse con el producto escalar estándar:

$$\langle (x_1, x_2, \dots, x_n), (y_1, y_2, \dots, y_n) \rangle = \mathbf{x} \cdot \mathbf{y} = x_1 y_1 + \dots + x_n y_n.$$

Una importante variante del producto escalar estándar se utiliza en el espacio-tiempo de Minkowski, es decir, \mathbf{R}^4 dotado del producto escalar

$$\langle \mathbf{x}, \mathbf{y} \rangle = x_1 y_1 + x_2 y_2 + x_3 y_3 - x_4 y_4.$$

Es crucial para el tratamiento matemático de la relatividad especial, donde la cuarta coordenada corresponde al tiempo.

Espacios vectoriales topológicos

Las cuestiones de convergencia se abordan considerando espacios vectoriales V con una topología compatible, es decir, una estructura que permite hablar de elementos que se encuentran cercanos unos a otros. Compatible quiere decir que la suma y producto por un escalar deben ser aplicaciones continuas, es decir, si \mathbf{x} e \mathbf{y} son vectores, y a es un escalar, una pequeña variación de \mathbf{x} e \mathbf{y} produce

una pequeña variación de $\mathbf{x} + \mathbf{y}$ y $a\mathbf{x}$. Si lo que varía es el escalar a , el cuerpo K debe estar dotado de una topología; una elección común son los números reales y los números complejos.

Espacio de Banach

En matemáticas, los **espacios de Banach**, llamados así en honor de Stefan Banach, son uno de los objetos de estudio más importantes en análisis funcional. Los espacios de Banach son típicamente espacios de funciones de dimensión infinita.

Definición

Un espacio de Banach es un espacio vectorial normado completo. Esto quiere decir que un espacio de Banach es un espacio vectorial V sobre el cuerpo de los números reales o el de los complejos con una norma $\|\cdot\|$ tal que toda sucesión de Cauchy (con respecto a la métrica $d(x, y) = \|x - y\|$) en V tiene un límite en V .

Ejemplos

De aquí en adelante, sea \mathbf{K} uno de los cuerpos \mathbf{R} o \mathbf{C} .

Los conocidos espacios euclidianos \mathbf{K}^n , donde la norma euclidiana de $x = (x_1, \dots, x_n)$ está dada por $\|x\| = (\sum |x_i|^2)^{1/2}$, son espacios de Banach.

El espacio de todas las funciones continuas $f: [a, b] \rightarrow \mathbf{K}$ definidas sobre un intervalo cerrado $[a, b]$ tiene la estructura de espacio de Banach si definimos la norma según $\|f\| = \sup \{ |f(x)| : x \in [a, b] \}$. Esta es, de hecho, una norma, gracias al hecho de que las funciones continuas definidas sobre un intervalo cerrado están acotadas. Este espacio es completo con esta norma, y el espacio de Banach resultante se denota por $C[a, b]$. Este ejemplo se puede generalizar al espacio $C(X)$ de todas las funciones continuas $X \rightarrow \mathbf{K}$, donde X es un espacio compacto, o al espacio de todas las funciones continuas *acotadas* $X \rightarrow \mathbf{K}$, donde X es cualquier espacio topológico, y aún al espacio $B(X)$ de todas las funciones acotadas $X \rightarrow \mathbf{K}$, donde X es cualquier conjunto. En todos estos ejemplos podemos multiplicar funciones y quedar en el mismo espacio: Todos estos espacios son, de hecho, álgebras de Banach unitarias.

Si $p \geq 1$ es un número real, podemos considerar el espacio de todas las sucesiones infinitas (x_1, x_2, x_3, \dots) de elementos en \mathbf{K} tales que la serie infinita $\sum_i |x_i|^p$ es finita. Entonces se define la norma- p de la sucesión como la raíz p -ésima del valor de la serie. Este espacio, junto a su norma, es un espacio de Banach; se denota por ℓ^p .

El espacio de Banach ℓ^∞ consiste en todas las sucesiones acotadas de elementos en \mathbf{K} ; la norma de una de estas sucesiones se define como el supremo de los valores absolutos de los miembros de la sucesión.

De nuevo, si $p \geq 1$ es un número real, podemos considerar a todas las funciones $f: [a, b] \rightarrow \mathbf{K}$ tales que $|f|^p$ es Lebesgue-integrable. Se define la norma de f como la raíz p -ésima de esta integral. Por sí mismo, este espacio no es un espacio de Banach porque existen funciones no nulas cuya norma es cero. Definimos una relación de equivalencia como sigue: f y g son equivalentes si y solo si la norma de $f - g$ es cero. El conjunto de las clases de equivalencia obtiene entonces la estructura de

espacio de Banach y es denotado por $L^p[a, b]$. Es crucial usar la integral de Lebesgue en lugar de la integral de Riemann en este caso, porque la integral de Riemann no daría un espacio completo. Estos ejemplos se pueden generalizar: ver espacios L^p para más detalles.

si X e Y son dos espacios de Banach, entonces podemos formar su suma directa $X \oplus Y$, que es un espacio de Banach también. Esta construcción se puede generalizar para la suma directa de una cantidad arbitraria de espacios de Banach.

Si M es un subespacio vectorial cerrado de un espacio de Banach X , entonces el espacio cociente X/M es un espacio de Banach también.

Finalmente, todo espacio de Hilbert es un espacio de Banach. El recíproco no es cierto.

Operadores lineales

Si V y W son espacios de Banach sobre el mismo cuerpo \mathbf{K} , el conjunto de todas las transformaciones lineales continuas $A : V \rightarrow W$ se denota por $L(V, W)$. Es de notar que en espacios de infinitas dimensiones no todas las funciones lineales son automáticamente continuas. $L(V, W)$ es un espacio vectorial, y definiendo la norma $\|A\| = \sup \{ \|Ax\| : x \text{ en } V \text{ con } \|x\| \leq 1 \}$ se transforma en un espacio de Banach.

El espacio $L(V) = L(V, V)$ forma un álgebra de Banach unitaria, donde la operación de multiplicación está dada por la composición de funciones lineales.

Espacio dual

Si V es un espacio de Banach y \mathbf{K} es el cuerpo subyacente (el de los números reales, o bien, el de los números complejos), entonces \mathbf{K} es un espacio de Banach (usando el valor absoluto como norma) y podemos definir al *espacio dual* V' por $V' = L(V, \mathbf{K})$. Este es, de nuevo, un espacio de Banach. Se puede usar para definir una nueva topología para V : la topología débil.

Existe un mapeo natural F de V a V'' definido por: $F(x)(f) = f(x)$ para todo x en V y f en V' . como consecuencia del teorema de Hahn-Banach, este mapeo es inyectivo; si llegara a ser sobreyectivo, entonces el espacio de Banach V se dice reflexivo. Los espacios reflexivos tienen muchas propiedades geométricas importantes. Un espacio es reflexivo si y solo si su espacio dual es reflexivo, lo que ocurre si y solo si su bola unitaria es compacta en la topología débil.

Por ejemplo, ℓ^p es reflexivo para $1 < p < \infty$ pero ℓ^1 y ℓ^∞ no son reflexivos. El dual de ℓ^p es ℓ^q donde p y q están relacionados por la fórmula $(1/p) + (1/q) = 1$. Ver espacios L^p para más detalles.

Relación con espacios de Hilbert

Como se menciona anteriormente, cada espacio de Hilbert es un espacio de Banach porque, por definición, un espacio de Hilbert es completo con respecto a la norma asociada a su producto interior.

No todos los espacios de Banach son espacios de Hilbert. Una condición necesaria y suficiente para que un espacio de Banach sea también un espacio de Hilbert es la **identidad del paralelogramo**:

$$\|u + v\|^2 + \|u - v\|^2 = 2(\|u\|^2 + \|v\|^2)$$

para todo u y v en nuestro espacio de Banach V , y donde $\|\cdot\|$ es la norma sobre V .

Si la norma de un espacio de Banach satisface esta identidad, entonces el espacio es un espacio de Hilbert, con el producto interior dado por la **identidad de polarización**. Si V es un espacio de Banach real entonces la identidad de polarización es

$$(u, v) = \frac{1}{4}(\|u + v\|^2 - \|u - v\|^2)$$

y en el caso que V sea un espacio de Banach complejo la identidad de polarización está dada por

$$(u, v) = \frac{1}{4}(\|u + v\|^2 - \|u - v\|^2 - i(\|u + iv\|^2 - \|u - iv\|^2))$$

Para demostrar que la identidad del paralelogramo implica que la forma definida por la identidad de polarización es verdaderamente un producto interior, uno verifica algebraicamente que esta forma es aditiva, de donde, se sigue por inducción que la forma es lineal sobre los enteros y racionales.

Entonces, como todo real es límite de alguna sucesión de Cauchy de racionales, la completitud de la norma extiende la linealidad sobre toda la recta real. En el caso complejo uno puede probar también que la forma bilineal es lineal sobre i en un argumento, y conjugada lineal en el otro.

Derivada de Fréchet

Dada una aplicación (no necesariamente lineal) $f: V \rightarrow W$ entre dos espacios de Banach es posible definir la derivada de esta función generalizando el caso de \mathbb{R}^n . Intuitivamente, si x es un elemento de V , la derivada de f en el punto x es una forma lineal continua que aproxima f cerca de x .

Formalmente, se dice que f es *diferenciable* en x si existe una forma lineal continua $A: V \rightarrow W$ tal que

$$\lim_{h \rightarrow 0} \frac{\|f(x + h) - f(x) - A(h)\|}{\|h\|} = 0.$$

El límite aquí se toma sobre todas las sucesiones de elementos no nulos de V que converjan al nulo de V . Si el límite existe, escribimos $Df(x) = A$ y le llamamos la derivada de f en x .

Esta noción de derivada es una generalización de la derivada ordinaria de funciones $\mathbf{R} \rightarrow \mathbf{R}$, pues las funciones lineales de \mathbf{R} a \mathbf{R} son las multiplicaciones por números reales.

Si f es diferenciable en *todos* los puntos x de V , entonces $Df: V \rightarrow L(V, W)$ es otra función entre espacios de Banach (que *no* es, en general, lineal), que posiblemente, se puede diferenciar de nuevo, definiendo así derivadas más altas de f . La n -ésima derivada en un punto x se puede ver como una función multilineal $V^n \rightarrow W$.

La diferenciación es una operación lineal en el siguiente sentido: si f y g son dos funciones $V \rightarrow W$ que son diferenciables en x , y r y s son escalares de \mathbf{K} , entonces $rf + sg$ es diferenciable en x con $D(rf + sg)(x) = rD(f)(x) + sD(g)(x)$.

La regla de la cadena es también válida en este contexto: si $f: V \rightarrow W$ es diferenciable en x que pertenece a V , y $g: W \rightarrow X$ es diferenciable en $f(x)$, entonces la función compuesta $g \circ f$ es diferenciable en x ya la derivada es la composición de las derivadas:

$$D(g \circ f)(x) = D(g)(f(x)) \circ D(f)(x).$$

Generalizaciones

Muchos espacios importantes en análisis funcional, por ejemplo el espacio de todas las funciones infinitamente diferenciables de \mathbf{R} en \mathbf{R} o el espacio de todas las distribuciones sobre \mathbf{R} son espacios vectoriales completos, pero no normados, no siendo espacios de Banach entonces. En los espacios de Fréchet aún se tiene una métrica completa, mientras que los espacios LF son espacios vectoriales uniformes que surgen como límites de espacios de Fréchet.

Espacio de Hilbert

En matemáticas, el concepto de **espacio de Hilbert** es una generalización del concepto de espacio euclídeo. Esta generalización permite que nociones y técnicas algebraicas y geométricas aplicables a espacios de dimensión dos y tres se extiendan a espacios de dimensión arbitraria, incluyendo a espacios de dimensión infinita. Ejemplos de tales nociones y técnicas son la de ángulo entre vectores, ortogonalidad de vectores, el teorema de Pitágoras, proyección ortogonal, distancia entre vectores y convergencia de una sucesión. El nombre dado a estos espacios es en honor al matemático David Hilbert quien los utilizó en su estudio de las ecuaciones integrales.

Más formalmente, se define como un espacio de producto interior que es completo con respecto a la norma vectorial definida por el producto interior. Los espacios de Hilbert sirven para clarificar y para generalizar el concepto de series de Fourier, ciertas transformaciones lineales tales como la transformación de Fourier, y son de importancia crucial en la formulación matemática de la mecánica cuántica.

Los espacios de Hilbert y sus propiedades se estudia dentro del análisis funcional.

Introducción

Como se explica en el artículo dedicado a los espacios de producto interior, cada producto interior $\langle \cdot, \cdot \rangle$ en un espacio vectorial H , que puede ser real o complejo, da lugar a una norma $\|\cdot\|$ que se define como sigue:

$$\|x\| = \sqrt{\langle x, x \rangle}$$

Decimos que H es un **espacio de Hilbert** si es completo con respecto a esta norma. Completo en este contexto significa que cualquier sucesión de Cauchy de elementos del espacio converge a un elemento en el espacio, en el sentido que la norma de las diferencias tiende a cero. Cada espacio de Hilbert es así también un espacio de Banach (pero no viceversa).

Todos los espacios finito-dimensionales con producto interior (tales como el espacio euclídeo con el producto escalar ordinario) son espacios de Hilbert. Esto permite que podamos extrapolar nociones desde los espacios de dimensión finita a los espacios de Hilbert de dimensión infinita (por ejemplo los espacios de funciones). Sin embargo, los ejemplos infinito-dimensionales tienen muchos más usos. Estos usos incluyen:

- La teoría de las representaciones del grupo unitarias.
- La teoría de procesos estocásticos cuadrado integrables.
- La teoría en espacios de Hilbert de ecuaciones diferenciales parciales, en particular formulaciones del problema de Dirichlet.
- Análisis espectral de funciones, incluyendo teorías de wavelets.
- Formulaciones matemáticas de la mecánica cuántica.

El producto interior permite que uno adopte una visión "geométrica" y que utilice el lenguaje geométrico familiar de los espacios de dimensión finita. De todos los espacios vectoriales topológicos infinito-dimensionales, los espacios de Hilbert son los de "mejor comportamiento" y los más cercanos a los espacios finito-dimensionales.

Los elementos de un espacio de Hilbert abstracto a veces se llaman "vectores". En las aplicaciones, son típicamente sucesiones de números complejos o de funciones. En mecánica cuántica por ejemplo, un conjunto físico es descrito por un espacio complejo de Hilbert que contenga las "funciones de ondas" para los estados posibles del conjunto. Véase formulación matemática de la mecánica cuántica.

Una de las metas del análisis de Fourier es facilitar un método para escribir una función dada como la suma (posiblemente infinita) de múltiplos de funciones bajas dadas. Este problema se puede estudiar de manera abstracta en los espacios de Hilbert: cada espacio de Hilbert tiene una base ortonormal, y cada elemento del espacio de Hilbert se puede escribir en una manera única como suma de múltiplos de estos elementos bajos.

Los espacios de Hilbert fueron nombrados así por David Hilbert, que los estudió en el contexto de las ecuaciones integrales. El origen de la designación, aunque es confuso, fue utilizado ya por Hermann Weyl en su famoso libro *la teoría de grupos y la mecánica cuántica* publicado en 1931. John von Neumann fue quizás el matemático que más claramente reconoció su importancia.

Ejemplos

En los siguientes ejemplos, asumiremos que el cuerpo subyacente de escalares es \mathbb{C} , aunque las definiciones son similares al caso de que el cuerpo subyacente de escalares sea \mathbb{R} .

Espacios euclídeos

El primer ejemplo, que ya había sido avanzado en la sección anterior, lo constituyen los espacios de dimensión finita con el producto escalar ordinario.

En otras palabras, \mathbb{C}^n con la definición de producto interior siguiente:

$$\langle x, y \rangle = \sum_{k=1}^n \overline{x_k} y_k$$

donde la barra sobre un número complejo denota su conjugación compleja.

Espacios de sucesiones

Sin embargo, mucho más típico es el espacio de Hilbert infinito dimensional.

Si B es un conjunto, definimos $\ell^2(B)$ sobre B , de la forma:

$$\ell^2(B) = \left\{ x : B \rightarrow \mathbb{C} : \sum_{b \in B} |x(b)|^2 < \infty \right\}$$

Este espacio se convierte en un espacio de Hilbert con el producto interior

$$\langle x, y \rangle = \sum_{b \in B} \overline{x(b)} y(b)$$

para todo x e y en $\ell^2(B)$.

B no tiene por que ser un conjunto contable en esta definición, aunque si B no es contable, el espacio de Hilbert que resulta no es separable.

Expresado de manera más concreta, cada espacio de Hilbert es isomorfo a uno de la forma $\ell^2(B)$ para un conjunto adecuado B . Si $B = \mathbb{N}$, se escribe simplemente ℓ^2 .

Espacios de Lebesgue

Éstos son espacios funcionales asociados a espacios de medida (X, M, μ) , donde M es una σ -álgebra de subconjuntos de X y μ es una medida contablemente aditiva en M . Sea $L^2_\mu(X)$ el espacio de funciones medibles cuadrado-integrables complejo-valoradas en X , módulo el subespacio de esas funciones cuya integral cuadrática sea cero, o equivalentemente igual a cero casi por todas partes. *cuadrado integrable* significa que la integral del cuadrado de su valor absoluto es finita. *módulo igualdad casi por todas partes* significa que las funciones son identificadas si y sólo si son iguales salvo un conjunto de medida 0.

El producto interior de las funciones f y g se da como:

$$\langle f, g \rangle = \int_X \overline{f(t)} g(t) d\mu(t)$$

Uno necesita demostrar:

- Que esta integral tiene de hecho sentido.
- Que el espacio que resulta es completo.

Éstos son hechos técnicamente fáciles. Obsérvese que al usar la integral de Lebesgue se asegura de que el espacio sea completo. Vea espacios L^p para discusión adicional de este ejemplo.

Espacios de Sobolev

Los espacios de Sobolev, denotados por $W^{m,p}(\Omega)$ son otro ejemplo de espacios de Hilbert, que se utilizan muy a menudo en el marco de las ecuaciones en derivadas parciales definidas sobre un cierto dominio Ω . Los espacios de Sobolev generalizan los espacios L^p .

Además de los espacios de Sobolev generales $W^{m,p}$ se usan ciertas notaciones particulares para cierto tipo de espacios:

- $H^m(\Omega) = W^{m,2}(\Omega)$
- $H_0^m(\Omega) = \{f \in H^m(\Omega) \mid f|_{\partial\Omega} = 0\}$

Bases ortonormales

Un concepto importante es el de una **base ortonormal** de un espacio de Hilbert H : esta es una familia $\{e_k\}_{k \in B}$ de H satisfaciendo:

- Los elementos están normalizados: Cada elemento de la familia tiene norma 1: $\|e_k\| = 1$ para todo k en B
- Los elementos son ortogonales: Dos elementos cualesquiera de B son ortogonales, esto quiere decir: $\langle e_k, e_j \rangle = 0$ para todos los k, j en B cumpliendo la condición $j \neq k$.
- Expansión densa: La expansión lineal de B es densa en H .

También utilizamos las expresiones *secuencia ortonormal* y *conjunto ortonormal*. Los ejemplos de bases ortonormales incluyen:

- El conjunto $\{(1,0,0), (0,1,0), (0,0,1)\}$ forma una base ortonormal de \mathbf{R}^3
- La secuencia $\{f_n: n \in \mathbf{Z}\}$ con $f_n(x) = \exp(2\pi i n x)$ forma una base ortonormal del espacio complejo $L^2([0, 1])$
- La familia $\{e_b: b \in B\}$ con $e_b(c) = 1$ si $b = c$ y 0 en caso contrario, forma una base ortonormal de $\ell^2(B)$.

Obsérvese que en el caso infinito-dimensional, una base ortonormal no será una base en el sentido del álgebra lineal; para distinguir los dos, la última base se llama una base de Hamel.

Usando el lema de Zorn, se puede demostrar que *cada* espacio de Hilbert admite una base ortonormal; además, cualesquiera dos bases ortonormales del mismo espacio tienen el mismo cardinal. Un espacio de Hilbert es separable si y solamente si admite una base ortonormal numerable.

Puesto que todos los espacios separables infinito-dimensionales de Hilbert son isomorfos, y puesto que casi todos los espacios de Hilbert usados en la física son separables, cuando los físicos hablan de *espacio de Hilbert* quieren significar el separable.

Si $\{e_k\}_{k \in B}$ es una base ortonormal de H , entonces cada elemento x de H se puede escribir como:

$$x = \sum_{k \in B} \langle e_k, x \rangle e_k$$

Incluso si B no es numerable, sólo contablemente muchos términos en esta suma serán diferentes a cero, y la expresión está por lo tanto bien definida. Esta suma también se llama la *expansión de Fourier* de x .

Si $\{e_k\}_{k \in B}$ es una base ortonormal de H , entonces H es *isomorfo* a $\ell^2(B)$ en el sentido siguiente: existe una función lineal biyectiva $\Phi : H \rightarrow \ell^2(B)$ tal que

$$\langle \Phi(x), \Phi(y) \rangle = \langle x, y \rangle$$

para todo x y y en H .

Operaciones en los espacios de Hilbert

Suma directa y producto tensorial

Dado dos (o más) espacios de Hilbert, podemos combinarlos en un espacio más grande de Hilbert tomando su suma directa o su producto tensorial. La primera construcción se basa en la unión de conjuntos y la segunda en el producto cartesiano.

La suma directa requiere que $H_1 \cap H_2 = \{0\}$, y es el mínimo espacio de Hilbert que "contiene" a la unión de los dos conjuntos:

$$H_1 \cup H_2 \hookrightarrow H_1 \oplus H_2, \quad \dim(H_1 \oplus H_2) = \dim(H_1) + \dim(H_2)$$

Mientras que el producto tensorial es el mínimo espacio de Hilbert que "contiene" al producto cartesiano:

$$H_1 \times H_2 \hookrightarrow H_1 \otimes H_2, \quad \dim(H_1 \otimes H_2) = \dim(H_1) \cdot \dim(H_2)$$

Complementos y proyecciones ortogonales

Si S es un subconjunto del espacio de Hilbert H , definimos el conjunto de vectores ortogonales a S

$$S^\perp = \{x \in H : \langle x, s \rangle = 0 \ \forall s \in S\}$$

S^\perp es un subespacio cerrado de H y forma, por tanto, un espacio de Hilbert. Si V es un subespacio cerrado de H , entonces el V^\perp se llama el *complemento ortogonal* de V . De hecho, cada x en H puede entonces escribirse unívocamente como $x = v + w$ con v en V y w en V^\perp . Por lo tanto, H es la suma

directa interna de Hilbert de V y V^\perp . El operador lineal $P_V: H \rightarrow H$ que mapea x a v se llama la *proyección ortogonal* sobre V .

Teorema. La proyección ortogonal P_V es un operador lineal auto-adjunto en H con norma ≤ 1 con la propiedad $P_V^2 = P_V$. Por otra parte, cualquier operador lineal E *auto-adjunto* tal que $E^2 = E$ es de la forma P_V , donde V es el rango de E . Para cada x en H , $P_V(x)$ es el elemento único v en V que minimiza la distancia $\|x - v\|$.

Esto proporciona la interpretación geométrica de $P_V(x)$: es la mejor aproximación a x por un elemento de V .

Reflexividad

Una propiedad importante de cualquier espacio de Hilbert es su reflexividad, es decir, su espacio bidual (dual del dual) es isomorfo al propio espacio. De hecho, se tiene todavía más, el propio espacio dual es isomorfo al espacio original. Se tiene una descripción completa y conveniente del espacio dual (el espacio de todas las funciones lineales continuas del espacio H en el cuerpo base), que es en sí mismo un espacio de Hilbert. De hecho, el teorema de representación de Riesz establece que para cada elemento ϕ del H' dual existe un y solamente un u en H tal que

$$\phi(x) = \langle u, x \rangle$$

para todo x en H y la asociación $\phi \leftrightarrow u$ proporciona un isomorfismo antilineal entre H y H' . Esta correspondencia es explotada por la notación bra-ket popular en la física pero que hace fruncir el ceño a los matemáticos.

Operadores en espacios de Hilbert

Operadores acotados

Para un espacio H de *Hilbert*, los operadores lineales continuos $A: H \rightarrow H$ son de interés particular. Un tal operador continuo es acotado en el sentido que mapea conjuntos acotados a conjuntos acotados. Esto permite definir su norma como

$$\|A\| = \sup \{ \|Ax\| : \|x\| \leq 1 \}.$$

La suma y la composición de dos operadores lineales continuos son a su vez continuas y lineales. Para y en H , la función que envía x a $\langle y, Ax \rangle$ es lineal y continua, y según el teorema de representación de Riesz se puede por lo tanto representar en la forma

$$\langle A^*y, x \rangle = \langle y, Ax \rangle.$$

Esto define otro operador lineal continuo $A^*: H \rightarrow H$, el *adjunto* de A .

El conjunto $L(H)$ de todos los operadores lineales continuos en H , junto con la adición y las operaciones de composición, la norma y la operación adjunto, formas una C^* -álgebra; de hecho, éste es el origen de la motivación y el más importante ejemplo de una C^* -álgebra.

Un elemento A en $L(H)$ se llama *auto-adjunto* o *hermitiano* si $A^* = A$. Estos operadores comparten muchas propiedades de los números reales y se ven a veces como generalizaciones de ellos.

Un elemento U de $L(H)$ se llama *unitario* si U es inversible y su inverso viene dado por U^* . Esto puede también ser expresado requiriendo que $\langle Ux, Uy \rangle = \langle x, y \rangle$ para todos los x, y en H . Los operadores unitarios forman un grupo bajo composición, que se puede ver como el grupo de automorfismos de H .

Operadores no acotados

En mecánica cuántica, uno también considera operadores lineales que no necesariamente son continuos y que no necesariamente están definidos en todo espacio H . Uno requiere solamente que se definan en un subespacio denso de H . Es posible definir a operadores no acotados auto-adjuntos, y éstos desempeñan el papel de los *observables* en la formulación matemática de la mecánica cuántica.

Ejemplos de operadores no acotados auto-adjuntos en el espacio de Hilbert $L^2(\mathbf{R})$ son:

- Una extensión conveniente del operador diferencial

$$[Af](x) = -i \frac{d}{dx} f(x),$$

donde i es la unidad imaginaria y f es una función diferenciable de soporte compacto.

- El operador de multiplicación por x :

$$[Bf](x) = xf(x).$$

éstos corresponden a los observables de momento y posición, respectivamente, expresados en unidades atómicas. Observe que ni A ni B se definen en todo H , puesto que en el caso de A la derivada no necesita existir, y en el caso de B la función del producto no necesita ser cuadrado-integrable. En ambos casos, el conjunto de argumentos posibles forman subespacios densos de $L^2(\mathbf{R})$.

Referencias

- Dieudonne, Jean Alexandre. Fundamentos de análisis moderno. — Barcelona. Buenos Aires : Reverté, 1966 . — 359 p.

Citas

1. ↑ La nomenclatura deriva del alemán

Referencias

Referencias históricas

- Banach, Stefan (1922) (en francés). *Sur les opérations dans les ensembles abstraits et leur application aux équations intégrales* (On operations in abstract sets and their application to integral equations). 3. Fundamenta Mathematicae. ISSN 0016-2736.
- Bolzano, Bernard (1804) (en alemán). *Betrachtungen über einige Gegenstände der Elementargeometrie* (Considerations of some aspects of elementary geometry). <http://dml.cz/handle/10338.dmlcz/400338>.
- Bourbaki, Nicolas (1969) (en francés). *Éléments d'histoire des mathématiques* (Elements of history of mathematics). Paris: Hermann.
- Grassmann, Hermann (1844) (en alemán). *Die Lineale Ausdehnungslehre - Ein neuer Zweig der Mathematik*. <http://books.google.com/books?id=bKgAAAAAMAAJ&pg=PA1&dq=Die+Lineale+Ausdehnungslehre+ein+neuer+Zweig+der+Mathematik>.
- Hamilton, William Rowan (1853) (en inglés). *Lectures on Quaternions*. Royal Irish Academy. <http://historical.library.cornell.edu/cgi-bin/cul.math/docviewer?did=05230001&seq=9>.
- Möbius, August Ferdinand (1827) (en alemán). *Der Barycentrische Calcul : ein neues Hilfsmittel zur analytischen Behandlung der Geometrie* (Barycentric calculus: a new utility for an analytic treatment of geometry). http://mathdoc.emath.fr/cgi-bin/oeitem?id=OE_MOBIUS__1_1_0.
- Moore, Gregory H. (1995), «The axiomatization of linear algebra: 1875–1940», *Historia Mathematica* **22** (3): 262–303, ISSN 0315-0860-->
- Peano, Giuseppe (1888) (en italiano). *Calcolo Geometrico secondo l'Ausdehnungslehre di H. Grassmann preceduto dalle Operazioni della Logica Deduttiva*. Turin.

Subespacio vectorial

En álgebra lineal, un **subespacio vectorial** es el subconjunto de un espacio vectorial, que debe cumplir ciertas características específicas.

Definición

Sean $(V, +, K, *)$ un espacio vectorial y S un subconjunto de V .

S es subespacio vectorial de V si $(S, +, K, *)$ es espacio vectorial en sí mismo, siendo $+$ y $*$ las mismas operaciones definidas en V . Las bases de un subespacio son el subconjunto de "alfa" y "beta" en el menor subespacio formado por la recta que pasa por dos puntos.

Condición de existencia de subespacio

El criterio para la verificación de que S sea subespacio de V , es que ambas operaciones ($+$ entre elementos del conjunto S y $*$ con escalares del cuerpo K) sean cerradas, es decir, den como resultado elementos que también pertenezcan a S . Estas antes mencionadas se dan con la suma y la multiplicación para los vectores.

Para ello se definen 4 axiomas que de cumplirse, garantizan la existencia del subespacio vectorial. Sea V un espacio vectorial, se define S como subespacio vectorial si y solo si:

1. S no es un conjunto vacío.

$$S \neq \emptyset$$

2. S es igual o está incluido en V .

$$S \subseteq V$$

3. La suma es ley de composición interna.

$$\forall \vec{x} \in S \wedge \forall \vec{y} \in S \Rightarrow \vec{x} + \vec{y} \in S$$

4. El producto es ley de composición externa.

$$\forall \vec{x} \in S \wedge \forall a \in K \Rightarrow a \cdot \vec{x} \in S$$

Si estas cuatro condiciones se cumplen entonces el conjunto es un subespacio.

Operaciones con subespacios

Sea $(V, +, K, *)$ un espacio vectorial; $(S, +, K, *)$ y $(W, +, K, *)$ subespacios de V , se definen las siguientes operaciones:

Unión

$$S \cup W = [X \in V / X \in S \vee X \in W]$$

En la gran mayoría de los casos la unión de dos subespacios no es un subespacio de V , pues no se cumple con la ley de composición interna. **Sí** pertenece de forma segura la unión a V en los casos en que S este contenido en W o viceversa.

Intersección

$$S \cap W = [X \in V / X \in S \wedge X \in W]$$

La intersección de dos subespacios es un subespacio de V .

Suma

$$S + W = [X \in V / X = (X_1 + X_2) \wedge X_1 \in S \wedge X_2 \in W]$$

La suma de dos subespacios es un subespacio de V .

Suma directa

Si la intersección entre S y W es el subespacio trivial (es decir, el vector nulo), entonces a la suma se la llama "suma directa".

Es decir que si $S \cap W = \vec{0} \Rightarrow S \oplus W$.

Dimensiones de subespacios

Esta fórmula resuelve que la dimensión de la suma de los subespacios S y W será igual a la dimensión del subespacio S más la dimensión del subespacio W menos la dimensión de la intersección de ambos.

Por ejemplo, siendo $\dim(S) = 3$ y $\dim(W) = 2$ y teniendo como intersección un subespacio de dimensión 1.

Luego, $\dim(S + W) = 4$.

En la suma directa

En el caso particular de la suma directa, como $S \cap W = \vec{0} \Rightarrow \dim(S \cap W) = 0$.

La fórmula de Grassman resulta:

$$\dim(S \oplus W) = \dim(S) + \dim(W)$$

Entonces en el ejemplo anterior, resultaría $\dim(S \oplus W) = 5$.

Referencias

1. ↑ Bourbaki, 1969, ch. "Álgebra linéaire et algèbre multilinéaire", pp. 78–91.
2. ↑ Bolzano, 1804.
3. ↑ Möbius, 1827.
4. ↑ Hamilton, 1853.
5. ↑ Grassmann, 1844.
6. ↑ Peano, 1888, ch. IX.
7. ↑ Banach, 1922.

Álgebra sobre un cuerpo

En matemáticas, un **álgebra** sobre un cuerpo K , o una **K -álgebra**, es un espacio vectorial A sobre K equipado con una noción compatible de multiplicación de elementos de A . Una generalización directa admite que K sea cualquier anillo conmutativo. Algunos autores utilizan el término "álgebra" como sinónimo de "álgebra asociativa".

Definiciones

Para ser exactos, sea $(V_{\mathbb{K}}, +)$ un espacio vectorial sobre el cuerpo \mathbb{K} , y supongamos que existe una operación binaria definida entre vectores:

$$(\cdot) : V_{\mathbb{K}} \times V_{\mathbb{K}} \rightarrow V_{\mathbb{K}}$$

Tal que es bilineal y distributiva respecto a la suma, es decir, tal que para todo $u, v, w \in V, \lambda \in \mathbb{K}$:

1. $u \cdot (v + w) = u \cdot v + u \cdot w$
2. $(v + w) \cdot u = v \cdot u + w \cdot u$
3. $u \cdot (\lambda v) = (\lambda u) \cdot v = \lambda(u \cdot v)$

Entonces con esta operación, $V_{\mathbb{K}}$ se convierte en un *álgebra* sobre \mathbb{K} y \mathbb{K} es el *cuerpo base* del álgebra $\mathcal{A} = (V_{\mathbb{K}}, +, \cdot)$. La segunda operación se llama "multiplicación". Sin embargo, la operación en varias clases especiales de álgebra toma diversos nombres:

Las álgebras también se pueden definir más generalmente sobre cualquier anillo unitario R : necesitamos un módulo \mathcal{A} sobre A y una operación bilineal de multiplicación que satisfaga las mismas identidades que arriba; entonces \mathcal{A} es una R -álgebra, y R es el *anillo* bajo \mathcal{A} . Dos álgebras \mathcal{A} y \mathcal{B} sobre \mathbb{K} son **isomorfas** si existe una K *biyección* - función lineal $f: \mathcal{A} \rightarrow \mathcal{B}$ tal que $f(\mathbf{x}\mathbf{y}) = f(\mathbf{x})f(\mathbf{y})$ para todo \mathbf{x}, \mathbf{y} en \mathcal{A} . Para todos los propósitos prácticos, las álgebras isomorfas son idénticas; solamente se diferencian en la notación de sus elementos.

Características

Para las álgebras sobre un cuerpo, la multiplicación bilineal de $\mathcal{A} \times \mathcal{A}$ a \mathcal{A} es determinada totalmente por la multiplicación de los elementos de la base de A . Inversamente, una vez que ha sido elegida una base para \mathcal{A} , los productos de los elementos de base se pueden fijar arbitrariamente, y entonces extender de una manera única a un operador bilineal en \mathcal{A} , es decir de modo que la multiplicación que resulta satisfaga las leyes del álgebra.

Así, dado el cuerpo K , cualquier álgebra se puede especificar salvo un isomorfismo dando su dimensión (digamos n), y especificar los n^3 *coeficientes de estructura* $c_{i,j,k}$, que son escalares. Estos coeficientes de estructura determinan la multiplicación en \mathcal{A} vía la regla siguiente:

$$\mathbf{e}_i \mathbf{e}_j = \sum_{k=1}^n c_{i,j,k} \mathbf{e}_k$$

Donde $\mathbf{e}_1, \dots, \mathbf{e}_n$ una base de A . El único requisito en los coeficientes de la estructura es que, si la dimensión n es un número infinito, entonces esta suma debe converger (en cualquier sentido que sea apropiado para la situación). Observe, sin embargo, que diversos conjuntos de coeficientes de estructura pueden dar lugar a álgebras isomorfas.

En física matemática, los coeficientes de estructura se escriben a menudo c_{ij}^k , y se escribe usando el convenio de sumación de Einstein como

$$\mathbf{e}_i \mathbf{e}_j = c_{ij}^k \mathbf{e}_k.$$

Si se aplica esto a vectores escritos en notación de índice, entonces se convierte en

$$(\mathbf{xy})^k = c_{ij}^k x^i y^j.$$

Si K es solamente un anillo conmutativo y no un cuerpo, entonces lo mismo funciona si A es un módulo libre sobre K . Si no es, entonces la multiplicación todavía está determinada totalmente por su acción en un conjunto generador de A ; sin embargo, las constantes de estructura no se pueden especificar arbitrariamente en este caso, y saber solamente las constantes de estructura no especifica el álgebra módulo isomorfismo.

Clases de álgebra y ejemplos

Un **álgebra conmutativa** es una en que la multiplicación es conmutativa; un álgebra asociativa es una en que la multiplicación es asociativa. Éstas incluyen las clases más familiares de álgebra.

Álgebras asociativas

Entre los ejemplos de álgebra asociativa podemos destacar:

- - el álgebra de todas las *matrices* n -por- n sobre el cuerpo (o anillo conmutativo) K . Aquí la multiplicación es multiplicación ordinaria de matrices.
 - las álgebra grupo, donde un grupo sirve de base del espacio vectorial y la multiplicación del álgebra amplía la multiplicación del grupo.
 - el álgebra conmutativa $K[x]$ de todos los polinomios sobre K , es un espacio vectorial de dimensión infinita (alef-0) sobre el cuerpo en el que se definen.
 - las álgebras de funciones, tales como el \mathbf{R} -álgebra de todas las funciones continuas real-valoradas definidas en el intervalo $[0, 1]$, o la \mathbf{C} -álgebra de todas las funciones holomórficas definidas en algún conjunto abierto en el plano complejo. Éstas son también conmutativos.
 - las álgebras de incidencia se construyen sobre ciertos conjuntos parcialmente ordenados.
 - las álgebras de operadores lineales, por ejemplo en un espacio de Hilbert. Aquí la multiplicación del álgebra viene dada por la composición de operadores. Estas

álgebras también llevan una topología; se definen muchas de ellas en un espacio subyacente de Banach que las convierte en un álgebra de Banach. Si una involución se da también, obtenemos B-estrella-álgebras y C-estrella-álgebras. Éstas se estudian en análisis funcional.

Álgebras no asociativas

Las clases más conocidas de álgebras no-asociativas son las que son casi asociativas, es decir, en que una cierta ecuación simple obliga las diferencias entre diversas maneras de asociar la multiplicación de elementos. Éstos incluyen:

- Álgebra de Lie, para las cuales requerimos la identidad de Jacobi $z(xy) + (yz)x + (zx)y = 0$ y anticonmutatividad: $xy = -yx$. Para estas álgebras el producto se llama el *corchete de Lie* y se escribe $[x, y]$ en vez de xy . Los ejemplos incluyen:
 - Espacio euclidiano \mathbf{R}^3 con la multiplicación dada por el producto vectorial (con K el cuerpo \mathbf{R} de los números reales);
 - Álgebra de los campos vectoriales en una variedad diferenciable (si K es \mathbf{R} o los números complejos \mathbf{C}) o una variedad algebraica (para el general K);
 - Cada álgebra asociativa da lugar a un álgebra de Lie usando el conmutador como corchete de Lie. De hecho cada álgebra de Lie se puede construir de esta manera, o es una subálgebra de un álgebra de Lie así construida.
- Álgebra de Jordan, para las cuales requerimos $(xy)x^2 = x(yx^2)$ y también $xy = yx$.
 - Cada álgebra asociativa sobre un cuerpo de característica distinta de 2 da lugar a un álgebra de Jordan definiendo una nueva multiplicación $x \circ y = (1/2)(xy + yx)$. En contraste con el caso del álgebra de Lie, no toda álgebra de Jordan se puede construir de esta manera. Las que sí se pueden se llaman *especiales*.
- Álgebras alternativas, para las cuales requerimos que $(xx)y = x(xy)$ y $(yx)x = y(xx)$. Los ejemplos más importantes son los octoniones (un álgebra sobre los reales), y generalizaciones de los octoniones sobre otros cuerpos. (todas las álgebras asociativas son obviamente alternativas.) Salvo isomorfismo las únicas álgebras alternativas reales finito-dimensionales son los reales, los complejos, los cuaterniones y los octoniones.
- Álgebras potencia-asociativas, para las cuales requerimos que $x^m x^n = x^{m+n}$, donde $m \geq 1$ y $n \geq 1$. (aquí definimos formalmente x^{n+1} recurrentemente como $x(x^n)$.) Los ejemplos incluyen todas las álgebras asociativas, todas las álgebras alternativas, y los sedeniones.

Más clases de álgebra

- Las álgebras de división, en las cuales el inverso multiplicativo existe o la división puede ser realizada. Las álgebras finito-dimensionales de división sobre el cuerpo de los números reales se pueden clasificar bien.
- Álgebras cuadráticas, para las cuales requerimos $xx = re + sx$, para algunos elementos r y s en el cuerpo de base, y e una unidad para el álgebra. Los ejemplos incluyen todas las álgebras alternativas finito-dimensionales, y el álgebra de las matrices reales 2-por-2. Salvo un isomorfismo las únicas álgebras reales alternativas, cuadráticas sin divisores de cero son los reales, los complejos, los cuaterniones, y los octoniones.

- Las álgebras de Cayley-Dickson (donde K es \mathbf{R} , que comienzan con:
 - \mathbf{C} (una álgebra conmutativa y asociativa);
 - los cuaterniones \mathbf{H} (una álgebra asociativa);
 - los octoniones (un álgebra alternativa);
 - los sedeniones (un álgebra potencia-asociativa, como todas las álgebras de Cayley-Dickson).
- Las álgebras de Poisson se consideran en la cuantización geométrica. Tienen **dos** multiplicaciones, haciéndolas álgebras conmutativas y álgebras de Lie de diversas maneras.

Álgebra de Clifford

Las **álgebras de Clifford** son álgebras asociativas de importancia en matemáticas, en particular en teoría de la forma cuadrática y del grupo ortogonal y en la física. Se nombran así por William Kingdon Clifford.

Definición formal

Sea V un espacio vectorial sobre un cuerpo k y $q : V \rightarrow k$ una forma cuadrática en V . El álgebra de Clifford $C(q)$ es un álgebra asociativa unital sobre k junto con la función lineal $i: V \rightarrow C(q)$ definido por la propiedad universal siguiente: para cada álgebra asociativa A sobre k con una función lineal $j: V \rightarrow A$ tal que para cada v en V se tiene $j(v)^2 = q(v)1$ (donde 1 denota la identidad multiplicativa de A), hay un homomorfismo único del álgebra $f: C(q) \rightarrow A$ tal que el diagrama siguiente conmuta

$$\begin{array}{ccc} V & \rightarrow & C(q) \\ \downarrow & \swarrow & \\ A & & \end{array}$$

es decir tal que $fi = j$.

El álgebra de Clifford existe y puede ser construida como sigue: tome el álgebra tensorial $T(V)$ concientada por el ideal generado por

$$v \otimes v - q(v)1.$$

Se sigue de esta construcción que i es inyectivo, y V se puede considerar como subespacio lineal de $C(q)$.

Sea

$$B(u, v) = q(u + v) - q(u) - q(v)$$

la forma bilineal asociada a q . Que es una consecuencia de la definición que la identidad

$$uv + vu = B(u, v)$$

vale en $C(q)$ para cada par (u, v) de vectores en V . Si el cuerpo es de característica distinta de 2 esta expresión se puede utilizar como definición alternativa.

El álgebra de Clifford $C(q)$ es filtrada por subespacios

$$k \subset k + V \subset k + V + V^2 \subset \dots$$

de los elementos que se pueden escribir como monomios de 0, 1, 2,... vectores en V . El álgebra graduada asociada es canónicamente isomorfa al álgebra exterior ΛV del espacio vectorial. Esto muestra en particular que

$$\dim C(q) = 2^{\dim V}.$$

Una manera más simple de considerar esto es eligiendo una base arbitraria e_1, e_2, \dots para V . Usando la relación de anticonmutación podemos expresar siempre un elemento del álgebra de Clifford como combinación lineal de monomios del tipo

$$e_{i_1} e_{i_2} e_{i_3} \cdots e_{i_n}, i_1 < i_2 < \cdots < i_n$$

que da un isomorfismo explícito con el álgebra exterior. Obsérvese que éste es un isomorfismo de espacios vectoriales, *no* de álgebras.

Si V tiene dimensión finita par, el cuerpo es algebraicamente cerrado y la forma cuadrática es no degenerada, el álgebra de Clifford es simple central. Así por el teorema de Artin-Wedderburn es (no canónicamente) isomorfa a un álgebra de matrices. Se sigue que en este caso $C(q)$ tiene una representación irreducible de dimensión $2^{\dim(V)/2}$ que es única salvo un isomorfismo (no único). Éste es la famosa *representación por espinor*, y sus vectores se llaman espinores.

En caso de que el cuerpo k sea el cuerpo de números reales el álgebra de Clifford de una forma cuadrática de signatura p, q es generalmente denotada $C(p, q)$. Se han clasificado estas álgebras reales de Clifford como sigue...

Las álgebras de Clifford son importantes en la física. Los físicos consideran generalmente las álgebras de Clifford expresadas por las matrices $\gamma_1, \dots, \gamma_n$ que tienen la propiedad que

$$\gamma_i \gamma_j + \gamma_j \gamma_i = 2\delta_{ij}$$

donde δ es la matriz de una forma cuadrática del tipo p, q con respecto a una base ortonormal de e_1, \dots, e_n .

Representaciones de álgebras de Clifford

En matemáticas, las **representaciones de las álgebras de Clifford** se conocen también como **módulos de Clifford**. En general un álgebra de Clifford C es un álgebra simple central sobre una cierta extensión del cuerpo L del *cuerpo* K sobre el cual se define la forma cuadrática Q que define a C .

Representaciones matriciales de las álgebras reales de Clifford

Tendremos que estudiar *matrices* anticonmutantes ($AB = -BA$) porque en las álgebras de Clifford los vectores ortogonales anticonmutan

$$A \cdot B = \frac{1}{2}(AB + BA) = 0$$

Para las álgebras de Clifford reales $R_{p,q}$ se necesitan $p + q$ matrices mutuamente anticonmutantes, de las cuales p tienen +1 como cuadrado y q tienen -1 como cuadrado.

$$\begin{aligned}\gamma_a^2 &= +1 & \text{si } 1 \leq a \leq p \\ \gamma_a^2 &= -1 & \text{si } p+1 \leq a \leq p+q \\ \gamma_a \gamma_b &= -\gamma_b \gamma_a & \text{si } a \neq b\end{aligned}$$

El sistema "K" para nombrar matrices

Primero presentamos un método cómodo para nombrar *matrices* $2^n \times 2^n$

$$K_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, K_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, K_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, K_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Note que K_0 es la matriz identidad. Los nombres fueron elegidos de tal manera que hay una regla simple para recordar los productos:

$$\begin{aligned}K_1 K_2 &= K_3 \\ K_1 K_3 &= K_2 \\ K_2 K_3 &= K_1 \\ K_2 K_1 &= -K_3 \\ K_3 K_1 &= -K_2 \\ K_3 K_2 &= -K_1.\end{aligned}$$

El incremento de índices da resultado positivo. Índices que disminuyen da resultado negativo.

¡Atención! Éstas no son las mismas relaciones que valen para la base estándar de los cuaterniones. Si se nombrara $i = i_1$, $j = i_2$ y $k = i_3$ se conseguiría

$$\begin{aligned}i_1 i_2 &= i_3 \\ i_2 i_3 &= i_1 \\ i_3 i_1 &= i_2\end{aligned}$$

la última regla es diferente. Veremos más adelante que los quaterniones puros i , j y k se pueden representar por K_{12} , K_{20} y K_{32}

Se recalca que

$$K_0^2 = K_1^2 = K_3^2 = K_0$$

$$K_2^2 = -K_0$$

K_2 es la única con el cuadrado negativo, así que puede ser vista como la representación más simple de i .

Entonces damos a todos los posibles productos de Kronecker un nombre (véase multiplicación de matrices):

$$K_{ab} = K_a \otimes K_b$$

$$K_{abc} = K_a \otimes K_{bc} = K_a \otimes K_b \otimes K_c$$

Algunos ejemplos

$$K_{30} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, K_{11} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Cada índice tiene su *nivel* (2x2, 4x4, 8x8, 16x16...)

K_{13} es una K_3 en el nivel 2x2 y una K_1 en el nivel 4x4. Con esta notación es muy fácil multiplicar matrices cuadradas grandes puesto que

$$(A \otimes B)(C \otimes D) = AB \otimes CD$$

Resolvamos un ejemplo

$$K_{123} K_{222} = K_{301}$$

nivel-8x8 1 por 2 da 3

nivel-4x4 2 por 2 da 0 pero recuerda el signo menos

nivel-2x2 3 por 2 da 1 pero con otra vez un signo menos

(hay cancelación de los dos signos menos así que el resultado es K_{301})

Podemos ahora comenzar a construir los conjuntos de matrices mutuamente anticonmutantes ortogonales, a veces llamadas las matrices de Dirac. Es obvio que dos tales matrices anticonmutan si anticonmutan en un número impar de índices (el índice 0 conmuta con el resto de índices).

K_{13} por ejemplo anticonmuta con

$$K_{01}, K_{02}, K_{11}, K_{12}, K_{20}, K_{23}, K_{30}, K_{33}$$

y conmuta con

$$K_{00}, K_{10}, K_{13}, K_{21}, K_{22}, K_{31}, K_{32}.$$

Si el *índice* 2 aparece un número par de veces en el nombre entonces el cuadrado de la matriz es más (+) la matriz identidad, vamos a llamar a esto un *Kplus*

$$\text{ejemplos son } K_1, K_{22}, K_{311}, K_{2222}$$

Si el *índice* 2 aparece un número impar de veces en el nombre entonces el cuadrado de la matriz es menos (-) la matriz identidad, vamos a llamar a esto un *Kminus*

$$\text{ejemplos son } K_2, K_{222}, K_{211}, K_{1222}$$

Ahora tenemos una manera muy simple de construir los conjuntos posibles más grandes de matrices anticonmutantes.

Comience con un conjunto existente $\{K_1, K_2, K_3\}$

Inserte un nuevo índice constante (por ejemplo un 1 en la primera posición) y se obtiene $\{K_{11}, K_{12}, K_{13}\}$

Entonces agregue dos matrices más que anticonmuten en el nuevo nivel y conmuten en el viejo nivel (por medio del índice cero 0)

Se consigue $\{K_{11}, K_{12}, K_{13}, K_{20}, K_{30}\}$

Otros ejemplos

$$\{K_{21}, K_{22}, K_{23}, K_{10}, K_{30}\}$$

$$\{K_{31}, K_{32}, K_{33}, K_{10}, K_{20}\}$$

$$\{K_{111}, K_{112}, K_{113}, K_{120}, K_{130}, K_{200}, K_{300}\}$$

$$\{K_{211}, K_{212}, K_{213}, K_{220}, K_{230}, K_{100}, K_{300}\}$$

$$\{K_{311}, K_{312}, K_{313}, K_{320}, K_{330}, K_{100}, K_{200}\}$$

Se consigue siempre un conjunto con un número impar de matrices y hay siempre un *Kplus* más que *Kminus*.

Cada uno de ellas se puede escribir como el producto de todas las demás. Ejemplo $K_{11} K_{12} K_{13} K_{20} = K_{30}$.

Álgebra de Clifford real $R_{2,0}$

$p = 2$ y $q = 0$ por tanto necesitamos 2 *Kplus* como vectores base

grado 0 (el escalar)

$$1 = K_0$$

grado 1 (los vectores)

$$\gamma_1 = K_1 \Rightarrow \gamma_1^2 = K_0 = 1$$

$$\gamma_2 = K_3 \Rightarrow \gamma_2^2 = K_0 = 1$$

grado 2 (el pseudoescalar)

$$\gamma_1 \wedge \gamma_2 = \gamma_1 \gamma_2 = K_2 \Rightarrow (\gamma_1 \wedge \gamma_2)^2 = (\gamma_1 \gamma_2)^2 = K_2^2 = -1$$

$n = p + q = 2$ y se tienen $2^2 = 4$ elementos así que es lo que I. Portious llama un *álgebra* universal de Clifford.

Álgebra de Clifford real $R_{1,1}$

$p = 1$ y $q = 1$ necesitamos un Kplus y 1 Kminus como vectores base

grado 0 (el escalar)

$$1 = K_0$$

grado 1 (los vectores)

$$\gamma_1 = K_1 \Rightarrow \gamma_1^2 = K_0 = 1$$

$$\gamma_2 = K_2 \Rightarrow \gamma_2^2 = -K_0 = -1$$

grado 2 (el pseudoescalar)

$$\gamma_1 \wedge \gamma_2 = \gamma_1 \gamma_2 = K_3 \Rightarrow (\gamma_1 \wedge \gamma_2)^2 = (\gamma_1 \gamma_2)^2 = K_3^2 = K_0 = 1$$

Aquí tenemos otra vez 2^n elementos en el álgebra con $n = p+q$ así que es otra vez un *álgebra* universal de Clifford.

Álgebra de Clifford real $R_{2,1}$

$p = 2$ y $q = 1$ necesitamos dos Kplus y 1 Kminus como vectores base

grado 0 (el escalar)

$$1 = K_0$$

grado 1 (los vectores)

$$\gamma_1 = K_1 \Rightarrow \gamma_1^2 = K_0 = 1$$

$$\gamma_2 = K_3 \Rightarrow \gamma_2^2 = K_0 = 1$$

$$\gamma_3 = K_2 \Rightarrow \gamma_3^2 = -K_0 = -1$$

La signatura es (+ + -)

grado 2 (los bivectores)

$$\gamma_1 \wedge \gamma_2 = \gamma_3 = K_2 \Rightarrow (\gamma_1 \wedge \gamma_2)^2 = -1$$

$$\gamma_1 \wedge \gamma_3 = \gamma_2 = K_3 \Rightarrow (\gamma_1 \wedge \gamma_3)^2 = +1$$

$$\gamma_2 \wedge \gamma_3 = -\gamma_1 = -K_1 \Rightarrow (\gamma_2 \wedge \gamma_3)^2 = +1$$

grado 3 (el pseudoescalar)

$$\gamma_1 \wedge \gamma_2 \wedge \gamma_3 = -1 \Rightarrow (\gamma_1 \wedge \gamma_2 \wedge \gamma_3)^2 = (-1)^2 = +1$$

Éste es el primer ejemplo de un álgebra no-universal de Clifford puesto que $p+q = 3$ y se tienen solamente 2^2 elementos y no 2^3 . La razón es muy simple, cada matriz se utiliza dos veces, una vez como vector y una vez como bivector. Y el pseudoscalar es precisamente real como el escalar.

(el dual de Hodge de cada elemento es simplemente menos el original)

$$*A = -A$$

Álgebra de Clifford real $R_{0,2}$

$p = 0$ y $q = 2$ necesitamos dos K minus como vectores base, esto no es posible con matrices reales 2×2 así que necesitamos utilizar las matrices 4×4 , tenemos muchas posibilidades. Esta álgebra es isomorfa con H (los cuaterniones)

grado 0 (el escalar)

$$1 = K_{00}$$

grado 1 (los vectores)

$$\gamma_1 = K_{12} \Rightarrow \gamma_1^2 = -K_{00} = -1$$

$$\gamma_2 = K_{20} \Rightarrow \gamma_2^2 = -K_{00} = -1$$

La signatura es (- -)

grado 2 (el pseudoescalar)

$$\gamma_1 \wedge \gamma_2 = K_{12}K_{20} = K_{32} \Rightarrow (\gamma_1 \wedge \gamma_2)^2 = K_{32}^2 = -K_{00} = -1$$

El isomorfismo con los cuaterniones es como sigue

1 es escalar, i y j son vectores y k = el ij es el pseudoescalar.

Un número de Clifford es una combinación lineal de los 4 elementos 1 i j y k.

$$1 = K_{00}, \quad i = K_{12}, \quad j = K_{20} \quad k = K_{32}$$

El uso de k como pseudoescalar (el producto de i por j) es un poco extraño pero perfectamente correcto.

Álgebra de Clifford real $R_{0,3}$

p = 0 y q = 3 necesitamos 3 Kminus como vectores base, ésta es la manera usual de trabajar con cuaterniones i, j y k pero ahora son vectores base y el ijk = -1 es el pseudoescalar. Esta álgebra es otra vez isomorfa con H (los cuaterniones)

grado 0 (el escalar)

$$1 = K_0$$

grado 1 (los vectores)

$$\begin{aligned} \gamma_1 &= K_{12} = i \Rightarrow \gamma_1^2 = -K_{00} = -1 \\ \gamma_2 &= K_{20} = j \Rightarrow \gamma_2^2 = -K_{00} = -1 \\ \gamma_3 &= K_{32} = k \Rightarrow \gamma_3^2 = -K_{00} = -1 \end{aligned}$$

La signatura es (- - -)

grado 2 (los bivectores)

$$\begin{aligned} \gamma_1 \wedge \gamma_2 &= K_{12}K_{20} = K_{32} = \gamma_3 \\ \gamma_3 \wedge \gamma_1 &= K_{32}K_{12} = K_{20} = \gamma_2 \\ \gamma_2 \wedge \gamma_3 &= K_{20}K_{32} = K_{12} = \gamma_1 \end{aligned}$$

grado 3 (el pseudoescalar)

$$\gamma_1 \wedge \gamma_2 \wedge \gamma_3 = K_{12}K_{20}K_{32} = -K_{00} = -1$$

Un número de Clifford es aquí otra vez una combinación lineal de los 4 elementos 1 i j y k. el uso de -1 como pseudoescalar (los ijk) es el usual, solamente que hace del álgebra un nuevo ejemplo de un álgebra no-universal de Clifford, puesto que p + q = 3 y se tienen solamente 2^2 elementos.

Álgebra de Clifford real $R_{3,0}$

Ésta es la famosa álgebra de Pauli, si se piensa en K_{02} como i y K_{00} como 1. Tenemos tres K plus como vectores de base.

grado 0 (el escalar)

$$1 = K_0$$

grado 1 (los vectores)

$$\gamma_1 = K_{10} = \sigma_1 \Rightarrow \gamma_1^2 = K_{00} = +1$$

$$\gamma_2 = K_{22} = \sigma_2 \Rightarrow \gamma_2^2 = K_{00} = +1$$

$$\gamma_3 = K_{30} = \sigma_3 \Rightarrow \gamma_3^2 = K_{00} = +1$$

La signatura es (+ + +)

grado 2 (los bivectores)

$$\sigma_1 \wedge \sigma_2 = K_{10}K_{22} = K_{32} = K_{02}K_{30} = i\sigma_3$$

$$\sigma_3 \wedge \sigma_1 = K_{30}K_{10} = -K_{20} = K_{02}K_{22} = i\sigma_2$$

$$\sigma_2 \wedge \sigma_3 = K_{22}K_{30} = K_{12} = K_{02}K_{10} = i\sigma_1$$

grado 3 (el pseudoescalar)

$$\sigma_1 \wedge \sigma_2 \wedge \sigma_3 = K_{10}K_{22}K_{30} = K_{02} = i$$

Luego i es el pseudoscalar y las ecuaciones para los bivectores significan de hecho que cada bivector es la estrella de Hodge de un vector no parte del bivector.

Álgebra de Clifford real $R_{3,1}$

Ésta es, tal vez, el álgebra de Clifford real más interesante porque permite la construcción de las ecuaciones tipo Dirac sin números complejos. Majorana la descubrió. Los espinores reales se llaman los espinores de Majorana. El álgebra también se conoce como el álgebra de Majorana. Hace uso de todas las 16 matrices reales 4×4 . Los cuatro vectores de base son de hecho las tres matrices de Pauli (K plus) completadas con una cuarta matriz antihermitiana (K min). La signatura es (+ + + -) Para la signatura (+ - - -) o (- - - +) comúnmente usada en física se necesita matrices complejas 4×4 o matrices reales 8×8 porque no se puede formar 3 matrices 4×4 anticonmutantes K min.

vea $R_{1,3}$ para algunas representaciones.

grado 0 (el escalar)

$$1 = K_0$$

grado 1 (los vectores)

$$\begin{aligned}\gamma_1 &= K_{10} \Rightarrow \gamma_1^2 = K_{00} = +1 \\ \gamma_2 &= K_{22} \Rightarrow \gamma_2^2 = K_{00} = +1 \\ \gamma_3 &= K_{30} \Rightarrow \gamma_3^2 = K_{00} = +1 \\ \gamma_4 &= K_{23} \Rightarrow \gamma_4^2 = -K_{00} = -1\end{aligned}$$

La signatura es (+ + + -)

grado 2 (los bivectores, las rotaciones de "árbol" y las "alzas" (boosts) de árbol)

$$\begin{aligned}\gamma_1\gamma_2 &= K_{10}K_{22} = K_{32} \Rightarrow (\gamma_1\gamma_2)^2 = -K_{00} = -1 \\ \gamma_1\gamma_3 &= K_{10}K_{30} = K_{20} \Rightarrow (\gamma_1\gamma_3)^2 = -K_{00} = -1 \\ \gamma_2\gamma_3 &= K_{22}K_{30} = K_{12} \Rightarrow (\gamma_2\gamma_3)^2 = -K_{00} = -1 \\ \gamma_1\gamma_4 &= K_{10}K_{23} = K_{33} \Rightarrow (\gamma_1\gamma_4)^2 = K_{00} = +1 \\ \gamma_2\gamma_4 &= K_{22}K_{23} = -K_{01} \Rightarrow (\gamma_1\gamma_2)^2 = K_{00} = +1 \\ \gamma_3\gamma_4 &= K_{30}K_{23} = -K_{13} \Rightarrow (\gamma_1\gamma_2)^2 = K_{00} = +1\end{aligned}$$

grado 3 (los pseudovectores, los duales de Hodge de los vectores)

$$\begin{aligned}\gamma_2\gamma_3\gamma_4 &= K_{22}K_{30}K_{23} = K_{31} \Rightarrow (\gamma_2\gamma_3\gamma_4)^2 = K_{00} = +1 \\ \gamma_1\gamma_3\gamma_4 &= K_{10}K_{30}K_{23} = -K_{03} \Rightarrow (\gamma_1\gamma_3\gamma_4)^2 = K_{00} = +1 \\ \gamma_1\gamma_2\gamma_4 &= K_{10}K_{22}K_{23} = -K_{11} \Rightarrow (\gamma_1\gamma_2\gamma_4)^2 = K_{00} = +1 \\ \gamma_1\gamma_2\gamma_3 &= K_{10}K_{22}K_{30} = K_{02} = i \Rightarrow (\gamma_1\gamma_2\gamma_3)^2 = -K_{00} = -1\end{aligned}$$

el último fue el pseudoescalar en $R_{3,0}$

grado 4 (el pseudoescalar)

$$\gamma_1\gamma_2\gamma_3\gamma_4 = K_{10}K_{22}K_{30}K_{23} = K_{21} \Rightarrow (\gamma_1\gamma_2\gamma_3\gamma_4)^2 = -K_{00} = -1$$

Álgebra geométrica

En las matemáticas, **álgebra geométrica** es un término aplicado a la teoría de las álgebras de Clifford y teorías relacionadas, siguiendo un libro del mismo título por Emil Artin. Este término también ha tenido reciente uso en los tratamientos de la misma área en la literatura física. En David Hestenes *et al.* **álgebra geométrica** es una reinterpretación de las álgebras de Clifford sobre los reales (lo que se afirma como una vuelta al nombre y a la interpretación originales previstos por William Clifford). Los números reales se utilizan como escalares en un espacio vectorial V . Desde ahora en adelante, un vector es algo en V mismo. El producto externo (producto exterior, o producto cuña) \wedge se define tal que se genere el álgebra graduada (álgebra exterior de Hermann Grassmann) de $\Lambda^n V_n$ de multivectores. El **álgebra geométrica** es el álgebra generada por el **producto geométrico** (el cual es pensado como fundamental) con (para todos los multivectores A, B, C)

1. Asociatividad
2. Distributividad sobre la adición de multivectores: $A(B + C) = AB + AC$ y $(A + B)C = AC + BC$
3. La contracción para cualquier "vector" (un elemento de grado uno) a , a^2 es un escalar (número real)

Llamamos esta álgebra un **álgebra geométrica** \mathcal{G}_n .

El punto distintivo de esta formulación es la correspondencia natural entre las entidades geométricas y los elementos del álgebra asociativa. La conexión entre las álgebra de Clifford y las formas cuadráticas vienen de la propiedad de contracción. Esta regla también da al espacio una métrica definida por el naturalmente derivado producto interno. Debe ser observado que en álgebra geométrica en toda su generalidad no hay restricción ninguna en el valor del escalar, puede suceder que sea negativa, incluso cero (en tal caso, la posibilidad de un producto interno está eliminada si se requiere $(x, x) \geq 0$).

El producto escalar usual y el producto cruzado tradicional del álgebra vectorial (en \mathbb{R}^3) hallan sus lugares en el álgebra geométrica \mathcal{G}_3 como el producto interno:

$$a \cdot b = \frac{1}{2}(ab + ba)$$

(que es simétrico) y el producto externo:

$$a \wedge b = \frac{1}{2}(ab - ba)_{\text{con:}}$$

$$a \times b = -i(a \wedge b)$$

(que es antisimétrico). Relevante es la distinción entre los vectores axiales y polares en el álgebra vectorial, que es natural en álgebra geométrica como la mera distinción entre los vectores y los bivectores (elementos de grado dos). El i aquí es la unidad pseudoscalar del 3-espacio euclidiano, lo que establece una dualidad entre los vectores y los bivectores, y se lo llama así debido a la propiedad prevista $i^2 = -1$.

Un ejemplo útil es $\mathbb{R}_{3,1}$, y generar $\mathcal{G}_{3,1}$, un caso del álgebra geométrica llamada **álgebra del espacio-tiempo** por Hestenes. El tensor del campo electromagnético, en este contexto, se convierte en simplemente un bivector $\mathbf{E} + i\mathbf{B}$ donde la unidad imaginaria es el elemento de volumen, dando un ejemplo de la reinterpretación geométrica de los "trucos tradicionales".

Boosts en esta métrica de Lorentz tienen la misma expresión e^{β} que la rotación en el espacio euclidiano, donde β es, por supuesto, el bivector generado por el tiempo y las direcciones del espacio implicadas, mientras que en el caso euclidiano es el bivector generado por las dos direcciones del espacio, consolidando la "analogía" casi hasta la identidad.

Sistema numérico

En álgebra abstracta, un **sistema numérico** es un tipo de estructura algebraica.

Definición

Un conjunto \mathbb{S} es un **sistema numérico** si en él están definidas dos operaciones matemáticas binarias asociativas y conmutativas, denominadas adición y multiplicación, y si además se cumple que la multiplicación es distributiva con respecto a la adición. Para a, b y c elementos de \mathbb{S} :

- *Propiedad asociativa de la adición:* $(a + b) + c = a + (b + c)$
- *Propiedad conmutativa de la adición:* $a + b = b + a$
- *Propiedad asociativa de la multiplicación:* $(a.b).c = a.(b.c)$
- *Propiedad conmutativa de la multiplicación:* $a.b = b.a$
- *Propiedad distributiva de la multiplicación sobre la adición:* $a.(b + c) = a.b + a.c$

La adición y la multiplicación no necesariamente deben ser las de la aritmética elemental.

Ejemplos notables

En esta sección se listan aquellos ejemplos de casos que salen de lo que indican la intuición o el sentido común. La aparición de "rarezas" hace que deba intervenir especialmente la razón además de la apariencia inmediata que dan los sentidos. Esto se conoce en filosofía como "buen sentido" y en matemáticas: "aplicar las definiciones al pie de la letra" o con rigor lógico. La visión de estos casos enseña más que los ejemplos sencillos.

Los conjuntos forman un sistema numérico

En la Teoría de conjuntos se definen la unión de conjuntos y la intersección de conjuntos. Podemos asimilar la unión a una adición y la intersección a una multiplicación y viceversa (como veremos más adelante).

Con esta convención, los conjuntos forman un sistema numérico:

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

El choque con la intuición

Es una práctica didáctica que los maestros utilicen objetos como manzanas o naranjas y la noción de conjunto para enseñar a sumar. Esta práctica podrá ser útil a la hora de enseñar, pero descansa en ideas no demasiado meditadas. Para las consideraciones que siguen utilizaremos la convención de asimilar la suma a la unión de conjuntos y el producto a la intersección, como en el título anterior.

**La unión de conjuntos es asimilable a la suma ordinaria solamente si los conjuntos son disjuntos:*

En una primera aproximación tenemos que dos conjuntos que tengan tres y cuatro elementos, respectivamente, y que no contengan elementos comunes, darán por unión un conjunto de siete elementos, conforme a la intención del docente para lo que desea lograr en el alumno. Pero si esos conjuntos tuvieran dos elementos comunes la unión daría por resultado un conjunto de cinco elementos.

Se ve afectado el papel del elemento identidad para la adición o elemento nulo de la suma.

Podríamos asimilar al conjunto vacío como el elemento identidad para la suma, ya que: $\emptyset \cup A = A \cup \emptyset = A$; pero también $A \cup A = A$ y si $B \subset A$ tenemos el mismo resultado, con lo que cada conjunto y todos los conjuntos incluidos en él lo dejan idéntico con respecto a la unión. Pero el conjunto vacío es el único que lo hace con todos los conjuntos.

- *La intersección es más chocante en cuanto a su paralelismo con el producto.*

La intersección de dos conjuntos disjuntos distintos del conjunto vacío darán por resultado el conjunto vacío. Esto equivale a decir que en el sistema numérico que forman los conjuntos hay **divisores de cero**. La intersección de conjuntos con elementos comunes dejará un conjunto con menos elementos que el menor de ellos. A lo sumo igual al menor de ellos, si está incluido dentro del conjunto mayor.

- *La unidad o elemento identidad para la multiplicación.*

Si adoptamos el uso intuitivo o hasta la formulación formal de los conjuntos, el sistema carecerá de unidad, puesto que no habrá ningún conjunto cuya intersección con otro cualquiera deje a ese idéntico. En el caso que se definiera un conjunto universal, referencial o de referencia, éste sería la unidad. Al estar cualquier conjunto definido a partir de él, la intersección de cualquier conjunto con el de referencia daría por resultado el conjunto menor. Pero esta unidad es un poco diferente de la idea intuitiva que se tiene a partir de la aritmética.

- Una segunda propiedad distributiva.

En los conjuntos la unión es distributiva con respecto a la intersección:

$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. Para los números que manejamos en la aritmética esto sería cierto solamente para: $a + (b \cdot c) = a \cdot b + a \cdot c$ si y sólo si $a = b = c = 0$

Conclusión

La segunda propiedad distributiva que cumplen los conjuntos permitiría que invirtiéramos la elección de las denominaciones para las operaciones de unión e intersección y el sistema seguiría siendo numérico. Deberíamos estudiar si las diferencias con respecto a los números familiares que fueron señaladas no cambian en este caso. Los números naturales, enteros, racionales, reales y complejos que conocemos forman sistemas numéricos. Para que los elementos de un conjunto sean considerados pertenecientes a un sistema numérico las operaciones definidas deben cumplir pocas propiedades. Esta amplitud hace que aparezcan ejemplos como éste, tan lleno de sorpresas. En álgebra se debe aplicar las definiciones al pie de la letra y si algo las cumple, es.

Los restos de módulo 2

Los restos de módulo 2, con las operaciones de suma y multiplicación de restos, forman un sistema numérico. La congruencia de Gauss es una relación de equivalencia. El cociente del conjunto \mathbb{Z} por una relación de equivalencia lo divide en clases disjuntas. En el caso de las congruencias de módulo 2 lo que se hace es dividir a los enteros en números pares e impares. Las operaciones de suma y multiplicación definidas permiten responder de qué paridad es el resultado de una suma o multiplicación de números pares o impares, en cualquier combinación que se utilice. Los símbolos "0" y "1" representan a los restos posibles de la división entera por 2: 0 para los números pares y 1 para los impares. La expresión $1 + 1 = 0$ es equivalente a: impar + impar = par.

Tabla de sumar		
+	0	1
0	0	1
1	1	0

Tabla de multiplicar		
\times	0	1
0	0	0
1	0	1

Con las tablas es fácil comprobar que las operaciones son conmutativas, asociativas y que el producto es distributivo con respecto a la suma. Tenemos, entonces, un sistema numérico de dos símbolos. Para una comprensión más profunda, ver aritmética modular.

Bibliografía

Adler, Irving (1970). *La Nueva Matemática*. Buenos Aires: Editorial Universitaria de Buenos Aires, Colección Ciencia Joven, 288 páginas, en rústica. Traducción del inglés: Jorge Jáuregui. Original: The New Mathematics, The John Day Company, New York.