LECCIONES DE MATEMATICA MODERNA

Por JOSE JAVIER ETAYO

(Catedrático de la Facultad de Ciencias Matemáticas de la Universidad de Madrid)

PRESENTACION

El C. O. D. y la Inspección de la Iglesia de Zaragoza organizaron conjuntamente en esta ciudad, durante los días 15 de julio a 3 de agosto, ambos inclusive, un Curso de Formación del Profesorado de Enseñanza Media, con lecciones de Ciencias, Letras y Formación religiosa. Entre las primeras, y con el pensamiento de que las modernas estructuras matemáticas puedan pronto encontrar acomodo en los programas del Bachillerato, o, en cualquier caso, de la conveniencia de que los profesores de matemáticas de este grado estén formados en las nuevas corrientes, incluyeron un programa de 16 conferencias de cuya confección y desarrollo hicieron al autor de estas líneas el honor de encargarse.

Este programa, seguido con alentadora dedicación por unos 200 religiosos y religiosas, es el que se ha recogido en este librito, con la pretensión de servir de guía y recordatorio a cuantos asistieron, y que repetidamente nos lo han solicitado, o de suplir, en los que no pudieron acudir y deseen iniciarse en estas materias, la enseñanza auditiva.

Dicho queda, por tanto, que lo que aquí se recoge es, casi literalmente, la exposición hecha en el curso. No debe pensarse, pues, que su redacción es la de un libro pensado y elaborado, sino la transcripción de esas lecciones que, si también hemos procurado que sean pensadas y elaboradas, lo son como tales lecciones, no como se elaboraría un libro. Por ello, puede en ciertas ocasiones resultar prolija la explicación o reiterativa en algunos puntos. Precisamente hemos huído adrede de la concisión de un texto, para quedarnos con la explanación de este texto.

Queremos, pues, que quede explícito que no se trata de un libro de algebra moderna o de unas nociones de topología, de los cuales abundan los realmente excelentes, sino de la elección de algunos temas concretos, que for-

men un conjunto coherente, y de la exposición y facilitación de esos temas a los aún no iniciados en ellos. Era nuestra ambición que, después de haber seguido el curso, pudieran los interesados estudiar por su cuenta algunos de los numerosos textos a su disposición, una vez familiarizados con ese modo de pensar y de vencer la innegable aridez que hace a veces insalvables los primeros obstáculos.

Se observará por ello que hemos huído de un desarrollo sistemático y exhaustivo de materias. Hemos preferido, ante todo, exponer conceptos, habituar a los oyentes a las nociones fundamentales, repitiéndolas en cuantas ocasiones hubiera lugar, hasta que fueran bien asimiladas. Prescindimos, pues, de demostraciones engorrosas que puedan hacer perder el hilo de la idea; las hemos dejado sin demostrar, advirtiéndolo previamente. Pero si una demostración tenía la doble virtud de ser sencilla y de servir de modelo de unas técnicas imposibles de desconocer para el iniciado, no sólo la incluíamos sino que la repetíamos en ocasiones análogas. No se trata, como se ve, de un curso orgánico con teoremas rígidamente encadenados, sino de hacer esto compatible, en lo posible, con un cursillo de dieciséis días para quienes desean conocer una primera introducción a los problemas de la matemática moderna.

No se olvide tampoco, sobre todo, que los asistentes a él eran en su casi totalidad Licenciados en alguna de las ramas de Ciencias, a los que se podía hablar, por consiguiente, como a conocedores de una amplia zona de la matemática clásica. No puede extrañar, pues, que supongamos desde un principio conocidos los números reales o los complejos, por ejemplo, en algunos ejemplos o ejercicios, aunque después construyamos esos cuerpos en otro capítulo posterior de las lecciones. Ha sido justamente preocupación a lo largo de ellas utilizar para cada concepto los ejemplos ilustrativos más sencillos y conocidos de todos para hacer más fácilmente asimilable la abstracción del mismo concepto.

Más aún: debe tenerse en cuenta que, al mismo tiempo que nuestras lecciones, se desarrollaron por los Profesores Rodríguez Vidal y Abellanas otras dedicadas a la Matemática del Preuniversitario, lo que hizo que, armonizando ambos cursos, hayamos dado por sabidas algunas cuestiones que, como las congruencias de números enteros o el concepto de vector libre y sus coordenadas respecto de un sistema de referencia, les fueron explicadas en ese otro curso.

En ocasiones hemos descendido a divagaciones, incluso de tipo histórico, al tratar de algunos problemas. Hemos pensado que siempre es ello conveniente para centrar las cuestiones y, sobre todo, para hacer ver la evolución

que a lo largo del tiempo sufren algunos conceptos matemáticos, lo cual puede situar en su verdadera perspectiva el hecho de que hoy se intente estudiar según las líneas de la matemática actual, observando cómo cada época ha tenido su matemática moderna que ha consistido siempre en sistematizar y poner de manifiesto las ideas implícitas en las épocas precedentes.

Por otra parte, esta evolución del pensamiento, aun del especificamente matemático, entra dentro de un acervo cultural útil, y a veces imprescindible, para quienes desempeñan la misión de formar a nuestros jóvenes Por ello hemos insistido también a veces en denunciar algunos errores que se deslizan frecuentemente en los textos. Singularmente, uno que queremos una vez más recalcar: la confusión entre números complejos y vectores. Los primeros forman un álgebra y los vectores un espacio vectorial; sólo lo que de espacio vectorial tiene el álgebra de los complejos es trasladable a los vectores. Resulta entonces incorrecto hablar de producto y cociente de vectores cuando se quiere referir a las mismas operaciones entre números complejos. Sólo la suma de complejos y su producto por números reales son traducibles en términos de vectores.

Nos excusamos, finalmente, de que dieciséis horas no den más de sí. Por esa causa, las lecciones de topología nos han quedado reducidas al mínimo. Ni aún hemos podido llegar a los conceptos de compacidad y continuidad uniforme incluídos en nuestro programa. Pero, por otra parte, fué muy denso el cúmulo de nociones que los oyentes hubieron de asimilar casi a presión para que lamentemos esta mutilación. Y tampoco hemos querido incluir nuevas cosas en esta exposición escrita, pues queremos que sea un fiel trasunto de lo que en el curso se trató.

Los ejercicios del final de cada capítulo recogen algunos de los que se propusieron en las clases prácticas que se celebraron durante los mismos días. Están espigados de entre libros que tratan de estos temas o sugeridos por las lecciones teóricas. No tienen más finalidad que la de servir de complemento al habituar y hacer más inteligibles las ideas expuestas en esas líneas.

Han colaborado en estas clases prácticas y, sobre todo, de un modo esencial en la toma y redacción de estas notas, hasta el punto de que sin su ayuda no habrían podido ver la luz, los Hnos. Adolfo de Perinat, F. S. C., y José Garay, H. M. Nuestra gratitud por ello.

Colmaría nuestra satisfacción saber que esta modesta aportación pudiera servir, como pretendimos con las lecciones originales, para hacer tomar gusto por esta concepción de la matemática a los no conocedores de ella, y que no desmereciera del indudable éxito global del cursillo.

Zaragoza, agosto de 1963.

J. J. ETAYO

I. NOCIONES SOBRE CONJUNTOS

1. DEFINICIONES

La idea de conjunto es primitiva. Puede ser definido como reunión de elementos. El hecho de que un elemento a pertenece a un conjunto A se expresa por $a \in A$ y se lee "a pertenece a A". Cuando a no pertenezca a A escribiremos $a \notin A$.

Un conjunto puede describirse por extensión y por comprensión.

a) *Por extensión*, enumerando cada elemento. Por ejemplo, el conjunto de alumnos de una clase mediante la relación de sus nombres. Para la definición por extensión empleamos la notación

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

encerrando entre llaves todos los elementos del conjunto C.

No sirve, entre otros casos, la definición por extensión, cuando el conjunto tiene infinitos elementos.

b) *Por comprensión*, expresando una propiedad que verifican todos los elementos del conjunto y solo ellos. Por ejemplo, si C es el conjunto de puntos de la circunferencia de centro O y radio r, lo definiremos como el conjunto de puntos que tienen la propiedad de estar a una distancia r de O, y escribiremos:

$$C = \{P \mid \text{dist. } OP = r\}.$$

Expresaremos a veces el hecho de que el conjunto C está definido por la propiedad p mediante la notación $C(p)$.

2. INCLUSION DE CONJUNTOS

Diremos que un conjunto C está contenido en otro C' cuando todo elemento de de C pertenece a C'; si $a \in C$, también $a \in C'$. Se dice de C que es un subconjunto de C'.

Es inmediato ver que la inclusión goza de las siguientes propiedades:

1.º *Reflexiva:* $C \subset C$.

2.º *Transitiva:* Si $C \subset C'$ y $C' \subset C''$, entonces $C \subset C''$.

3.º *Antisimétrica:* Si $C \subset C'$ y $C' \subset C$, todo elemento de C pertenece a C', y todo elemento de C' pertenece a C. Luego ambos conjun-

tos constan de los mismos elementos y son, por tanto, el mismo conjunto o conjuntos iguales. Escribiremos, pues:

Si $C \subset C'$ y $C' \subset C$, se verifica $C = C'$.

3. IMPLICACION

Veamos cómo la relación de inclusión entre C y C' se traduce entre las propiedades p y p', que definen a ambos.

Que $C \subset C'$ quiere decir que si $a \in C$, también $a \in C'$, esto es: si a tiene la propiedad p, tiene también la p'; o todavía, la propiedad p *implica* la propiedad p'. Lo escribiremos:

$$p \Rightarrow p'.$$

Entonces p es una *condición suficiente* para que se verifique la propiedad p' y, a su vez, p' es *condición necesaria* de p.

Ejemplo:

Sean $C = \{\text{múltiplos de 4 } (p)\}$ y $C' = \{\text{pares } (p')\}$.

Por ser $C \subset C'$ deducimos que una condición suficiente para que un número sea par es que sea múltiplo de 4. Y una condición necesaria para que un número sea múltiplo de 4 es que sea par.

$$\text{Si } C = C' \begin{cases} C \subset C' \\ C' \subset C \end{cases} \quad \text{luego} \quad \begin{cases} p \Rightarrow p' \\ p' \Rightarrow p \end{cases}$$

y lo expresaremos:

$$p \Leftrightarrow p'.$$

Es decir: se verifica p si y sólo si se verifica p'. Entonces p y p' se dicen equivalentes.

Ejemplo:

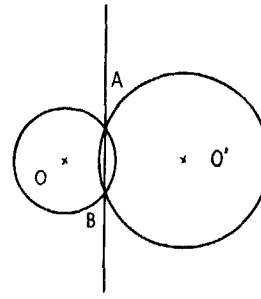
Si $C = \{\text{múltiplos de 5 } (p)\}$ y
$C' = \{\text{números terminados en 0 o en 5 } (p')\}$.

Por ser $C = C'$ deducimos que la condición necesaria y suficiente para que un número sea múltiplo de 5 es que termine en cero o 5.

4. LUGARES GEOMETRICOS

Si se trata de conjuntos de puntos de un espacio, se llama lugar geométrico al conjunto de puntos que verifican una propiedad y solamente la verifican ellos.

Ejemplo: Sea, por una parte, el conjunto de puntos de la recta AB, que une los puntos de intersección de dos circunferencias, O y O', y por otra tratamos de hallar el lugar geométrico de todos los puntos que tienen igual potencia respecto de las dos circunferencias, O y O'. Definimos así los dos conjuntos:



$$C = \{P \mid P \in AB \ (p)\}$$
$$C' = \{P' \mid \text{Pot}_{o} \ P' = \text{Pot}_{o'} \ P' \ (p')\}$$

para los que podemos demostrar geométricamente que

$$\left.\begin{array}{lll} p \Rightarrow p' & \text{ya que} & C \subset C' \\ p' \Rightarrow p & \text{"} & C' \subset C \end{array}\right\} \quad \text{luego} \quad C = C',$$

o sea, la recta AB es el lugar geométrico de los puntos de igual potencia respecto de O y de O'.

Esto nos hace ver que, en general, los problemas de lugares geométricos se reducen a problemas de inclusión de conjuntos o, lo que es equivalente, a establecer condiciones necesarias y suficientes.

5. PROPIEDADES DE LA IGUALDAD DE CONJUNTOS

Es inmediato demostrar, a partir de su definición, que la igualdad de conjuntos goza de las siguientes propiedades:

1.º *Reflexiva:* $C = C$.

2.º *Recíproca* o *simétrica:* $C = C' \Rightarrow C' = C$.

3.º *Transitiva:* $C = C'$ y $C' = C'' \Rightarrow C = C''$.

Si p, p' y p'' definen los conjuntos C, C' y C'', lo anterior se traduce en

1.º $p \Leftrightarrow p$.

2.º $p \Leftrightarrow p' \Rightarrow p' \Leftrightarrow p$.

3.º $p \Leftrightarrow p'$ y $p' \Leftrightarrow p'' \Rightarrow p \Leftrightarrow p''$.

Estas propiedades, llamadas de la igualdad lógica o de la equivalencia, son las que, como veremos, nos permitirán introducir una clasificación en un conjunto, lo que equivale a ponerlo en condiciones de ser estudiable. La ciencia opera siempre sobre clases de elementos equivalentes respecto de una cierta relación de equivalencia, nunca sobre los mismos elementos aislados.

6. PRODUCTO DE CONJUNTOS

Dados dos conjuntos, $C = \{a, b, c, \ldots\}$ y $C' = \{a', b', c', \ldots\}$, se llama *conjunto producto* de ambos y se escribe $C \times C'$ aquel cuyos elementos son todos los pares ordenados que se forman tomando como primera componente del par un elemento de C y como segunda componente uno de C'. Brevemente:

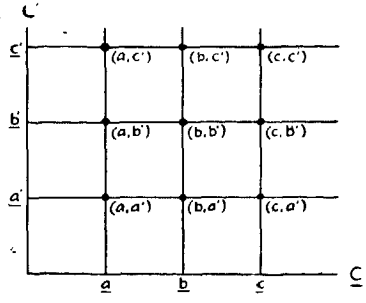
$$C \times C' = \{(a, a'), \quad (a, b'), \ldots\ldots; \quad (b, a'), \quad (b, b') \ldots\ldots\},$$

o bien

$$C \times C' = \{(x, y) \mid x \in C, \ y \in C'\}$$

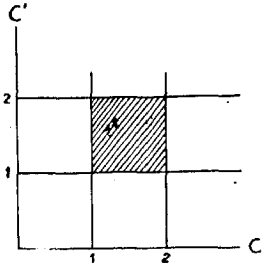
A veces el conjunto producto puede tener una representación gráfica. Veamos algunos ejemplos:

1.º Los elementos de C y de C' se pueden representar como puntos de sendas rectas. Los de $C \times C'$ son los nudos de la red de la figura.



2.° $C = \{x \in R \mid 1 \leq x \leq 2\}$
$C' = \{y \in R \mid 1 \leq y \leq 2\}$

Donde R es el conjunto de los números reales. $C \times C'$ está representado por los puntos del cuadrado rayado.



3.° Si $C = C' = R$, $C \times C'$ será el plano real.

4.° C es el conjunto de puntos de un plano:

$$C = \{(x, y) \mid x, y \in R\}.$$

C' son los puntos de una recta:

$$C' = \{z \mid z \in R\}.$$

$C \times C'$ será el espacio real de tres dimensiones:

$$\{(x, y, z) \mid x \in R,\ y \in R,\ z \in R\}.$$

Este último ejemplo nos sugiere la posibilidad de construir un conjunto producto de varios conjuntos: C, C', C'', ..., multiplicándolos sucesivamente de la siguiente forma:

$$C \times C' \times C'' \times \ldots = [(C \times C') \times C''] \times \ldots = \{(a,\ a',\ a'', \ldots) \mid a^{(i)} \in C^{(i)}\},$$

lo cual equivale a dotar a este producto de la propiedad asociativa:

$$(C \times C') \times C'' = C \times (C' \times C'').$$

7. FUNCION

El concepto de función es uno de los más sencillos y repetidos en nuestras actividades habituales. Si queremos, por poner un ejemplo sencillo, numerar los elementos de un conjunto X de objetos cualesquiera, lo que hacemos al numerar es asignar a cada objeto un nú-

mero: a uno de los objetos, el 1; a otro distinto, el 2, etc. Es decir, formar parejas objeto-número. Diremos que a cada objeto le corresponde el número que forma pareja con él. Numerar, entonces, equivale a asignar a cada objeto del conjunto X un elemento de un conjunto de números $Y = \{1, 2, 3, \ldots\}$: el número que forma pareja con él. Esa asignación de un número a cada objeto podemos considerarla como una función o correspondencia en la que a cada objeto le corresponde el número asignado a él por la operación de contar.

Tenemos, pues, en esencia, dos tipos de operaciones para establecer, en general, una correspondencia entre dos conjuntos X e Y: una es la de formación de parejas de elementos, una de cada conjunto, y otra la de elección de algunas de estas parejas que serán las que establezcan la correspondencia. La primera operación equivale a formar el conjunto producto $X \times Y$ de ambos conjuntos y la segunda será la elección de un cierto subconjunto F de este conjunto producto.

Recíprocamente, si

$$X \times Y = \{(x, y) \mid x \in X, y \in Y\} \quad \text{y} \quad F \subset X \times Y,$$

este subconjunto F nos permite dar una ley por la cual a cada $x \in X$ le hacemos corresponder los elementos $y \in Y$ tales que $(x, y) \in F$. Esta ley se llama *correspondencia* o *función* y, como vemos, viene definida por un subconjunto F del conjunto producto $X \times Y$.

Si, por ejemplo,

$$X = \{x_1, x_2, x_3, \ldots\}, \qquad Y = \{y_1, y_2, \ldots\},$$

será:

$$X \times Y = \{(x_1, y_1), (x_1, y_2), \ldots\ldots; (x_2, y_1), (x_2, y_2), \ldots\ldots; \ldots\ldots\}$$

Sea

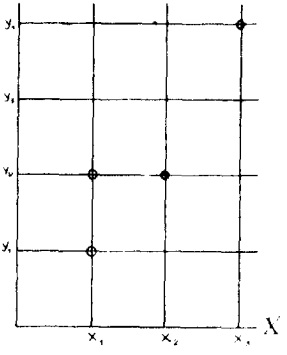
$$F = \{(x_1, y_1), (x_1, y_2), (x_2, y_2), (x_3, y_4)\}.$$

Diremos entonces que el subconjunto F establece una correspondencia entre X e Y en la cual a x_1 corresponden y_1 e y_2, a x_2 el y_2 y a x_3 el y_4, lo que podíamos expresar así:

$$\begin{aligned} x_1 &\longrightarrow y_1 \\ x_1 &\longrightarrow y_2 \\ x_2 &\longrightarrow y_2 \\ x_3 &\longrightarrow y_4 \end{aligned} \qquad [1]$$

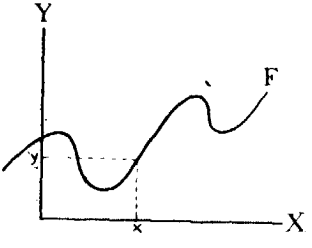
En la representación gráfica, que correspondería a la del ejem-

plo 1.º del producto de conjuntos, el subconjunto F está representado por los nudos rodeados de un círculo:



Si se trata del caso $X = Y = R$, y F fuese el subconjunto representado por la curva de la figura, a cada número real $x \in X$ le corresponderá mediante F el número o números y tales que

$$(x, y) \in F.$$



Suele utilizarse una notación mediante la que se designa a la función por una letra f, de modo que el hecho de que $y \in Y$ sea el elemento correspondiente a $x \in X$ se expresa por $y = f(x)$. Esto equivale, por tanto, a decir que $(x, y) \in F$. f es una letra genérica que puede ser sustituida en cada caso concreto por el nombre de la función, si lo tiene; por ejemplo, $y = \text{sen } x$. En el ejemplo [1], que hemos puesto antes, si f es la función definida por

$$F = \{(x_1, y_1), (x_1, y_2), (x_2, y_2), (x_3, y_4)\},$$
$$y_1 = f(x_1)$$
$$y_2 = f(x_1)$$
$$y_3 = f(x_2)$$
$$y_4 = f(x_3)$$

También se dice que y pertenece a la *imagen* de x:

$$y \in \text{im. } (x),$$

y que x es del *original* de y:

$$x \in \text{or. } (y).$$

Son, pues, equivalentes las siguientes expresiones:

$$y = f(x) \Leftrightarrow y \in \text{im. } (x) \Leftrightarrow x \in \text{or. } (y) \Leftrightarrow (x, y) \in F.$$

Al conjunto de las imágenes de todos los elementos de X, que representaremos por im. $(X) = f(X) = \text{im. } (f)$, se le llama *campo de variabilidad de la función*. Al conjunto de los originales de todos los elementos de Y:

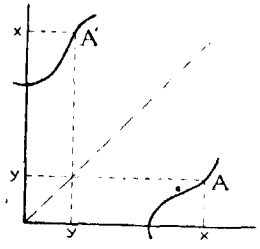
$$\text{or. } (Y) = \text{or. } (f) = f^{-1}(Y), \qquad [2]$$

le llamaremos *campo de variabilidad de la variable independiente*.

Las últimas expresiones [2] que hemos escrito equivalen a pasar de cada elemento de Y a su original en X, esto es, a una correspondencia entre Y y X. Ahora bien, como para cada y que sea imagen de x, ocurre que x es original de y, resulta que a cada correspondencia entre X e Y, dada por un conjunto F de pares (x, y), se le puede asignar otra correspondencia entre Y y X definida por el conjunto $\{(y, x)\}$ de los mismos pares de F, pero escritos en orden inverso. Esta correspondencia se obtiene, pues, de la anterior cambiando entre sí los papeles de los conjuntos X e Y y dejando invariante el subconjunto F que establece la función, bien entendido que en la segunda correspondencia los pares de F aparecen en el orden inverso que en la primera. A la segunda correspondencia entre Y y X se le llama *inversa* (o *función inversa*) de la primera, y si ésta venía representada por f, la inversa se representa por f^{-1}. Resulta, pues, la equivalencia

$$y = f(x) \Leftrightarrow x = f^{-1}(y),$$

que concuerda con [2].



En la representación gráfica, si (x, y) es un par de los que define la función f, (y, x) será uno de los de f^{-1}, lo que nos dice que si un

punto A pertenece a la gráfica de f, el punto A' simétrico de A respecto de la bisectriz de las dos rectas pertenece a la gráfica de f^{-1}. Las gráficas de dos funciones inversas son, pues, simétricas respecto de esa bisectriz.

8. APLICACIONES

Aplicación de X en Y es una función de X en Y de forma que cada original de f tiene una sola imagen en Y. También se llama *correspondencia unívoca* o *función uniforme*. La representaremos a veces así:

$$X \xrightarrow{f} Y.$$

Si una aplicación tiene además la propiedad de que cada elemento del campo de variabilidad de la función tiene un solo original en X, la correspondencia se llama *biunívoca*. Equivale a decir que tanto f como f^{-1} son aplicaciones.

Por ejemplo, la función $y = 2x$ es biunívoca. La $y = x^2$, donde $x, y \in R$ es una aplicación, pero no biunívoca. También es una aplicación no biunívoca la función que hace corresponder a cada persona su padre. La función que asigna a cada día las temperaturas medidas durante él en una ciudad no es aplicación, ni tampoco su inversa. Lo mismo ocurre a la función [1].

9. RELACIONES

Introducir una relación R entre los elementos de un conjunto C, ya sea, por ejemplo, una relación de paralelismo o de perpendicularidad entre un conjunto de rectas o de parentesco o de amistad entre un conjunto de personas, etc., no es otra cosa que señalar para cada par de elementos de C, si están o no en la relación R.

Pero tomar todos los pares de C equivale a formar el conjunto $C \times C$, y señalar cuáles de esos pares cumplen la relación R es elegir un subconjunto de $C \times C$, al cual podemos representar por la misma letra R. Entonces una relación queda, según esto, definida por el subconjunto $R \subset C \times C$. Y esto último es lo mismo que decir que *una relación es una correspondencia de C consigo mismo.*

De acuerdo, pues, con lo dicho para las funciones, si dos elementos de C están en la relación R es que verifican $(a, b) \in R$, o bien que en la correspondencia que establecen entre C y C es $b \in$ im. (a). Para

el caso de estas funciones particulares que son las relaciones se acostumbra a utilizar la notación aRb. O sea:

$$aRb \Leftrightarrow (a,\ b) \in R \Leftrightarrow b \in \text{im. } (a).$$

R es aquí un símbolo genérico, análogo al f de las funciones, que se puede sustituir en cada relación particular por el símbolo que la indique. Así, si la relación R es la de paralelismo y a y b están en esa relación de paralelismo, es decir, son paralelas, se escribirá: $a \parallel b$. Si la relación entre rectas fuese la de perpendicularidad, pondríamos $a \perp b$, etc.

Las principales propiedades que pueden tener las relaciones son:

1.° *Reflexiva* o *idéntica:* Cuando para todo $a \in C$ se verifica aRa, es decir, que todo elemento de C está en la relación dada consigo mismo. Por ejemplo, la relación de igualdad, la de paralelismo, la de paisanaje cumplen la propiedad idéntica. No la tienen la relación de perpendicularidad ni la de paternidad.

2.° *Simétrica* o *recíproca:* $aRb \Rightarrow bRa$.

El paralelismo y la perpendicularidad son relaciones que gozan de la propiedad simétrica. La paternidad, no: si a es padre de b, b no es padre de a.

3.° *Transitiva:* $aRb,\ bRc \Rightarrow aRc$.

El paralelismo es una relación transitiva y no lo es la perpendicularidad: si a es perpendicular a b y b lo es a c, a no es perpendicular a c.

4.° *Antisimétrica:* $aRb,\ bRa \Rightarrow a = b$.

La relación de "inclusión" entre conjuntos veíamos que cumplía esta propiedad; también la relación "menor o igual" entre números.

Las relaciones que cumplen las propiedades 1, 2, 3 se llaman de *equivalencia* y suele reemplazarse la R por el signo $\backsim$. Asimismo, las que cumplen las propiedades 1, 3, 4 se llaman relaciones *de orden* y su signo específico es $\preceq$.

10. RELACIONES DE EQUIVALENCIA

Dada una relación $\backsim$ en un conjunto C definamos en C subconjuntos o clases $\{a\}$, $\{b\}$, ..., de manera que cada clase esté formada por todos los elementos de C equivalentes entre sí respecto de la relación definida. La clase $\{a\}$ representa la de todos los elementos equivalentes a a, es decir,

$$x \in \{a\} \Leftrightarrow a \backsim x,$$

o sea,

$$\{a\} = \{x \mid x \backsim a\}.$$

Vamos a demostrar que estas clases son disjuntas, o sea, que no tienen elementos comunes y que todo elemento de C pertenece a alguna clase.

La última afirmación es inmediata, pues $a \in \{a\}$ para todo $a \in C$, ya que $a \backsim a$.

Si $\{a\} \neq \{b\}$ no puede existir ningún elemento que pertenezca a las dos clases, ya que, en efecto, si $c \in \{a\}$ y $c \in \{b\}$ será, respectivamente, $c \backsim a$ y $c \backsim b$, o bien aplicando la propiedad recíproca a la primera de las dos anteriores relaciones. $a \backsim c$, $c \backsim b$, y de aquí por la transitiva, $a \backsim b$. Luego todo elemento de $\{a\}$, por ser equivalente a a, será equivalente a b y pertenecerá, por tanto, a $\{b\}$, y recíprocamente. De donde $\{a\} \subset \{b\}$ y $\{b\} \subset \{a\}$, o sea, $\{a\} = \{a\}$, contra la hipótesis.

Nos hemos apoyado para esta demostración en las tres propiedades que caracterizan una relación de equivalencia.

Cuando los elementos de un conjunto C se han distribuido en clases de modo que cada elemento pertenezca a una y solo una de las clases se dice que se ha establecido una *clasificación* en C. Resulta entonces que toda relación de equivalencia establece una clasificación en un conjunto. Recíprocamente, si en un conjunto existe una clasificación, se puede introducir una relación de equivalencia en el conjunto, diciendo que dos elementos son equivalentes cuando pertenecen a la misma clase. Es inmediato comprobar que esta es, en efecto, una relación de equivalencia. A las clases así definidas por una relación de equivalencia se las llama *clases de equivalencia*.

Estas consideraciones explican que podamos clasificar un conjunto de personas por su lugar de nacimiento o por edades, etc., pues esas relaciones, paisanaje, etc., son relaciones de equivalencia. No podemos, en cambio, clasificarlas atendiendo a la amistad entre ellas, ya que la amistad, por no cumplir en general la propiedad transitiva, no es una relación de equivalencia.

Dado, pues, un conjunto C y una clasificación en él definida por una relación de equivalencia R o $\backsim$ podemos formar un nuevo conjunto cuyos elementos sean cada una de estas clases. A este conjunto se le llama *conjunto de clases de equivalencia* de C respecto de la relación de equivalencia R y se representa por C/R.

Si C es el conjunto de todas las rectas del plano y R la relación de paralelismo entre ellas C/R es el conjunto en que cada elemento consta de todas las rectas paralelas a una dada, o sea, de todas las rectas que tienen la misma dirección. C/R se puede considerar, pues, como el conjunto de todas las *direcciones* del plano.

Si C es el conjunto de todos los vectores del plano y R la relación de equipolencia de vectores, C/R tiene por elementos cada una de las clases de vectores equipolentes entre sí, que es lo que se llama un vector libre; luego C/R es el conjunto de todos los *vectores libres* del plano. Y así para cualquier otro ejemplo.

Dados dos conjuntos, A y B, es fácil ver también que una aplicación $A \xrightarrow{f} B$ establece una relación de equivalencia en A: la definida por la expresión:

$$a \backsim b \ (a, b \in A) \Leftrightarrow f(a) = f(b).$$

Ejemplos: 1.º $A = \{$polígonos del plano$\}$, $B = \{$números reales positivos$\}$; $A \xrightarrow{f} B$ es la aplicación que hace corresponder a cada polígono su área, que es un número de B. Cada clase en A está formada por todos los polígonos que tienen igual área.

2.º $A = Z = \{$conjunto de los números enteros$\}$, $B = \{0, 1, 2, 3, 4\}$; $Z \xrightarrow{f} B$ aplica a cada $a \in Z$ su resto de la división por 5. Cada clase en Z está formada por todos los enteros que dan igual resto al dividirlos por 5, es decir, es una clase de números congruentes módulo 5.

3.º $A = \{$funciones en $[a, b]$ con derivada continua en $[a, b]\}$.

$B = \{$funciones continuas en $[a, b]\}$.

$A \xrightarrow{D} B$ es tal que $D(f) = f'$, o sea, D es la aplicación derivada. Cada clase en A consta de todas las funciones de A que se diferencian en una constante, o sea, es la integral indefinida de una función de B.

4.º $A = \{$puntos del plano$\}$, $B = \{$números reales positivos$\}$.

$A \xrightarrow{f} B$ se define por $f(P) = \text{dist. } OP$, siendo O un punto fijo del plano. Las clases en A son circunferencias de centro O. Dos puntos del plano son equivalentes respecto de dicha relación de equivalencia si pertenecen a la misma circunferencia.

11. RELACIONES DE ORDEN

Un conjunto C, en el que existe una relación $\leq$ de orden, se dice que está *ordenado* con respecto a dicha relación.

C se dice además que está totalmente ordenado respecto de $\leq$ cuando para cualesquiera $a, b \in C$ se verifica $a \leq b$ o $b \leq a$.

Por ejemplo, el conjunto de partes de un conjunto con la relación de inclusión no es totalmente ordenado, pues dados los subconjuntos o partes A y B puede ocurrir que ni A esté contenido en B ni B en A.

Si en el conjunto de los números enteros establecemos la relación "a divide a b" que se denota por $a \mid b$, que es lo mismo que decir que b es múltiplo de a, ésta es una relación de orden. En efecto:

$$a \mid a$$

$$a \mid b, \quad b \mid a \Rightarrow a = b$$

$$a \mid b, \quad b \mid c \Rightarrow a \mid c.$$

Z queda, pues, ordenado respecto de esta relación, pero no totalmente ordenado, puesto que se pueden elegir dos enteros, a y b, tales que ni a divida a b ni b divida a a.

En cambio, si ordenamos Z por la relación "menor o igual", el conjunto queda totalmente ordenado, ya que dados cualesquiera $a, b \in Z$, o bien a es menor o igual que b o bien b es menor o igual que a.

12. OPERACIONES

Cuando pensamos en una operación cualquiera, por ejemplo, en la suma de dos enteros, podemos observar que equivale a asignar a cada par de enteros otro número entero, que es su suma; pero definirla para cada par de números enteros es lo mismo que definirla para cada elemento de $Z \times Z$, luego en definitiva una tal operación no es otra cosa que una aplicación de $Z \times Z$ en Z.

No siempre es así de sencillo. En el caso de producto escalar de vectores del plano, por ejemplo, a cada par de vectores, es decir, a cada elemento de $V \times V$ (siendo V el conjunto de vectores libres del plano) le corresponde un número real, luego el producto escalar es una aplicación $V \times V \longrightarrow R$.

También pueden ser distintos los conjuntos factores. Así, en el caso de multiplicación de un vector libre por un número real, para obtener otro vector, la aplicación que nos define esta operación es entonces:

$$V \times R \longrightarrow V.$$

Con toda generalidad podemos, pues, dar como definición de operación la siguiente: Se llama *operación* entre dos conjuntos A y B a una aplicación de $A \times B$ en un tercer conjunto C.

Los dos casos particulares más importantes de operaciones son los siguientes:

a) Cuando está definida por $A \times A \longrightarrow A$ la operación se llama *interna* o *ley de composición interna* (ejemplo 1.º).

b) Cuando es $A \times B \longrightarrow B$ se llama *ley de composición externa* en B (ejemplo 3.º).

En este caso el conjunto A se llama *dominio de operadores*. En nuestro ejemplo, los operadores son los números reales que operan sobre cada vector, multiplicándolo, para transformarlo en otro vector.

Otro ejemplo puede ser el siguiente: sea R el conjunto de todos los números reales y A el conjunto de todos los puntos del plano y fijamos en el plano un punto O. Establecemos entonces una aplicación:

$$A \times R \xrightarrow{f} A,$$

que haga corresponder a cada punto $p \in A$ y a cada número real $r \in R$ el punto $p' \in A$, que sea el transformado de p en la homotecia de centro O y razón r:

$$(p, r) \xrightarrow{f} p'.$$

Esta operación es una ley de composición externa en que la R es el dominio de operadores que operan sobre los puntos del plano transformándolos entre sí.

Cuando en un conjunto se ha definido una o más operaciones se dice que se ha dotado al conjunto de una *estructura*, la cual dependerá de las propiedades que tengan dichas operaciones. De un modo un poco vago podríamos decir que al introducir las operaciones pasamos de un conjunto "amorfo" en el que los elementos están simplemente agrupados o amontonados, a un conjunto ya "organizado", según una estructura determinada. Un mismo conjunto podrá ser estructurado de distintos modos, según el tipo de operaciones que en él definamos.

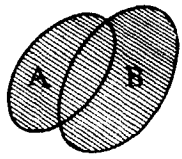
El estudio de las estructuras es precisamente el objeto primordial de la llamada Matemática moderna.

13. RETICULOS

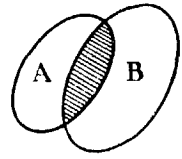
Dados dos conjuntos A y B, se define su *unión* $A \cup B$, como el conjunto que consta de todos los elementos que pertenecen al me-

nos a uno de los conjuntos A o B, y su *intersección*, $A \cap B$, como el conjunto de todos los elementos que pertenecen a A y a B.

Si los conjuntos son los del dibujo, la unión e intersección están representadas, respectivamente, por las partes rayadas.



$A \cup B$



$A \cap B$

Sea el conjunto $\mathcal{A}$, cuyos elementos son todos los subconjuntos de un conjunto U, incluído el conjunto vacío $\emptyset$, que es el conjunto que no posee ningún elemento.

Definamos dos leyes de composición interna: f_1, f_2: $\mathcal{A} \times \mathcal{A} \longrightarrow \mathcal{A}$ de la siguiente forma:

$$f_1(A, B) = A \cup B, \qquad f_2(A, B) = A \cap B.$$

Se ve fácilmente que dichas operaciones cumplen las siguientes propiedades:

1.ª *Asociativa:*

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

2.ª *Conmutativa:*

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

3.ª *Idempotente:*

$$A \cup A = A$$
$$A \cap A = A$$

4.ª *Simplificativa:*

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

Por gozar de estas propiedades se dice que el conjunto de partes de U es un retículo respecto de las dos operaciones unión e intersección. En general definiremos:

Retículo es un conjunto en el que se han definido dos operaciones internas que gozan de las cuatro propiedades anteriores.

Ejemplos: 1.º El anterior se llama retículo de las partes de un conjunto.

2.º El conjunto de todas las figuras lineales en el espacio, definiendo $A \cup B$ el conjunto de puntos de todas las rectas que resultan de unir cada punto de A con todos los de B y $A \cap B$ como en los conjuntos.

3.º En el conjunto de los enteros definimos los subconjuntos $A = \{a\}$ o conjunto de todos los múltiplos de un número a, $B = \{b\}$, etcétera, y llamamos:

$$A + B = \{a + b \quad a \in A,\ b \in B\}$$
$$A \cap B = \{c \quad c \in A,\ c \in B\}.$$

Respecto de estas dos operaciones los conjuntos de múltiplos de cada número entero constituyen un retículo.

Se puede demostrar que

$$A + B = \{\text{m. c. d. } (a, b)\}$$
$$A \cap B = \{\text{m. c. m. } (a, b)\}$$

4.º El conjunto de todos los sucesos, definiendo $A \cup B$ el hecho de suceder el A o el B y $A \cap B$ el suceder ambos simultáneamente.

5.º Si suponemos los conjuntos A y B definidos por las propiedades p y q, respectivamente, resultará que $A \cup B$ es el conjunto de todos los elementos que tiene la propiedad p "o" la propiedad q, mientras que $A \cap B$ es el conjunto de elementos que poseen las propiedades p "y" q. Esto sugiere considerar a las dos conjunciones o e y como operaciones entre proposiciones de un cierto universo lógico, ya que si A es una proposición y B otra, también "A o B" y "A y B" son, a su vez, proposiciones. Lo curioso es que estructurando el conjunto de proposiciones mediante las "operaciones" o e y, por tener estas operaciones las cuatro condiciones requeridas, queda definido el conjunto de proposiciones como un retículo. Este es el fundamento de la aplicación del álgebra a la lógica que dió origen a la hoy llamada lógica matemática.

14. PROPIEDADES DE LOS RETICULOS

Todo retículo es un conjunto ordenado, respecto de la siguiente relación de orden; dado un retículo R, definimos:

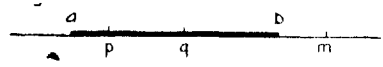
$$a \leq b \leftrightarrow a \cup b = b; \quad a \cap b = a.$$

Véase como ejercicio que esta relación es de orden.

En el retículo de las partes de un conjunto esta ordenación coincide con la de inclusión, ya que si $A \subset B$, entonces $A \cup B = B$ y $A \cap B = A$. No es cierto, en cambio, que todo conjunto ordenado sea retículo, a no ser que cumpla algunas condiciones más. Para ello tendremos que establecer algunas definiciones.

Dado un conjunto ordenado C y un subconjunto $S \subset C$, se dice que S está *acotado superiormente* por $m \in C$ cuando para todo $a \in S$ se verifica $a \leq m$; m se dice que es una *cota superior* de S. Si M es el conjunto de estas cotas y existe $s \in M$ tal que $s \leq m$ para todo $m \in M$, s es llamado *extremo superior* de S. Análogamente se definiría el *extremo inferior*.

Por ejemplo, si C es el conjunto de puntos de una recta y la ordenación establecida es $p \leq q$, si p no está a la derecha de q, y S es un segmento de extremos a y b, todo punto m a la derecha de b es una cota superior y el punto b es el extremo superior; análogamente a es el extremo inferior.



Pues bien, todo conjunto ordenado C, tal que para cada par de elementos a, $b \in C$ existe un extremo superior y un extremo inferior del subconjunto de C constituído por los elementos a y b, es un retículo. Bastará con que definamos las operaciones del retículo mediante las expresiones:

$$a \cup b = \text{extr. superior } (a, b).$$
$$a \cap b = \text{extr. inferior } (a, b).$$

Este resultado está sugerido por el retículo de partes de un conjunto que, como sabemos, está ordenado por la relación de inclusión. Entonces una cota superior de los conjuntos A y B será un conjunto M tal que $A \subset M$ y $B \subset M$, y como el menor conjunto que cumple estas dos condiciones es el conjunto $A \cup B$, resulta que $A \cup B = \text{extr. sup. } (A, B)$.

Del mismo modo, toda cota inferior de ambos conjuntos estará contenida en A y en B y $A \cap B$ es el mayor conjunto contenido en ambos, es decir, la mayor cota inferior, o sea, el extremo inferior.

EJERCICIOS

1. Pónganse ejemplos de conjuntos finitos, infinitos y de familias de conjuntos.

2. Los siguientes conjuntos están definidos por extensión, utilícese alguna propiedad que los defina por comprensión:

$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.
$\{1, 4, 9, 16, 25\}$.
$\{1, 2, 3, 5, 7, 11, 13, 17, 19, 23\}$.
$\{2, 4, 6, 8, 10\}$.
$\{-1, +1\}$.

3. Dados los conjuntos:

N: conjunto de los números naturales.
Z: íd. íd. enteros.
Q: id. id. racionales.
R: id. id. reales.
C: id. id. complejos.

Decir cuáles son ordenados y cuáles totalmente ordenados por la relación $\leq$.

4. Dado el conjunto $\{N, Z, Q, R, C\}$ (véase el ejercicio anterior). ¿Está ordenado este conjunto por la relación de inclusión? ¿Está totalmente ordenado?

5. Dado el conjunto $A = \{1, 2, 3, 4, 5\}$, ¿qué conjuntos X satisfacen simultáneamente a las relaciones

$$\{1, 2\} \subset X \qquad \text{y} \qquad X \subset A.$$

6. El conjunto producto $A \times A$ (producto cartesiano de A por sí mismo) tiene exactamente 9 elementos; dos de éstos son (p, q) y (r, q), donde p, q, r son distintos. ¿Cuáles son los siete restantes?

7. Dada una recta y un plano, ¿cuántos subconjuntos del mismo determinan?

8. Estudiar la intersección de los siguientes conjuntos:
   a) Una recta R y una circunferencia C.
   b) Dos circunferencias distintas C y C'.
   c) Dos círculos D y D'.

9. En un plano P se trazan dos circunferencias secantes. Determinar los subconjuntos que se forman.

10. Sea el conjunto universal $U = \{a, 1, b, 3, c, 5\}$. Sean $A = \{a, b, 3, 5\}$ y $B = \{b, c, 3, 5\}$.

a) Enumerar los subconjuntos de B. *b)* ¿Cuáles son los subconjuntos propios de B que a la vez lo son de A? *c)* ¿Cuáles son los subconjuntos de B disjuntos de A? *d)* ¿Qué subconjuntos de A están contenidos en B?

11. Demostrar que si A es el conjunto de elementos que gozan de la propiedad W y B el conjunto de los elementos que tienen la propiedad T y C es el conjunto de elementos que tienen a la vez las propiedades W y T, se verifica $C \subset A$ y $C \subset B$.

12. Definir sirviéndose de la noción de intersección de conjuntos, los siguientes entes geométricos: cuerda, segmento circular, sector circular, paralelogramo, rombo, trapecio. (NOTA: Para las tres últimas definiciones empléese la noción de *banda:* subconjunto de plano comprendido entre dos paralelas.)

13. Cada conjunto contiene como subconjuntos a sí mismo y al conjunto vacío (subconjuntos triviales o impropios). ¿Puede decirse de aquí que cada conjunto contiene al menos dos subconjuntos? ¿En qué condiciones un conjunto contiene exactamente dos subconjuntos?

14. Averiguar cuáles de las propiedades reflexiva, simétrica, transitiva o antisimétrica son aplicables a las relaciones siguientes:

a) «Es la madre de», para personas.
b) «Es de la misma longitud que», para segmentos
c) «No es igual a», para números.
d) «Primos entre sí», para números.
e) «Perpendicular a», para segmentos.
f) «Divisible por», para números.
g) «Contenido en», para conjuntos.
h) «Complementario de», para conjuntos.

15. Hay tres formas de expresar formalmente una relación:

$$aRb, \qquad (a, b) \in R, \qquad b \in \text{im. } (a).$$

Escribir de estas tres maneras las propiedades que definen a R como relación de equivalencia.

16. Estudiar las siguientes relaciones binarias de equivalencia:

a) «Paralela a», para rectas.
b) «Equipolente a», para vectores.
c) «Semejante a», para triángulos.

Definiendo por abstracción, respectivamente, cada uno de los conceptos de *dirección, vector libre* y *forma.*

17. Dado el conjunto producto $N \times N$, donde N es el conjunto de números naturales, se define una relación entre las parejas:

$$(a, b), (c, d) \in N \times N,$$

de la forma siguiente:

$$(a, b) \backsim (c, d) \leftrightarrow a + d = b + c.$$

Demostrar que esto es una relación de equivalencia. (Cada clase de equivalencia define así un número entero.)

18. Si en un conjunto C cada elemento a está en una relación R con un elemento (eventualmente él mismo) y se cumple: «De aRc y bRc se sigue aRb», entonces R es una relación de equivalencia. Demostrarlo.

19. Estudiar las aplicaciones siguientes:

a) Aplicación «valor absoluto» de un número complejo en un número real.

b) Aplicación «determinante de una matriz cuadrada».

c) La aplicación definida por la proyección estereográfica.

d) La aplicación «permutación de un conjunto», definida como transformación de un conjunto en sí mismo.

e) La aplicación «sucesión» del conjunto de los números naturales sobre cualquier conjunto.

f) Las transformaciones puntuales de la óptica geométrica.

II. ESTRUCTURAS ALGEBRAICAS

La primera estructura que hemos estudiado ha sido el retículo. Vamos ahora a dedicarnos a las llamadas estructuras algebraicas, que son las definidas mediante la introducción en un conjunto de elementos aritméticos o algebraicos, números, polinomios, matrices..., de las operaciones algebraicas, suma y producto. Nos ocuparemos en este capítulo de las estructuras algebraicas respecto de una sola operación interna, para estudiar posteriormente las estructuras con dos operaciones internas o una interna y otra externa.

1. SEMIGRUPOS Y GRUPOS

Dado un conjunto G y una operación interna definida sobre los elementos de dicho conjunto: $G \times G \longrightarrow G$, denotaremos esta operación por el signo genérico $\cdot$, de modo que expresaremos el resultado de la operación:

$$a \cdot b = c, \qquad \text{para todo } a, b \in G.$$

Y entonces también $c \in G$.

El signo $\cdot$ se sustituirá en cada caso por el de suma o producto, según sea la operación.

Si esta operación es asociativa se verificará:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c),$$

y entonces el conjunto se llama *semigrupo*.

Semigrupo.—Es todo conjunto sobre el que está definida una operación interna que goza de la propiedad asociativa.

Puede existir además un elemento, que denotaremos por e, tal que para todo $a \in G$ se verifique:

$$e \cdot a = a \qquad \text{y} \qquad a \cdot e = a.$$

Si G es un conjunto de números y $\cdot$ es la suma, $e = 0$, y si $\cdot$ es el producto, $e = 1$. Al elemento e se le llama *elemento neutro*, y se dice entonces que el semigrupo posee elemento neutro.

Si además para cada $a \in G$ existe un elemento $a \in G$, tal que

$$a \cdot a = e,$$

al conjunto se le llama grupo; a se llama *simétrico* o *inverso* de a, que es $-a$ para la operación suma y $a^{-1} = 1/a$, si la operación es el producto.

Grupo.—Un conjunto G sobre el que está definida una ley de composición interna $\cdot$ es un grupo si la ley $\cdot$ posee las tres propiedades siguientes:

1.ª La ley de composición es asociativa.

2.ª Tiene elemento neutro.

3.ª Todo elemento tiene simétrico o inverso.

Puede además el grupo, o el semigrupo, poseer la propiedad conmutativa, es decir:

$$a \cdot b = b \cdot a;$$

entonces el grupo, o el semigrupo, se llama *conmutativo* o *abeliano*.

2. EJEMPLOS

1.º Los números naturales, respecto de la operación suma, forman un semigrupo conmutativo.

2.º Los números naturales, respecto de la operación producto, forman un semigrupo conmutativo y con elemento neutro.

3.° El conjunto Z de los números enteros forma grupo respecto de la suma.

4.° El conjunto Q de los números racionales (menos el cero) es un grupo abeliano respecto de la multiplicación.

5.° Los retículos son también semigrupos respecto de las operaciones $\cup$, $\cap$:

$$A \cup (B \cup C) = (A \cup B) \cup C \qquad A \cap (B \cap C) = (A \cap B) \cap C$$
$$\emptyset \cup A = A \qquad U \cap A = A,$$

donde A, B, C son subconjuntos del universal U. Vemos, según el cuadro anterior que el elemento $\begin{Bmatrix} \emptyset \\ U \end{Bmatrix}$ hace de elemento neutro respecto de la operación $\begin{Bmatrix} \cup \\ \cap \end{Bmatrix}$. Es decir, son retículos con elemento neutro.

6.° Dados los conjuntos C, C' y C'' y las correspondencias o funciones f, g tales que:

$$C \xrightarrow{f} C' \xrightarrow{g} C'',$$

donde f está definida sobre C, y donde g está definida sobre C', de forma que:

$$a' = f(a) \in C' \qquad \text{y} \qquad a'' = g(a') \in C'';$$

si aplicamos sucesivamente las funciones f y g:

$$g[f(a)] = a'' \in C'',$$

que se escribe:

$$gf(a) = a'';$$

la correspondencia gf nos hace pasar directamente de a a a'', y se llama producto de f y g. La notación $gf(a)$ indica que al elemento a se aplica primero la función f y a $f(a)$ se le aplica luego g.

El producto de aplicaciones así definido goza, por su misma definición, de la propiedad asociativa: $h(gf) = (hg)f$. Si llamamos *aplicación idéntica* a una aplicación i: $A \longrightarrow A$, tal que $i(a) = a$ para todo $a \in A$, resulta inmediato que $fi = f$. El conjunto de aplicaciones entre conjuntos es, pues, un semigrupo con elemento neutro respecto del producto de aplicaciones que hemos definido.

En general no será grupo, ya que si $f(a) = a'$, la aplicación inversa de f transformará el elemento a' en el conjunto de sus originales de A, uno de los cuales es a, y, si bien $a \in$ or. (a'), no será en

general $a = \text{or.}\,(a')$. Si se verificara esto, f sería biunívoca, ya que a' sólo tendría un original a. Entonces:

$$f^{-1}[f(a)] = f^{-1}(a') = a,$$

luego $f^{-1}f(a) = a$ para todo $a \in A$, lo que nos dice que $f^{-1}f = i$. De modo que si todas las aplicaciones definidas entre los conjuntos son biunívocas, esas aplicaciones constituyen un grupo respecto del producto de aplicaciones. Este grupo, en general, no será abeliano.

3. SIGNIFICACION DEL GRUPO

En los ejemplos anteriores se ilustra una propiedad que queda en realidad de manifiesto en las mismas definiciones. Cuando un conjunto es un semigrupo respecto de una operación, pero no es grupo, podemos efectuar en él dicha operación, por ser ésta interna, pero no la inversa. Así, en el conjunto N de los números naturales que es un semigrupo aditivo, podemos sumar números naturales y obtenemos así un número natural; pero, salvo casos particulares, no podemos restar, dentro del mismo conjunto, dos números naturales. Del mismo modo, en el semigrupo multiplicativo de los enteros podemos multiplicar, pero no dividir, ya que, en general, dados dos enteros, no existe otro entero que sea su cociente.

Sólo cuando pasamos del semigrupo a un cierto grupo que lo contiene, podemos ya efectuar la operación inversa. Al pasar de N a Z, que es un grupo aditivo, podemos ya restar dos enteros cualesquiera, ya que por definición:

$$a - b = a + (-b) \qquad \text{y} \qquad -b \in Z$$

para todo $b \in Z$, por ser Z grupo aditivo.

Igual ocurre cuando pasamos de los enteros, Z, a los racionales, Q. En Z no se puede dividir, pero sí en Q, que es grupo multiplicativo, ya que si $a, b \in Q$, entonces $b^{-1} \in Q$ y se puede efectuar:

$$a/b = ab^{-1} \in Q.$$

Siempre que se pasa, pues, de la estructura de semigrupo a la de grupo se posibilita la operación opuesta a la que nos ha servido para definir el semigrupo.

Este es el proceso que históricamente ha seguido la evolución del concepto de número. Cuando la aritmética ha definido una operación en el conjunto de números existentes, sólo casualmente podría ocurrir que también la operación inversa fuese posible. El conjunto de números, en general, formaba un semigrupo, pero no un grupo, respecto de esa operación. Entonces la ampliación del campo

de los números se hacía siempre con la tendencia a dar sentido en el nuevo campo a la operación inversa.

Parece, entonces, que de los números naturales, que podían sumarse y multiplicarse, se pasase a los enteros para poder restar, y de éstos a los racionales para poder dividir. Así es como hoy estudiaríamos una teoría de números. No fué así, sin embargo, como históricamente sucedieron las cosas, como no es así tampoco como se introducen en el estudio elemental. El niño aprende antes los quebrados que los números negativos, y así también, históricamente, se introdujeron antes los números racionales positivos y después, bastantes siglos después, los números negativos, enteros y fraccionarios. Es decir, se buscó antes la inversa de la operación producto que la de la operación suma, aun siendo ésta anterior en la mente humana. ¿Cuál es la explicación de este fenómeno?

Fue en el siglo XVI cuando realmente comienzan a usarse los números negativos de un modo sistemático, a raíz de los trabajos de CARDANO, que investigaba la solución de la ecuación $x + n = 0$, con n número positivo, únicos números que entonces contaban. Las críticas de sus contemporáneos para quienes esa ecuación no tenía sentido, ilustran definitivamente el hecho. Porque todas ellas estaban basadas en el siguiente razonamiento: si la ecuación tuviera solución, ésta sería un número que sumado con n, nos daría cero, luego habría de ser un número más pequeño que cero, es decir, más pequeño que nada, y como no puede existir una cantidad más pequeña que nada, la ecuación carece de sentido.

En este razonamiento está claramente implícito que hasta aquella fecha el número no tenía otra significación que la de representar una cantidad y, por lo tanto, había de ser mayor o igual que cero, puesto que no cabían más alternativas que la de existir una cantidad a representar o no existir ninguna. Por eso ya desde los griegos existían los números naturales y también los fraccionarios positivos y se preveía la existencia de los irracionales, pero sólo positivos. En cambio, nada se sabía de los negativos. Sólo después de ser éstos introducidos y utilizados formalmente, se cayó en la cuenta de que tenían también un sentido en términos de cantidad, cuando se querían expresar cantidades de dos cualidades opuestas. El signo era la expresión de la cualidad.

4. CONCEPTO DE MAGNITUD Y CANTIDAD

De las consideraciones anteriores parece desprenderse que los conceptos de magnitud y cantidad pueden introducirse a través de los de grupo y semigrupo, según se atienda o no a la cualidad.

Cuando definimos la *magnitud* como un ente en el que se ha definido la igualdad y la suma, ya se ve que es una estructura respecto de una operación interna de suma.

Otras definiciones que se han dado son ya incorrectas. Si se dice que una magnitud es una cantidad que puede aumentar o disminuir, y luego que cantidad es lo que puede medirse, y al hablar de medida necesitamos saber qué cosa es una magnitud, que es aquello en que se define la medida, hemos caído en un círculo vicioso. Pero analizando estas ideas, sacadas de la observación, podemos precisar a qué hemos de llamar magnitud y cantidad.

Decir que la magnitud es una cantidad que puede aumentar o

disminuir, esto es, que puede convertirse en otra cantidad distinta, da la idea de magnitud como conjunto de cantidades. Al mismo tiempo, decir que éstas pueden aumentar o disminuir equivale a imponer que este conjunto de cantidades sea ordenado.

Desde nuestro nuevo punto de vista podremos definir así la *magnitud* como un semigrupo abeliano ordenado respecto de la operación suma.

Un semigrupo conmutativo, S, en el que está definida una suma, se dice que está *ordenado*, si para cualesquiera a, b pertenecientes a S, existe un $c \in S$, tal que:

$$a \leq b \Leftrightarrow a + c = b.$$

Es fácil ver que esta relación es una relación de orden.

Llamamos, pues, *magnitud* a todo semigrupo aditivo, abeliano y ordenado. Cada elemento del semigrupo es una *cantidad*.

Ejemplos.—Sea una recta en que determinamos segmentos. Establecemos una relación de congruencia R entre los segmentos de la recta: dos segmentos A_1A_2 y B_1B_2, son *congruentes* cuando, transportados el uno sobre el otro, coinciden. Establecemos una operación suma entre los elementos de distintas clases: para sumar dos segmentos (uno de cada clase) se sitúa un representante de la segunda clase a continuación del de la primera, y la suma de ambas clases es la clase definida por el segmento que tiene el origen del primero y el extremo del segundo.

Es inmediato que la suma así definida no depende del representante de la clase que escojamos para efectuarla. También se ve que dicha suma es conmutativa y asociativa. Entonces resulta que hemos construido un semigrupo de clases aditivo, conmutativo, que también es ordenado, el cual nos sirve para definir la magnitud "longitud de segmentos". La longitud de un segmento particular es la clase engendrada por ese segmento. Equivaldría a decir que todos los segmentos de la misma clase son equivalentes respecto de la longitud o que tienen igual longitud.

Podemos asimismo decir que dos polígonos son equivalentes cuando pueden descomponerse en el mismo número de triángulos iguales. Establecemos así una relación de equivalencia entre los polígonos que nos define el área mediante una triangulación. El conjunto de clases de polígonos equivalentes es la magnitud "área de polígonos" y una de las clases es la cantidad área de cada polígono de la clase.

Si en lugar de trabajar con cantidades positivas, lo hacemos con cantidades positivas y negativas, es decir, trabajamos sobre una estructura de grupo, podemos aplicar los resultados de la teoría ante-

rior. Unicamente habremos de definir aquí lo que se entiende por ordenación de un grupo.

Decimos que un grupo G está *ordenado* cuando contiene a un semigrupo S, tal que si $a \in G$, se verifica que a o $-a \in S$.

Entonces definimos una ordenación según esta ley así:

$$a \leq b \Leftrightarrow b - a \in S.$$

Por lo cual, dados $a, b \in G$: $\begin{cases} b - a \in S, & \text{o} \\ a - b \in S \end{cases}$

Se trata, pues, no sólo de una ordenación en G, sino de una ordenación total: todo grupo con estas condiciones está totalmente ordenado.

En definitiva, llamamos *magnitud* a todo semigrupo o grupo aditivo, abeliano y ordenado.

5. MAGNITUDES ESCALARES

Dentro de las magnitudes, las llamadas escalares cumplen, además de las anteriores condiciones, esta otra: el tener una ordenación arquimediana.

Se dice que los elementos de un conjunto C tienen ordenación *arquimediana* cuando dados $a, b \in C$,

si $a \leq b$, existe un número natural $n \in N$, tal que $b \leq na$. [3]

Aun cuando se trate de un semigrupo o grupo aditivo tiene sentido el producto $na = a + a + a + \ldots\ldots + a$ con n sumandos iguales a a.

Los números naturales tienen ordenación arquimediana, pero no la tienen, por ejemplo, los elementos del conjunto $Z \times Z$, en los que se haya definido una relación de orden así:

$$(a, b) < (c, d) \qquad \text{si} \quad \begin{cases} a < c & \text{o} \\ a = c, & b < d, \end{cases}$$

llamando suma de dos elementos a la definida por:

$$(a, b) + (a', b') = (a + a', b + b').$$

En efecto, dados los elementos $(0, 1)$ y $(1, a)$, se cumple:

$$(0, 1) < (1, a),$$

pero no existe ningún $n \in N$, tal que $(1, a) \leq n(0, 1)$, ya que:

$$n(0, 1) = (0, n) \qquad \text{y} \qquad (0, n) < (1, a).$$

Estas magnitudes escalares son la generalización de las que se pueden representar mediante "escalas", es decir, mediante puntos de una recta, de tal modo que la distancia de cada punto a un punto fijo mida cada una de las cantidades de esa magnitud. Pero esta representación, que equivale a la definida por los segmentos de una recta, es precisamente el ejemplo más sencillo, y quizá originario, del cumplimiento del postulado de Arquímedes, que es el que hemos utilizado en [3] como definición de ordenación arquimediana.

En resumen, pues, una *magnitud escalar* es un semigrupo (o grupo) aditivo, abeliano y arquimediano.

Todavía, una vez definido este concepto, no podemos, mientras no estudiemos la noción de cuerpo, multiplicar y dividir cantidades de una misma magnitud ni comparar magnitudes entre sí, idea básica para poder definir el concepto de medida. Enviamos al lector que desee puntualizar estos extremos al libro de P. ABELLANAS, *Matemáticas para físicos e ingenieros*, Ed. Romo, Madrid, 1963.

6. HOMOMORFISMOS E ISOMORFISMOS

Sean G y G' dos grupos y h una aplicación de G en G':

$$G \xrightarrow{h} G'.$$

Decimos que h es un *homomorfismo* si conserva la operación que define el grupo, esto es, si

$$h(a \cdot b) = h(a) \cdot h(b),$$

para cualesquiera $a, b \in G$.

Más específicamente, si G y G' son aditivos y

$$h(a) = a', \qquad h(b) = b' \in G',$$

se deberá tener, para que h sea un homomorfismo:

$$h(a + b) = h(a) + h(b) = a' + b'.$$

Si G y G' fuesen ambos multiplicativos, el homomorfismo cumplirá:

$$h(a \cdot b) = h(a) \cdot h(b).$$

Puede ocurrir que G sea aditivo y G' multiplicativo, o viceversa. En ese caso se tendrá, respectivamente:

$$h(a + b) = h(a) \cdot h(b)$$
$$h(ab) = h(a) + h(b).$$

Ejemplo.—Un ejemplo sencillo de homomorfismo nos lo proporciona nuestro modo usual de contar las horas. Supuesto que conocié-

semos la "hora cero", en un momento dado habrían transcurrido un número n de horas, todo lo grande que se quiera; sin embargo, nosotros, al contar de 24 en 24, hacemos corresponder a cada hora, contada a partir de la hora cero, su resto de la división por 24. Y a la suma de horas corresponde la suma de sus restos al dividir por 24.

Si la correspondencia definida por el homomorfismo es biunívoca, esto es, si para cada $h(a)$ existe *un solo* elemento a original de $h(a)$ en

$$a \xrightarrow{h} h(a),$$

entonces se llama *isomorfismo*.

Ejemplo.—Llamemos R^+ al grupo multiplicativo de los números reales positivos y R al grupo aditivo de todos los números reales y sea la correspondencia la función "logaritmo":

$$R^+ \xrightarrow{\log} R.$$

Esta correspondencia es biunívoca, pues para todo $x \in R^+$,

$$x \text{ determina } (\log \cdot x).$$

Además se verifica que si $x, y \in R^+$ $\begin{cases} x \longrightarrow \log x \\ y \longrightarrow \log y \end{cases}$

$$x \cdot y \longrightarrow \log (x \cdot y) = \log x + \log y,$$

o sea que la transformada del producto $x \cdot y$ es igual a la suma de las transformadas: $\log x + \log y$.

La correspondencia definida por la función exponencial es, en cambio, un isomorfismo del grupo aditivo R sobre el grupo multiplicativo R^+.

Decir que dos grupos son isomorfos es lo mismo que decir que, en cuanto grupos, son identificables, esto es, que los resultados que obtengamos al operar con los elementos de uno de ellos se corresponden con los que se obtienen al operar con los elementos correspondientes del otro. Por eso se suelen identificar los grupos isomorfos, considerando como idénticos dos elementos, uno de cada grupo, que se correspondan en el isomorfismo.

Es lo que hacemos en muchas ocasiones en problemas, incluso de la Matemática elemental. Cuando queremos, por ejemplo, sumar ángulos, recurrimos o bien a colocarlos como dos ángulos contiguos que tengan un lado común y decir que el ángulo suma es el definido por los otros dos lados, o bien a medir ambos ángulos y decir que el ángulo suma es el que tiene por medida la suma de las de los otros dos. Al decir esto, implícitamente reconocemos el isomorfismo entre los ángulos y sus medidas, ya que la suma de dos ángulos implica la suma de sus medidas.

Si, en particular $G = G'$, el homomorfismo recibe el nombre particular de *endomorfismo* y el isoformismo el de *automorfismo*.

En el grupo aditivo Z se puede definir el automorfismo:

$$a \longrightarrow -a,$$

en el cual a

$$a + b \longrightarrow -(a + b) = -a - b.$$

Del mismo modo en el grupo multiplicativo Q de los números racionales menos el cero, es un automorfismo la aplicación

$$a \longrightarrow a^{-1},$$

en la que al producto $a \cdot b$ corresponde el número $\frac{1}{ab} = \frac{1}{a} \cdot \frac{1}{b}$, es decir, el producto de los correspondientes.

7. SUBGRUPO

Sea H un subconjunto del grupo G; diremos que H es un subgrupo de G si, respecto de la misma ley interna de G, los elementos de H forman a su vez un grupo.

Esto implica, por tanto, que dicha ley sea asociativa, que posea elemento neutro (que es el mismo que el del grupo G) y cada elemento su inverso. Por ejemplo, el grupo aditivo de los enteros es un subgrupo del de los racionales. El grupo multiplicativo de los racionales es un subgrupo del de los reales.

Damos a continuación un criterio que nos permite conocer cuándo un subconjunto de un grupo G es un subgrupo.

TEOREMA.—*La condición necesaria y suficiente para que* H *sea un subgrupo de* G *es que para cada par* a, b ∈ H *se cumpla:*

$$a - b \in H.$$

La condición es necesaria:

Supuesto que H es grupo y que $a, b \in H$, también $-b \in H$ y, por tanto, la operación interna:

$$a + (-b) = a - b,$$

definida sobre todos los elementos de H da como resultado un elemento de H.

La condición es suficiente. Probemos que si $a - b \in H$, H es un grupo que por estar contenido en G, será un subgrupo de G.

La antedicha condición podemos expresarla en particular:

$$a - a \in H \Rightarrow 0 \in H.$$

O sea, que el elemento neutro pertenece a H.

Si el $0 \in H$, entonces

$$0 - b = 0 + (-b) \in H,$$

que, por ser $b \in H$ arbitrario, nos dice que el opuesto de cualquier elemento pertenece a H.

Y, como la operación definida sobre G es la misma que la definida sobre H, si es asociativa en G también lo es en H. Queda así demostrada la condición suficiente para que H sea subgrupo.

Otro ejemplo de subgrupo, fácilmente reconocible por este criterio, es el subconjunto de los enteros pares respecto al grupo aditivo de los enteros. No lo es, en cambio, el conjunto de los impares, ya que la diferencia de dos números impares no es impar sino par.

8. NUCLEO DE UN HOMOMORFISMO

Antes de definir lo que se entiende por núcleo de un homomorfismo demostraremos el siguiente teorema:

TEOREMA.—*Sean* G *y* G′ *dos grupos aditivos y* h *un homomorfismo de* G *en* G′, *se verifica:*

1.º $h(0) = 0$, *siendo* 0 *el elemento neutro de ambos grupos.*

2.º $h(-a) = -h(a)$ *para todo* $a \in G$.

3.º $h(a - b) = h(a) - h(b)$.

DEMOSTRACIÓN.—1.º Como $a = a + 0$, aplicando el homomorfismo se tiene:

$$h(a) = h(a + 0) = h(a) + h(0) \Rightarrow h(0) = 0.$$

2.º De $a + (-a) = 0 \Rightarrow h[a + (-a)] = h(0) = 0$; luego

$$h(a) + h(-a) = 0 \Rightarrow h(-a) = -h(a).$$

3.º $h(a - b) = h[a + (-b)] = h(a) + h(-b) = h(a) - h(b)$.

Lo mismo ocurriría si ambos grupos o uno de ellos fuesen multiplicativos. Bastaría sustituir donde correspondiese el cero por el elemento unidad, el opuesto por el inverso y la diferencia por el cociente.

Se llama *núcleo* de un homomorfismo

$$G \xrightarrow{h} G'$$

al conjunto N de todos los elementos de G cuya imagen es el elemento neutro de G'.

TEOREMA.—*El núcleo* N *es un subgrupo de* G.

Basta con demostrar que si $a, b \in N$, también $a - b \in N$. Por hipótesis se verifica $h(a) = h(b) = 0$ para $a, b \in N$, en el supuesto de que G' sea aditivo. Lo mismo se haría en los demás casos. Entonces:

$$h(a - b) = h(a) - h(b) = 0 - 0 = 0.$$

Es decir, el elemento $a - b$ tiene como imagen el elemento 0, lo cual es lo mismo que afirmar que $a - b \in N$.

Por ejemplo, en el homomorfisco establecido entre el grupo aditivo Z y el formado por los tres restos $\{0, 1, 2\}$ de la división por 3, tal que a cada elemento de Z le hacemos corresponder su resto módulo 3, el núcleo de este homomorfismo es el subgrupo de Z formado por todos los múltiplos de 3.

9. GRUPO DE CLASES DE RESTOS

La situación que vamos a describir ahora es una generalización del ejemplo que acabamos de poner. En aquel homomorfismo a cada número entero le hacemos corresponder el resto mod. 3, lo que equivale a establecer las clases de números congruentes respecto del mod. 3. Sabemos que si

$$\left.\begin{array}{l} m_1 \equiv r_1 \ (3) \\ m_2 \equiv r_2 \ (3) \end{array}\right\} \quad \text{donde} \quad r_1, r_2 \in \{0, 1, 2\}.$$

Entonces $m_1 + m_2 \equiv r_1 + r_2 \ (3)$.

Si $r_1 + r_2 > 3$ y da resto r respecto de 3, entonces escribimos simplemente que $m_1 + m_2 \equiv r \ (3)$.

Este modo de operar en esencia equivale a lo siguiente: sea

$$(3) = \{\ldots\ldots, -6, -3, 0, 3, 6, \ldots\ldots\}$$

el conjunto de todos los múltiplos de 3 y llamemos

$$1 + (3) = \{\ldots\ldots, -5, -2, 1, 4, 7, \ldots\ldots\}$$
$$2 + (3) = \{\ldots\ldots, -4, -1, 2, 5, 8, \ldots\ldots\}.$$

Quedan así clasificados todos los números enteros en las tres clases (3), $1 + (3)$ y $2 + (3)$, que son respectivamente las clases de números que dan resto 0, 1 ó 2 al dividir por 3. Dos números enteros pertenecen a la misma clase cuando su diferencia es un múltiplo de 3, esto es, cuando su diferencia pertenece al subgrupo (3). Cualquiera de los elementos de una clase puede tomarse como representante de ella; en particular se suelen tomar el 0, 1 y 2 respectivamente.

Pues bien, sumando dos números, uno de cada clase, nos da otro número de otra clase, coincidente o no con las anteriores, pero de tal modo que si hubiéramos elegido otros números de las mismas primeras clases el resultado sería un número de la misma clase que la obtenida anteriormente. Esto es análogo a la ley de la suma de números congruentes a que nos hemos referido antes.

Podemos entonces formar una tabla de suma de clases que sería la siguiente:

$$0 + 0 = 0 \qquad 0 + 2 = 2 \qquad 1 + 2 = 0$$
$$0 + 1 = 1 \qquad 1 + 1 = 2 \qquad 2 + 2 = 1$$

entendiéndose que al escribir, por ejemplo, $1 + 2 = 0$ eso significa que $[1 + (3)] + [2 + (3)] = 0 + (3) = (3)$, es decir, que sumando cualquier número de la clase $1 + (3)$ con uno cualquiera de la clase $2 + (3)$ se obtiene un número de la clase (3), o todavía que la suma de un número que da resto 1, con otro que da resto 2, al dividir por 3, es un múltiplo de 3:

$$\begin{array}{r} a \equiv 1 \ (3) \\ b \equiv 2 \ (3) \\ \hline a + b \equiv 3 \ (3) \equiv 0 \ (3) \end{array}$$

Generalizamos ahora todo esto al caso de tratarse de un grupo aditivo abeliano G y de un subgrupo suyo H. G y H harán ahora el papel que en el caso particular anterior desempeñaban Z y (3). Si

$$H = \{h_1, h_2, h_3, \ldots\},$$

a cada elemento $a \in G$ diremos que le corresponde la clase

$$a + H = \{a + h_1, a + h_2, \ldots\}.$$

De la definición de clases así establecida resulta inmediatamente que dos elementos a, b pertenecen a la misma clase cuando su diferencia $a - b \in H$; en efecto, si a, $b \in m + H$, serán:

$$a = m + h_1, \qquad b = m + h_2;$$

luego $a - b = h_1 - h_2 \in H$, por ser H un subgrupo. De aquí resulta que la condición necesaria y suficiente para que dos clases $a + H$ y $b + H$ sean la misma clase es que $a - b \in H$.

A cada una de las clases así definidas le llamamos una *clase de restos* del grupo G respecto del subgrupo H. Al conjunto de todas ellas lo representaremos por G/H. Por todo el razonamiento seguido resulta que esas clases de restos son clases de equivalencia en G.

Vamos a demostrar que el conjunto G/H de clases de restos es un grupo aditivo. Para ello definimos la suma de dos clases así:

$$(a + H) + (b + H) = (a + b) + H.$$

Lo primero que hay que demostrar es que esta definición de suma es independiente de los dos representantes a y b elegidos para cada clase. Sean, en efecto, a' y b' respectivamente, otros representantes, es decir,

$$a' + H = a + H \Leftrightarrow a' - a \in H$$
$$b' + H = b + H \Leftrightarrow b' - b \in H$$

resulta, pues, que $(a' - a) + (b' - b) = (a' + b') - (a + b) \in H$, lo que equivale a decir que $(a' + b') + H = (a + b) + H$, es decir, que obtenemos la misma clase suma cualesquiera que sean los representantes de que nos sirvamos en las clases sumandos.

De la misma definición de suma resulta inmediatamente, por ser G un grupo, que se cumple la propiedad asociativa:

$$[(a + H) + (b + H)] + (c + H) = (a + H) + [(b + H) + (c + H)],$$

ya que ambos miembros son respectivamente iguales a

$$[(a + b) + c] + H = [a + (b + c)] + H.$$

Existe el elemento neutro de la suma de clases que es la clase $H = 0 + H$, ya que

$$(0 + H) + (a + H) = (0 + a) + H = a + H.$$

Y, finalmente, dada una clase cualquiera $a + H$, existe siempre otra, que es precisamente la $-a + H$, con la propiedad de que sumada con la anterior, nos da la clase neutra H. Esto completa la demostración de que G/H es un grupo.

Estudiemos ahora el homomorfismo que se puede establecer entre los dos grupos G y G/H. Haremos corresponder en este homomorfismo a cada elemento $a \in G$ el elemento $a + H \in G/H$. Evidentemente, por la definición de suma de clases esta aplicación conserva las operaciones de grupo; es, por tanto, un homomorfismo, al que llamaremos *homomorfismo natural* o *canónico*. El núcleo de este homomorfismo es precisamente el subgrupo H de G, como es inmediato comprobar.

Hemos establecido así una teoría recíproca a la del párrafo anterior. En él, dado un homomorfismo entre dos grupos, veíamos que el núcleo era un subgrupo del grupo original. Ahora hemos visto que, dado un grupo y un subgrupo suyo, se puede definir un homomorfismo entre el grupo dado y el grupo de clases de restos respecto

del subgrupo, de tal modo que el núcleo de ese homomorfismo es el subgrupo dado.

10. GRUPOS DE TRANSFORMACIONES

Sea C un conjunto cualquiera y consideremos el conjunto de todas las aplicaciones biunívocas de C en sí mismo. Vimos ya que este conjunto de transformaciones formaba un grupo respecto de la operación que habíamos definido como producto de transformaciones.

Vamos a ver ahora cómo un grupo de aplicaciones biunívocas definido en C permite establecer una clasificación en C. Bastará que veamos cómo podemos definir mediante dichas aplicaciones una relación de equivalencia.

Diremos que dos elementos de C son equivalentes respecto de la relación de equivalencia introducida por el grupo de transformaciones cuando hay una transformación del grupo que transforma uno de los elementos en el otro. Vamos a demostrar que ésta es, en efecto, una relación de equivalencia.

1.º *Propiedad reflexiva.*—$a \backsim a$, para todo $a \in C$.

En efecto, por formar un grupo el conjunto de transformaciones, existe entre ellas la transformación idéntica, es decir, la transformación que transforma cada elemento en sí mismo. Existe, pues, en el grupo una transformación que hace pasar de a a a, luego a es equivalente a sí mismo.

2.º *Propiedad recíproca.*—Si $a \backsim b$, existirá una transformación f que haga pasar de a a b. Pero entonces la inversa de f, que existe por formar grupo las transformaciones, transformará b en a, luego $b \backsim a$.

3.º *Propiedad transitiva.*—Supongamos que sea $a \backsim b$ y $b \backsim c$. Eso quiere decir que existe una transformación f que transforma a en b y otra g que transforma b en c. Entonces, en el grupo de transformaciones existe la transformación producto gf que transforma a en c, por definición de producto de transformaciones; de donde se sigue que $a \backsim c$.

Un ejemplo clásico de la clasificación engendrada por un grupo de transformaciones es el del concepto de Geometría según KLEIN. Según esta idea se trataría de definir grupos de transformaciones geométricas que, al clasificarnos las figuras de un cierto espacio, nos definirían una geometría para la cual todas las figuras de una misma clase serían equivalentes respecto de las propiedades características de esa geometría.

Los principales grupos de transformaciones geométricas que dan lugar a Geometrías de Klein son sucesivamente los siguientes:

El grupo de los movimientos, es decir, de las traslaciones, giros y simetrías y sus productos. Una figura cualquiera transformada por un movimiento pasa a ser otra figura igual a ella y de las mismas dimensiones o, como se suele llamar, congruente con ella. Respecto, pues, del grupo de los movimientos todas las figuras congruentes entre sí pertenecen a la misma clase. Para la Geometría correspondiente a este grupo todas las figuras congruentes son equivalentes, es decir, las puede estudiar como si se tratase de una misma figura. Esta Geometría será según esto, el estudio de todas las propiedades que permanecen invariantes por el grupo de los movimientos, y se llama *Geometría de la congruencia*.

Grupo de las semejanzas. Se puede considerar como constituido por todos los movimientos, homotecias y sus productos. Dos figuras serán semejantes, y por tanto equivalentes respecto de la relación definida por este grupo, cuando se pueda pasar de una a otra mediante una semejanza. Todas las figuras semejantes entre sí son, pues, la misma figura para la Geometría correspondiente a este grupo, que se llama *Geometría equiforme*, ya que las figuras conservan su forma al transformarse por semejanzas. La Geometría equiforme será, por lo tanto, el estudio de todas las propiedades de las figuras que permanecen invariantes por el grupo de las semejanzas. El grupo de los movimientos es un subgrupo del de las semejanzas, por lo que la Geometría de la congruencia puede considerarse como una subgeometría de la equiforme.

Análogamente, para no repetir las mismas ideas, en los grupos sucesivos de transformaciones que podemos ir considerando, llamaremos *Geometría afín* al estudio de las propiedades invariantes por el grupo de las afinidades; *Geometría proyectiva* a la correspondiente al grupo de las proyectividades, etc. En general, toda geometría en el sentido de Klein será, pues, la que estudia las propiedades invariantes mediante un grupo de transformaciones.

EJERCICIOS

1. Demostrar que las matrices cuadradas de cualquier orden, los vectores libres y los números complejos forman grupo aditivo, respectivamente.

2. ¿Forman grupo los números reales positivos con la adición? ¿Y con la multiplicación? ¿Lo forman los enteros pares con la adición? ¿Y los impares?

3. Estudiar las rotaciones y simetrías del cuadrado como grupo de transformaciones del mismo.

4. Idem para el triángulo equilátero.

5. Un semigrupo conmutativo S respecto a una operación suma se dice que está ordenado si para $a, b \in S$, existe un $c \in S$ tal que:

$$a \leq b \Leftrightarrow a + c = b.$$

Demuéstrese que cumple las tres propiedades de una relación de orden.

6. Un grupo G está ordenado cuando contiene a un semigrupo S, tal que para cualquier $a \in G$ se verifica:

$$a \quad o \quad -a \in G.$$

Entonces definimos una ordenación según esta ley:

$$a \preceq b \Leftrightarrow b - a \in S.$$

Y para cualesquiera a, $b \Rightarrow \begin{cases} b - a \in S \\ a - b \in S \end{cases}$

Demuéstrese que es una ley de ordenación.

7. Demostrar que las clases de números congruentes mod. (m) forman grupo abeliano.

8. Demostrar que los números 1, i, -1, $-i$ forman un grupo abeliano respecto de la multiplicación ordinaria.

9. Demostrar que en un grupo no conmutativo se verifica:

$$(ab)^{-1} = b^{-1}a^{-1}.$$

10. Si G es un conjunto no vacío con una multiplicación asociativa respecto a la cual todas las ecuaciones $xa = b$, $ay = b$ tienen soluciones x, $y \in G$, entonces G es un grupo.

11. Demostrar que si $x^2 = e$ (e es el elemento neutro) para cualquier $x \in G$, donde G es un grupo, G es conmutativo.

12. Demostrar que el grupo aditivo de enteros mod. (4) es isomorfo con el grupo de rotaciones del cuadrado.

13. Encontrar un grupo de transformaciones geométricas que sea isomorfo a los siguientes grupos abstractos:

a) Grupo aditivo de todos los números reales.

b) Grupo multiplicativo de todos los números reales no nulos.

c) Grupo aditivo de enteros mod. (6).

14. Si T es un subgrupo de S y S, a su vez, un subgrupo de G, T es un subgrupo de G.

15. Demostrar que en cualquier grupo G el conjunto de los elementos a, tales que:

$$ax = xa,$$

para cualquier $x \in G$, es un subgrupo de G.

III. ESTRUCTURAS RESPECTO DE DOS OPERACIONES

1. ANILLOS

En lo que sigue supondremos siempre que las dos operaciones definidas en un conjunto son la suma y el producto.

Un conjunto A en el que se han definido las operaciones de suma y producto se dice que es un *anillo* respecto de estas dos operaciones, cuando se verifica:

1.º A es un grupo abeliano respecto de la suma.

2.º Es un semigrupo respecto del producto.

3.º Posee la propiedad distributiva:

$$a(b + c) = ab + ac$$
$$(b + c)a = ba + ca.$$

Un anillo se dice *conmutativo* si el producto tiene la propiedad conmutativa y se dice que es un anillo *con elemento unidad*, si el semigrupo multiplicativo posee elemento unidad.

El ejemplo más sencillo de anillo es el conjunto Z de números enteros: es un anillo conmutativo con elemento unidad. También lo es el conjunto $Z[X]$ de todos los polinomios:

$$a_0 + a_1X + \ldots\ldots + a_nX^n,$$

en los que todos los coeficientes $a_i \in Z$. De igual modo definiríamos los anillos de polinomios $Q[X]$ en la indeterminada X con coeficientes del conjunto Q de los números racionales, etc. Asimismo forman anillo también los polinomios en varias indeterminadas, $X_1, X_2, \ldots, X_r$ con coeficientes en Z, anillo que se representa por

$$Z[X_1, X_2, \ldots\ldots, X_r].$$

En cualquier anillo se verifican las siguientes propiedades:

1.ª $a0 = 0$, para cualquier a del anillo, siendo 0 el elemento neutro de la suma. En efecto,

$$ab = a(b + 0) = ab + a0 \Rightarrow a0 = 0,$$

basándonos en la propiedad distributiva.

2.ª $a(-b) = -ab$.
En efecto,

$$a(b - b) = ab + a(-b) = a0 = 0.$$

Luego $a(-b)$ es, como se ve, el opuesto de ab.
Del mismo modo se demostraría que $(-a)b = -ab$.

3.ª $(-a)(-b) = ab$.

$$-a0 = (-a)(b - b) = (-a)b + (-a)(-b) = -ab + (-a)(-b) = 0,$$

de donde resulta el enunciado.

No es cierta, en cambio, la propiedad recíproca de la primera que acabamos de ver, es decir, de que $ab = 0$, no se sigue necesariamente

que uno, al menos, de los dos factores sea cero. Veamos un ejemplo en el que no ocurre esto.

Sea el conjunto de pares de números enteros (a, b), $a, b \in Z$ que ya hemos considerado en alguna otra ocasión, y definamos entre ellos las operaciones de suma y producto en la siguiente forma:

$$(a, b) + (c, d) = (a + c, b + d)$$
$$(a, b)\,(c, d) = (ac, bd).$$

Para estas dos operaciones es inmediato comprobar que ese conjunto de pares forma un anillo. El elemento neutro de la suma es el par (0, 0) y el del producto el (1, 1). Pues bien, se pueden encontrar productos de dos factores, ambos distintos del elemento neutro de la suma, cuyo producto sea, en cambio, éste. Por ejemplo:

$$(1, 0)\,(0, 1) = (0, 0).$$

Cuando en un anillo se verifica que $ab = 0$, sin ser cero, ni a, ni b, se dice que los elementos a y b son *divisores de cero*. Si un anillo no posee divisores de cero se dice que es un *dominio de integridad*. El anillo de los enteros, por ejemplo, es un dominio de integridad, y también el de los polinomios en una variable con coeficientes en Z.

2. DEFINICION DE CUERPO

En un anillo, en general, no existe para cada uno de sus elementos a el elemento inverso a^{-1}, tal que $aa^{-1} = 1$, ya que respecto de la multiplicación sólo se ha impuesto la condición de ser semigrupo. No obstante puede ocurrir que existan algunos elementos en el anillo que posean inverso, también perteneciente al anillo. Así ocurre, por ejemplo, con el elemento -1, que en el anillo de los números enteros tiene inverso, él mismo, ya que $(-1)\,(-1) = 1$. Del mismo modo, en el anillo de polinomios $Q[X]$, todos los elementos de Q, excepto el cero, es decir, todos los polinomios de grado cero, tienen inverso perteneciente al mismo anillo.

A los elementos de un anillo cuyos inversos pertenecen al anillo se les llama *unidades* de este anillo. No debe confundirse el concepto de unidad de un anillo que acabamos de definir, con el de elemento unidad del anillo, que es el elemento neutro de la multiplicación.

Cuando un anillo es dominio de integridad y se verifica que todos los elementos del anillo, excepto el cero, son unidades del mismo, al anillo se le llama cuerpo.

Cuerpo es, pues, un anillo en el que cada elemento tiene inverso. Equivale esto a decir que un cuerpo es un conjunto con dos operaciones, suma y producto, respecto de las cuales es grupo aditivo y

grupo multiplicativo y posee la propiedad distributiva. El grupo aditivo es siempre abeliano. Si el grupo multiplicativo es también abeliano, el cuerpo se llama *conmutativo;* si no lo es, será un cuerpo no conmutativo.

Los conjuntos de números racionales, reales y complejos son ejemplos sencillos de cuerpos.

Se puede demostrar fácilmente que todo cuerpo es un dominio de integridad. En efecto, si $ab = 0$, y $b \neq 0$, el elemento b^{-1} pertenece al cuerpo; multiplicando por él a la derecha la igualdad anterior se obtiene: $abb^{-1} = a = 0b^{-1} = 0$.

3. IDEAL DE UN ANILLO

A partir de aquí supondremos siempre que los anillos de que tratamos son conmutativos y con elemento unidad.

Dado un anillo A, se dice que un subconjunto suyo S es un *subanillo* de A cuando S es a su vez un anillo.

Por ser subanillo, S será subgrupo del grupo aditivo de A. Entonces, para comprobar si un subconjunto S de A es un subanillo suyo bastará demostrar que se cumplen las dos condiciones siguientes:

a) Si $a, b \in S \Rightarrow a - b \in S$.

b) $a, b \in S \Rightarrow ab \in S$.

Estas dos condiciones son necesarias y suficientes, como se puede probar en seguida.

Dados dos anillos, A y A', se dice que una aplicación h de A en A' es un *homomorfismo* cuando conserva las dos operaciones de suma y producto, esto es:

$$h(a + b) = h(a) + h(b).$$
$$h(ab) = h(a)\,h(b).$$

Como en el caso de los grupos se llama *núcleo* de ese homomorfismo al conjunto N de elementos de A que se representan sobre el 0 de A'.

Cuando el núcleo N del homomorfismo consta exclusivamente del elemento 0 de A, la aplicación h es entonces una correspondencia biunívoca y se llama *isomorfismo.*

Vamos ahora a demostrar que el núcleo de un homomorfismo es siempre un subanillo del anillo original A. En efecto, si

$$a, b \in N \Rightarrow h(a) = h(b) = 0;$$

entonces, por lo demostrado para grupos,

$$h(a - b) = h(a) - h(b) = 0 \Rightarrow a - b \in N.$$

Del mismo modo,

$$h(ab) = h(a)\, h(b) = 0 \Rightarrow ab \in N,$$

como queríamos demostrar.

Podemos observar que la última condición es superabundante. Para que $h(a)\, h(b)$ sea igual a cero bastará con que lo sea uno solo de los factores. Resulta entonces que el núcleo del homomorfismo cumple una condición multiplicativa más fuerte que la necesaria para ser simplemente subanillo. En efecto, si $a \in N$ y $b \in A$, aun cuando b no pertenezca a N, se tendrá que $ab \in N$, ya que

$$h(a)\, h(b) = 0 \cdot h(b) = 0.$$

Por cumplir esta condición más restrictiva se dice que el núcleo es un ideal del anillo A.

Definiremos, pues, el concepto de *ideal* de un anillo A diciendo que es cualquier subconjunto $I \subset A$, tal que satisfaga las dos siguientes condiciones:

1.ª $a,\ b \in I \Rightarrow a - b \in I.$

2.ª $a \in I,\ b \in A \Rightarrow ab \in I.$

Resulta, pues, que todo ideal de un anillo es un subanillo suyo y, por lo tanto, un subgrupo del grupo aditivo del anillo. No es cierto, en cambio, que, recíprocamente, todo subanillo sea un ideal.

Un ejemplo de ideal es el conjunto de todos los números pares en el anillo de los números enteros. También lo es el conjunto de múltiplos de un entero cualquiera.

En general, si A es un anillo cualquiera y a un elemento suyo, el conjunto de múltiplos de a, es decir, el conjunto

$$\{ax \mid x \in A\}$$

es un ideal de A. A los ideales de este tipo, engendrados por un único elemento del anillo, se les llama ideales *principales*. También el conjunto

$$\{a_1x_1 + a_2x_2 + \ldots\ldots + a_nx_n \mid x_i \in A\}$$

forma un ideal que se dice engendrado por los elementos

$$a_1,\ a_2,\ a_3,\ \ldots\ldots,\ a_n \in A.$$

La demostración es inmediata.

4. ANILLO DE CLASES DE RESTOS

Como dado un ideal I de un anillo A, este ideal es, como hemos visto, un subgrupo del grupo aditivo de A, podemos tomar clases de restos de este grupo respecto del subgrupo I en la forma en que lo vimos al hablar de grupos. Diremos ahora que mediante esta operación tomamos clases de restos del anillo A respecto del ideal I y llamamos al conjunto de estas clases A/I.

Por todas las propiedades que anteriormente estudiamos resultará que dos elementos $a, b \in A$ pertenecen a la misma clase de restos del conjunto de clases A/I cuando $a - b \in I$. Por analogía de las congruencias con números enteros, que es un caso particular de éste, escribiremos también eso mismo en la forma $a \equiv b(I)$.

También por el estudio hecho en los grupos resulta que el conjunto A/I es un grupo aditivo para la siguiente definición de suma:

$$(a + I) + (b + I) = (a + b) + I.$$

Si además de esta operación definimos en A/I un producto mediante:

$$(a + I)(b + I) = (ab) + I,$$

vamos a demostrar que respecto de estas dos operaciones A/I es un anillo. Lo primero que vamos a demostrar es la propiedad uniforme de la multiplicación, es decir, si

$$a' + I = a + I \qquad \text{y} \qquad b' + I = b + I,$$

entonces

$$a'b' + I = ab + I.$$

En efecto, de las hipótesis resulta:

$$a' - a \in I, \qquad b' - b \in I.$$

De aquí:

$$a'b' - ab = a'b' - a'b + a'b - ab = a'(b' - b) + (a' - a)b.$$

Como ambas diferencias pertenecen a I resulta que los dos sumandos pertenecen a I. Pero para cualquier ideal I, si dos elementos del anillo pertenecen a él, también pertenece su suma; en efecto, pertenece el opuesto de uno de ellos, ya que es el producto de él por el -1 del anillo, y entonces pertenecerá la diferencia del otro elemento menos este opuesto, es decir, la suma de los dos dados. Resulta entonces que $a'b' - ab \in I$, o sea, $a'b' + I = ab + I$, luego el resultado de la multiplicación es independiente de los representantes elegidos en las clases factores.

Es inmediata la propiedad asociativa, y en cuanto al elemento unidad de A/I se comprueba fácilmente que es la clase $1 + I$, siendo 1 el elemento unidad de A. También es evidente la propiedad distributiva.

Al anillo A/I así definido le llamaremos *anillo de clases de restos* del anillo A respecto de su ideal I. Por comodidad representaremos algunas veces a la clase $a + I \in A/I$ por la notación más sencilla $\bar{a}$. Entonces se puede escribir, como es costumbre, la relación de cada elemento de A a su clase de restos correspondiente en la forma:

$$a \equiv \bar{a}(I).$$

Esta relación entre a y $\bar{a}$ es un homomorfismo entre A y A/I. En efecto, si a b corresponde $\bar{b} = b + I$, por la definición de las operaciones anteriores, al elemento $a + b$ corresponderá el $\bar{a} + \bar{b}$, y al ab el $\bar{a}\bar{b}$. A este homomorfismo, como hemos hecho ya en otro caso análogo, le llamaremos *homomorfismo natural* o *canónico*. El núcleo de este homomorfismo es precisamente el ideal I.

En todo anillo existen siempre dos ideales, que se llaman *impropios*, que son el elemento O y todo el anillo. El primero de ellos es un ideal principal engendrado por el cero y consta exclusivamente de este elemento; cuando se quiere expresar este ideal se denotará en la forma (0). Análogamente, el ideal principal engendrado por el elemento 1 consta de todos los elementos del anillo, luego $(1) = A$. Todo ideal que no sea impropio se dirá *ideal propio*. Cualquier ideal propio contiene al ideal (0) y está contenido en el (1).

Vamos a demostrar que un cuerpo K no tiene más ideales que los dos ideales impropios. En primer lugar observaremos que si un ideal contiene al elemento 1, el ideal coincide con todo el anillo, es decir, es el ideal (1); la comprobación puede hacerla sin trabajo el lector. Bastará entonces con que demostremos que cualquier ideal de un cuerpo, distinto del ideal (0), contiene al 1; entonces ese ideal coincidirá con el cuerpo K. En efecto, si $I \neq (0)$, existirá en I un elemento $a \neq 0$, luego el elemento $a^{-1} \in K$ y, por tanto, su producto por $a \in I$ será el elemento $aa^{-1} = 1 \in I$, como queríamos demostrar.

5. OPERACIONES CON IDEALES

Veamos algunas analogías entre los anillos en general y el anillo de los enteros. Dado un anillo A, existe en él un conjunto de ideales. Si entre dos de ellos, I, I', se verifica $I \subset I'$, se dice que I' divide a I, o que I es múltiplo de I'.

Esta terminología se emplea por analogía con lo que ocurre en el anillo Z. Pues sean, por ejemplo, $I = \{\dot{6}\}$, $I' = \{\dot{3}\}$. Se verifica $I \subset I'$ y además $3 \mid 6$. Es decir, decimos que el ideal $\{\dot{3}\}$ divide al $\{\dot{6}\}$.

Se llama *unión* o *suma:*

$$I \cup I' = I + I' = \{a + a' \mid a \in I,\ a' \in I'\}.$$

La intersección se define como en los conjuntos

$$I \cap I' = \{a \mid a \in I,\ a \in I'\}.$$

Si el anillo es Z, consideremos los ideales

$$I = \{\dot{a}\} \qquad \text{e} \qquad I' = \{\dot{b}\}.$$

Como ya se vió anteriormente, en este caso:

$$I + I' = \{ha + kb \mid h,\ k \in Z\} = \{\dot{\text{m. c. d. }}(a, b)\}.$$

$$I \cap I' = \{x \mid x = am,\ x = bn;\ m, n \in Z\} = \{\dot{\text{m. c. m. }}(a, b)\}.$$

Generalizando esta nomenclatura llamamos:

$$\text{m. c. d. } (I, I') = I \cup I' = I + I'.$$
$$\text{m. c. m. } (I, I') = I \cap I'.$$

Demostraremos ahora que tanto $I + I'$ como $I \cap I'$ son ideales, siendo $I + I'$ el mínimo ideal que contiene a I e I' simultáneamente. Asimismo, $I \cap I'$ es el máximo ideal contenido en I e I'.

a) $I + I'$. Sean

$$a + a',\ b + b' \in I + I',$$

siendo $\begin{cases} a,\ b \in I \Rightarrow a - b \in I \\ a',\ b' \in I' \Rightarrow a' - b' \in I'. \end{cases}$

Sumando:

$$(a + a') - (b + b') = \underset{(\in I)}{(a - b)} + \underset{(\in I')}{(a' - b')} \in I + I'.$$

Por otra parte,

$$c(a + a') = \underset{(\in I)}{ca} + \underset{(\in I')}{ca'} \in I + I',$$

para cualquier $c \in A$.

b) $I \cap I'$.

Sean:

$$a,\ b \in I \cap I' \Rightarrow \left\{ \begin{array}{l} a,\ b \in I \Rightarrow a - b \in I \\ a,\ b \in I' \Rightarrow a - b \in I' \end{array} \right\} \Rightarrow a - b \in I \cap I'.$$

Por otra parte:

$$ca \in I,\ ca \in I' \Rightarrow ca \in I \cap I'.$$

Además, $I + I'$ es un divisor de I y de I', mientras que $I \cap I'$ es múltiplo de ambos. En efecto, para ver que $I \subset I + I'$, observemos que todo ideal posee el elemento 0 del anillo; el ideal I', por ejemplo, posee el elemento 0, ya que si $a' \in I'$, como $0 \in A$, el producto

$$a' \cdot 0 = 0 \in I'.$$

Entonces todo elemento $a \in I$ se puede escribir en la forma $a + 0$, con $a \in I$, $0 \in I'$, luego $a = a + 0 \in I + I'$, lo que nos dice que $I \subset I + I'$, y lo mismo $I' \subset I + I'$.

La demostración de que $I \cap I' \subset I$, $I \cap I' \subset I'$ es inmediata, de acuerdo con la definición de intersección.

Queda por demostrar que $I + I'$ es el máximo divisor, es decir, que si J es un ideal tal que $I \subset J$, $I' \subset J$, entonces $I + I' \subset J$. En efecto, sea

$$a + a', \qquad a \in I, \qquad a' \in I'$$

un elemento de $I + I'$; entonces $a \in J$ y $a' \in J$, luego $a + a' \in J$.

Así, que todo ideal que divide a I e I', divide a $I + I'$, luego éste es el m. c. d.

Del mismo modo, si un ideal $L \subset I$, $L \subset I'$, también $L \subset I \cap I'$, como es inmediato, luego todo ideal múltiplo de I y de I' es múltiplo de $I \cap I'$, así que éste es el m. c. m. de I e I'.

Todo lo anterior nos indica que el conjunto de ideales de un anillo es ordenado (no totalmente), y para dos elementos cualesquiera I, I' existe:

$$\text{extr. sup. } (I,\ I') = I + I' = \text{m. c. d. } (I,\ I').$$
$$\text{extr. inf. } (I,\ I') = I \cap I' = \text{m. c. m. } (I,\ I'),$$

luego el conjunto de ideales de un anillo, incluyendo los impropios, es un retículo respecto las operaciones $+$, $\cap$.

El ideal A (anillo) es el universal del retículo, pues,

$$A + I = A; \qquad A \cap I = I.$$

El (0) es el ínfimo, pues:

$$(0) + I = I; \qquad (0) \cap I = (0),$$

es decir, hacen el papel de U y $\emptyset$ del retículo de partes de un conjunto.

6. IDEALES PRIMOS Y MAXIMOS

Un ideal I se llama *máximo* cuando no está contenido en ningún ideal propio, o sea, si I máximo e $I \subset J \Rightarrow J = A$.

Pueden existir varios ideales máximos en un anillo. Por ejemplo, en Z son máximos $\{\dot{5}\}$, $\{\dot{7}\}$, $\{\dot{13}\}$, ..., y en general los múltiplos de cuualquier número primo, ya que, en efecto, si a y b son dos enteros y $\{\dot{a}\}$, $\{\dot{b}\}$ los ideales que engendran, vimos que $\{\dot{a}\} \subset \{\dot{b}\}$ si $b \mid a$. Entonces, si a es primo, no hay ningún $b \neq 1$ que lo divide y, por tanto, el único ideal que contiene al $\{\dot{a}\}$ es el

$$\{\dot{1}\} = \{1 \cdot x \mid x \in Z\} = Z,$$

luego $\{\dot{a}\}$ es máximo.

No lo es $\{\dot{6}\}$, pues

$$\{\dot{6}\} \subset \{\dot{2}\}.$$

Veamos ahora cómo se traduce el concepto de número primo en los ideales. Un ideal I es *primo* cuando se cumple que si

$$ab \in I, \qquad a \notin I \Rightarrow b \in I.$$

Entre números enteros equivale a decir que son los engendrados por los números primos y su definición no es más que la generalización de la propiedad de que si un número primo divide a un producto de dos números enteros, divide a uno de los factores.

Por ejemplo, si

$$ab = \dot{3}, \quad \text{y} \quad 3 \text{ no divide a } a \Rightarrow 3 \mid b,$$

o sea, si

$$ab \in \{\dot{3}\}, \text{ a } \notin \{\dot{3}\} \Rightarrow b \in \{\dot{3}\}.$$

Esto no ocurre con números no primos; por ejemplo:

$$24 = 3 \cdot 8 \in \{\dot{6}\}, \qquad 3 \notin \{\dot{6}\}, \qquad 8 \notin \{\dot{6}\}.$$

Veremos dos teoremas importantes, aunque sin demostrar totalmente.

TEOREMA.—*Si el ideal* $P \subset A$ *es primo, entonces* A/P *es un dominio de integridad* (no tiene divisores de 0), *y recíprocamente.*

La clase $a + P$ la llamaremos $\bar{a} \in A/P$. En particular,

$$P = 0 + P = \bar{0}.$$

Para ver que A/P es dominio de integridad, hemos de ver que si

$$\overline{ab} = \bar{0},\ \bar{a} \neq \bar{0} \Rightarrow \bar{b} = \bar{0}.$$

Para ello recordemos el homomorfismo canónico $A \longrightarrow A/P$, donde el núcleo es P, es decir, que todo elemento de A que se represente en el $\bar{0} \in A/P$, pertenece a P. Luego si en dicho homomorfismo

$$a \longrightarrow \bar{a},\ b \longrightarrow \bar{b} \Rightarrow ab \longrightarrow \overline{ab},$$

y la expresión a demostrar se traduce en estos términos:

$$ab \in P,\ a \notin P \Rightarrow b \in P,$$

afirmación que es inmediata, dada la definición de ideal primo.

Y lo mismo se demuestra la proposición recíproca.

TEOREMA.—*Si el ideal* $\mathrm{I} \subset \mathrm{A}$ *es máximo, se verifica:* 1.º, I *es primo;* 2.º, A/I *es cuerpo.*

Advertimos que no todo I primo es máximo, aunque esto sí que ocurre en el anillo Z.

En lugar de la demostración, veremos un ejemplo tomado en el anillo Z.

En adelante representaremos por (a) el ideal principal engendrado por a; es decir, $(a) = \{\dot{a}\}$. Sea

$$I = (5) \Rightarrow A/I = \{\bar{0},\ \bar{1},\ \bar{2},\ \bar{3},\ \bar{4}\}.$$

Hacemos la tabla de multiplicar:

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

prescindiendo, por comodidad, del trazo encima de cada número.

Por encontrarse la unidad en cada fila y columna, todo elemento tiene un inverso, y por cumplirse las demás condiciones, el conjunto A/I forma un cuerpo.

Veamos como contraejemplo lo que ocurre tomando el ideal $I = (6)$, que no es máximo:

$$A/I = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$$

	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

Solamente los elementos 1, 5 tienen inverso, luego no es un cuerpo.

Notemos en este ejemplo que existen divisores de $\bar{0}$. Por ejemplo, $\bar{2} \times \bar{3} = \bar{3} \times \bar{4} = \bar{0}$, luego tampoco es dominio de integridad. Esto es consecuencia del teorema anterior, ya que el ideal (6) no es primo, pues hemos dicho anteriormente que en el anillo Z coinciden los conceptos ideal primo e ideal máximo.

En todo caso, una vez demostrado que A/I es un cuerpo, quedaría demostrado que I es primo. Bastaría, en efecto, de acuerdo con el teorema anterior, comprobar que A/I es dominio de integridad, y esto quedó visto en cuanto probamos, en el párrafo 2 de este capítulo, la siguiente proposición: *Todo cuerpo es dominio de integridad.*

7. DIVISIBILIDAD EN LOS ANILLOS

Dados dos elementos, $a, b \in A$, decimos que a es un *divisor* de b, y lo representamos así:

$$a \mid b,$$

si existe un elemento $c \in A$, tal que

$$a \cdot c = b.$$

Si representamos por (a) y (b) los ideales engendrados por a y b, respectivamente, se deberá verificar:

$$(b) \subset (a),$$

es decir, que ideal (a) es divisor del (b).

Se dice que dos elementos a y b de A son *asociados* si

$$b = au,$$

donde u es una unidad del anillo A.

Como si $u \in A$ también $u^{-1} \in A$, entonces esto implica que si

$$b = au, \qquad b \cdot u^{-1} = a,$$

o sea,

$$a \mid b \qquad b \mid a.$$

Esto en los ideales (a), (b) se refleja de la siguiente manera:

$$(a) \subset (b), \quad (b) \subset (a) \Rightarrow (a) = (b).$$

Si dos elementos son asociados, sus ideales coinciden.

Toda unidad es asociada con el 1, pues por una parte 1 divide a u, y por otra, como $uu^{-1} = 1$, también u divide a 1. Entonces,

$$(u) = A;$$

el ideal engendrado por una unidad coincide con el anillo total.

Un elemento del anillo se llama *irreducible* cuando sólo es divisible por las unidades y por sus asociados.

En el anillo Z los elementos irreducibles son los números primos. Ejemplo, el 3, sólo es divisible por 1, — 1, 3, — 3.

Todo elemento no irreducible de un anillo se puede escribir como producto de elementos irreducibles:

$$a = r_1 r_2 \ldots\ldots r_n.$$

A esto se llama una *factorización* de a.

Dos factorizaciones que difieran sólo en el orden de los factores o en que se han introducido unidades, se consideran la misma.

Según lo que antecede, podemos definir ahora lo que se entiende por anillos de factorización única.

8. ANILLOS DE FACTORIZACION UNICA

Diremos que A es un *anillo de factorización única* si:

1) Todo elemento de A puede descomponerse en un número finito de factores irreducibles.

2) Esta descomposición es única.

Son anillos de factorización única Z y el anillo $Z[x]$ de polinomios en una indeterminada con coeficientes que pertenecen al anillo Z de los enteros, o el $Q[x]$, con coeficientes en Q.

No todos los anillos (aunque sí los más usuales) son de factori-

zación única. Por ejemplo, consideremos el anillo formado por los elementos de la forma

$$a + b\sqrt{-3} \qquad \text{con} \qquad a, b \in Z.$$

Este anillo, como puede verse fácilmente, es el anillo de polinomios en las distintas potencias de $\sqrt{-3}$, y cuyos coeficientes pertenecen a Z. Lo representaremos por $Z[\sqrt{-3}]$.

Definiendo entre los elementos de $Z[\sqrt{-3}]$ una suma:

$$(a_1 + b_1\sqrt{-3}) + (a_2 + b_2\sqrt{-3}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{-3},$$

vemos que es una operación interna, puesto que $a_1 + a_2$ y $b_1 + b_2 \in Z$. Se ve que es asociativa. Tiene elemento neutro, el $(0 + 0\sqrt{-3})$ y elemento inverso, para cada $a + b\sqrt{-3}$, el $(-a - b\sqrt{-3})$.

Definimos el producto como en los binomios algebraicos:

$$(a_1 + b_1\sqrt{-3})(a_2 + b_2\sqrt{-3}) = (a_1a_2 - 3b_1b_2) + (a_1b_2 + b_1a_2)\sqrt{-3}.$$

Este producto tiene elemento unidad, el

$$1 + 0\sqrt{-3};$$

pero no existe elemento inverso y sí tiene la propiedad distributiva. Así, pues, $Z[\sqrt{-3}]$ es un anillo con elemento unidad.

Pues bien, este anillo no es de factorización única, pues, por ejemplo, el elemento $4 + 0\sqrt{-3}$ podemos descomponerlo así:

$$4 = 2 \times 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

Con este ejemplo vemos que la teoría de la divisibilidad, que estamos habituados a aplicar en los anillos Z y $Q[x]$, por ejemplo, no es generalizable a cualquier tipo de anillos.

9. ANILLOS EUCLIDEOS

Aquellos anillos en los que son aplicables las propiedades de la divisibilidad que conocemos para Z y $Q[x]$, y que, por consiguiente, son una generalización de estos anillos, se llaman anillos euclídeos.

Un *anillo euclídeo* A viene caracterizado por las siguientes propiedades:

1) A cada elemento $a \in A$ se le puede asignar un entero, no negativo, $g(a)$, tal que si

$$a \mid b \Rightarrow g(a) \leq g(b).$$

El signo $\leq$ expresa que, como en particular para $a = b$ también $b \mid a$, no se excluye que $g(a) = g(b)$.

2) Dados cualesquiera $a, b \in A$, se pueden encontrar dos números, q y r, también de A, tales que:

$$a = bq + r \qquad \text{con} \qquad g(r) < g(b).$$

Son anillos euclídeos, como ya hemos apuntado antes, el Z si hacemos:

$$g(a) = |a|.$$

También $Q[x]$ si hacemos

$$g(p) = \text{grado del polinomio } p.$$

TEOREMA.—*Todo ideal, I, de un anillo euclídeo es un ideal principal, esto es, todos los elementos que forman el ideal son múltiplos de un único elemento.*

Escojamos un $a \in I$ con la condición de que $g(a)$ sea mínimo (puede haber más de un $a \in I$ que verifique esto).

Demostraremos que si

$$b \in I \Rightarrow b = aq, \qquad q \in A.$$

Como $a, b \in A$, por la propiedad 2) de los anillos euclídeos, podemos escribir:

$$b = aq + r \qquad \text{con} \qquad g(r) < g(a). \qquad [4]$$

Por otra parte, $r = b - aq$, donde $a, b \in I$ y $q \in A$, y por tanto, $b - aq \in I$, es decir,

$$r \in I.$$

Pero entonces no puede cumplirse

$$g(r) < g(a),$$

por ser $g(a)$ mínimo. Esto es lo mismo que afirmar que no existe un r que verifique [4] y que, por tanto,

$$b = aq.$$

Si a y b son dos elementos asociados que pertenecen a un anillo euclídeo se verifica simultáneamente:

$$a \mid b \qquad \text{y} \qquad b \mid a,$$

sus enteros asignados $g(a)$ y $g(b)$, verifican también simultáneamente:

$$g(a) \leq g(b) \qquad \text{y} \qquad g(b) \leq g(a),$$

lo cual implica, por ser $\leq$ una relación de orden, que

$$g(a) = g(b).$$

En particular, como cualquier unidad del anillo es asociada del elemento 1:

$$g(u) = g(1).$$

Pero cualquier otro $a \in A$ que no sea unidad verifica:

$$g(a) > g(1).$$

TEOREMA.—*Todo anillo euclideo es de factorización única.*

La demostración, de acuerdo con las propiedades de los anillos de factorización única, debe comprender dos partes:

1) Todo $a \in A$ se puede descomponer en un número finito de factores irreducibles r_i:

$$a = r_1 r_2 \ldots\ldots r_m.$$

2) Esta descomposición es única.

Demostraremos tan sólo la primera parte.

Supongamos que la propiedad de la descomposición se cumple para cualesquiera $b \in A$, tales que $g(b) < n$ y veamos que entonces podemos demostrar que se cumple para $g(a) = n$.

En efecto, supuesto que a no es irreducible (si lo fuera no habría nada que demostrar), se podrá descomponer en producto de dos factores, r y s, tales que:

$$a = r \cdot s,$$

y que ni r ni s sean unidades; entonces:

$$r \mid a \qquad \text{y} \qquad s \mid a,$$

o sea,

$$g(r) \leq g(a), \qquad g(s) \leq g(a). \qquad [5]$$

Como ni r ni s son unidades, a no es asociado con r (porque s sería unidad en este caso), ni con s (porque lo sería r), y, por tanto, las relaciones [5] son desigualdades estrictas:

$$g(r) < g(a) = n.$$
$$g(s) < g(a) = n.$$

Pero entonces, por hipótesis, tanto r como s, admiten una descomposición en producto de un número finito de factores irreducibles:

$$r = p_1 p_2 \ldots\ldots p_k$$
$$s = q_1 q_2 \ldots\ldots q_h$$

y entonces

$$a = r \cdot s = p_1 p_2 \ldots\ldots p_k q_1 q_2 \ldots\ldots q_l.$$

La demostración de la unicidad de esta descomposición la omitimos, como hemos dicho.

En todo anillo euclídeo se puede, por tanto, definir, a partir de los conceptos expuestos, una teoría de la divisibilidad análoga a la estudiada en el anillo de los enteros.

En particular, se puede hallar por el algoritmo de EUCLIDES el máximo común divisor de dos elementos cualesquiera del anillo. Y lo mismo que en los enteros, se verifica que m. c. d. $(a, b) = a\alpha + b\beta$, α y β son dos elementos del anillo.

En efecto, el conjunto de elementos $I = \{am + bn \mid m, n \in A\}$ es un ideal, como puede comprobarse inmediatamente, y por tratarse A de un anillo euclídeo, ese ideal será un ideal principal:

$$I = \{(a\alpha + b\beta)c \mid c \in A\}.$$

Resulta, pues, que todo elemento de la forma $am + bn$ es múltiplo de $a\alpha + b\beta$, luego para $m = 1$, $n = 0$ y para $m = 0$, $n = 1$ se tiene, respectivamente:

$$(a\alpha + b\beta) \mid a, \qquad (a\alpha + b\beta) \mid b,$$

así que $a\alpha + b\beta$ es un divisor común de a y b. Si p es un divisor, también de a y b, se tendrá:

$$p \mid a,\ p \mid b \Rightarrow p \mid (a\alpha + b\beta);$$

luego $a\alpha + b\beta$ es el m. c. d. (a, b).

10. CUERPO DE COCIENTES DE UN ANILLO

Dado un anillo A conmutativo con unidad y que sea dominio de integridad, establezcamos en $A \times A$ la siguiente relación:

$$(a, b)R(c, d) \Leftrightarrow ad = bc.$$

Esta relación es de equivalencia, pues

1.º $(a, b)R(a, b)$, ya que $ab = ba$.

2.º $(a, b)R(c, d) \Leftrightarrow ad = bc \Leftrightarrow cb = da \Leftrightarrow (c, d)R(a, b)$.

3.º $\left.\begin{matrix}(a, b)R(c, d) \Leftrightarrow ad = bc \Leftrightarrow adf = bcf \\ (c, d)R(e, f) \Leftrightarrow cf = de \Leftrightarrow cfb = deb\end{matrix}\right\} \Rightarrow$

$\Rightarrow adf = deb \Rightarrow af = be \Leftrightarrow (a, b)R(e, f)$.

Notemos que hemos necesitado la hipótesis de ser A conmutativo para demostrar las tres propiedades de R.

Veamos ahora que el conjunto $(A \times A)/R$ es un cuerpo respecto las dos operaciones que vamos a definir:

$$\{(a, b)\} + \{(c. d)\} = \{(ad + bc, bd)\}.$$
$$\{(a, b)\} \cdot \{(c, d)\} = \{(ac, bd)\}.$$

En primer lugar, hemos de ver que estas definiciones tienen sentido, es decir, el resultado no depende de los representantes elegidos para hacer la operación. La haremos solamente con la suma.

Sean, pues,

$$(a', b')R(a, b) \qquad \text{y} \qquad (c', d')R(c, d)$$
$$\{(a', b')\} + \{(c', d')\} = \{(a'd' + b'c', b'd')\}.$$

Ahora bien,

$$(ad + bc, db)R(a'd' + b'c', b'd'),$$

ya que

$$(ad + bc)b'd' = bd(a'd' + b'c');$$

como es fácil ver, basándose en la hipótesis de ser:

$$a'b = b'a; \qquad c'd = d'c.$$

Para demostrar que $(A \times A)/R$ forma cuerpo, veamos que las operaciones antes definidas cumplen todas las condiciones exigidas.

En primer lugar, son operaciones internas, por ser $a, b, c, d \in A$.

Para demostrar la propiedad asociativa basta comparar los resultados de las operaciones:

$$[(a, b) + (c, d)] + (e, f) \qquad \text{y} \qquad (a, b) + [(c, d) + (e, f)]$$
$$[(a, b) \cdot (c, d)] \cdot (e, f) \qquad \text{y} \qquad (a, b) \cdot [(c, d) \cdot (e, f)]$$

Lo haremos con la suma, siendo el caso del producto totalmente análogo:

$$[(a, b) + (c, d)] + (e, f) = (ad + bc, bd) + (e, f) = (adf + bcf + bde, bdf).$$
$$(a, b) + [(c, d) + (e, f)] = (a, b) + (cf + de, df) = (adf + bcf + bde, bdf).$$

El elemento neutro para la suma es la clase $\{(0, a)\}$, pues tomando por ejemplo el representante $(0, 1)$, se verifica:

$$(0, 1) + (b, c) = (b, c)$$

para cualquier (b, c).

El elemento unidad para el producto es la clase $\{(a, a)\}$, pues tomando por ejemplo el representante $(1, 1)$, se verifica:

$$(1, 1) \cdot (b, c) = (b, c)$$

para cualquier (b, c).

El elemento simétrico del (a, b) es $(-a, b)$ en la suma y (b, a) en el producto, pues se cumple:

$$(a, b) + (-a, b) = (0, bb) \in \{(0, 1)\}.$$
$$(a, b) \cdot (b, a) = (ab, ba) \in \{(1, 1)\}.$$

La propiedad distributiva se demuestra comprobando la igualdad de resultados en las operaciones:

$$[(a, b) + (c, d)] \cdot (e, f) = (ad + bc, bd) \cdot (e, f) = (ade + bce, bdf)$$
$$(a, b) \cdot (e, f) + (c, d) \cdot (e, f) = (ae, bf) + (ce, df) = (aedf + bfce, bfdf)$$
$$\in \{(ade + bce, bdf)\}.$$

Queda, pues, visto que el conjunto de clases $(A \times A)/R$ forma un cuerpo, llamado *cuerpo de cocientes del anillo A*.

Si $A = Z$ en el proceso anterior, resulta el cuerpo de los números racionales. En él acostumbramos a utilizar la notación $(a, b) = a/b$.

Si $A = Z[x]$, entonces

$$(A \times A)/R = \left\{ \frac{a_0 + a_1 x + \ldots\ldots + a_m x^m}{b_0 + b_1 x + \ldots\ldots + b_n x^n} \right\} \quad a_i,\ b_i \in Z$$

y este cuerpo formado por todas las expresiones racionales en x se designa por $Z(x)$.

Análogamente se procede con anillos de más de una variable.

Esta formación del cuerpo $Z(x)$ se llama adjunción de x al anillo Z.

11. CUERPO DE LOS NUMEROS REALES

Estudiemos ahora otro procedimiento para formar cuerpos, basado en el teorema visto anteriormente, según el cual, dado un ideal máximo $I \subset A$, el conjunto A/I es un cuerpo. Lo haremos aplicándolo al ejemplo de la construcción del cuerpo real R.

Definimos una aplicación del semigrupo N en el cuerpo Q:

$$1 \longrightarrow q_1; \qquad 2 \longrightarrow q_2; \qquad \ldots\ldots; \qquad n \longrightarrow q_n; \qquad \ldots\ldots$$

Esto es sencillamente una sucesión de números racionales, como ya sabíamos. Designaremos dicha sucesión brevemente por q_n.

q_n es convergente cuando, dado un número cualquiera, $\varepsilon > 0$, se puede encontrar un número $n_0 \in N$, tal que para todo par:

$$n,\ n' > n_0 \Rightarrow |q_n - q_{n'}| < \varepsilon.$$

q_n tiene por límite q (y se expresa $\lim q_n = q$) cuando para cualquier $\varepsilon > 0$ existe un $n_0 \in N$, tal que para todo $n > n_0 \Rightarrow |q - q_n| < \varepsilon$.

Como ya sabemos, toda sucesión que tiene límite es convergente, pero no es cierta la recíproca. Por tanto, la operación (de carácter topológico) de paso a límite no es siempre posible, dentro del campo de los números racionales.

Nos encontramos, pues, con una situación análoga a la vista en los números naturales y enteros. Para hacer posible en N la operación de restar se creaban los números enteros Z, y para hacer entre éstos posible la división se introdujeron los números racionales Q. Y ahora, a partir de éstos, construiremos un nuevo cuerpo que haga siempre posible la operación de paso a límite.

Veamos, en primer lugar, que el conjunto de sucesiones convergentes en Q forman un anillo respecto a las siguientes operaciones:

Si

$$q_n = q_1, q_2, \ldots\ldots, q_n, \ldots\ldots,$$
$$q'_n = q'_1 q'_2, \ldots\ldots, q'_n, \ldots\ldots,$$
$$q_n + q'_n = q_1 + q'_1, q_2 + q'_2, \ldots\ldots, q_n + q'_n, \ldots\ldots$$
$$q_n \cdot q'_n = q_1 \cdot q'_1, q_2 \cdot q'_2, \ldots\ldots, q_n \cdot q'_n, \ldots\ldots$$

Estas operaciones son internas, pues como ya sabe el lector, las sucesiones que resultan también son convergentes.

El carácter asociativo y distributivo se deduce de los mismos caracteres entre los números racionales. Las sucesiones:

$$0 = 0, 0, \ldots\ldots, 0, \ldots\ldots$$
$$1 = 1, 1, \ldots\ldots, 1, \ldots\ldots$$

son elementos neutros respecto de la suma y el producto, respectivamente.

Dada la sucesión

$$q_n = q_1, q_2, \ldots\ldots, q_n, \ldots\ldots$$

su opuesta es la

$$-q_1, -q_2, \ldots\ldots, -q_n, \ldots\ldots$$

pues sumadas dan la

$$0, 0, \ldots\ldots, 0, \ldots\ldots$$

En cambio, si algún $q_i = 0$ en la sucesión q_n, ésta no tiene inverso, pues los términos

$$\frac{1}{q_1}, \quad \frac{1}{q_2}, \quad \ldots\ldots, \quad \frac{1}{q_i}, \quad \ldots\ldots, \quad \frac{1}{q_n}, \quad \ldots\ldots$$

no forman sucesión, ya que $\dfrac{1}{q_i} \notin Q$.

Llamaremos, pues, A al *anillo de las sucesiones convergentes*.

Consideremos en A el subconjunto I de todas las sucesiones cuyo límite es 0, llamadas también *sucesiones nulas*. Desde luego, $I \subset A$, pues se dijo anteriormente que toda sucesión que tiene límite es convergente.

El subconjunto I es un ideal de A, como consecuencia de las dos siguientes propiedades de las sucesiones nulas. Si

$$\lim q_n = 0, \quad \lim q'_n = 0 \to \lim (q_n - q'_n) = 0,$$

o sea, si

$$q_n \in I, \quad q'_n \in I \Rightarrow q_n - q'_n \in I.$$

Si r_n converge y $\lim q_n = 0 \to \lim r_n q_n = 0$,

o sea, si

$$r_n \in A, \quad q_n \in I \Rightarrow r_n q_n \in I.$$

Formemos las clases de restos A/I. Para demostrar que forman cuerpo en lugar de ver que I es ideal máximo, probemos que en A/I todo elemento tiene un inverso, y como ya sabíamos que A/I es anillo, quedará demostrado que es un cuerpo.

Sea la clase $q_n + I$. Busquemos $s_n + I$, tal que

$$(q_n + I)(s_n + I) \in \{(1 + I)\}.$$

Si en q_n ningún término es nulo, la s_n será:

$$\frac{1}{q_1}, \quad \frac{1}{q_2}, \quad \ldots\ldots, \quad \frac{1}{q_n}, \quad \ldots\ldots,$$

como es fácil comprobar.

Si en q_n existen términos nulos, bastará con probar que podemos encontrar en la clase $q_n + I$ un representante que no tenga ningún término nulo. Sea, por ejemplo, para fijar ideas,

$$q_n = q_1, q_2, 0, 0, \ldots\ldots, 0, \ldots\ldots, q_n, \ldots\ldots$$

Elegimos un elemento de I, por ejemplo:

$$1, \quad \frac{1}{2}, \quad \frac{1}{3}, \quad \ldots\ldots, \quad \frac{1}{n}, \quad \ldots\ldots, \to 0,$$

que no tenga ningún término nulo. Si en esta sucesión cambiamos por 0 los términos correspondientes a los no nulos en la q_n, sigue siendo sucesión nula: 0, 0, 1/3, 1/4, ... Sumando esta sucesión que pertenece a I con la dada q_n obtenemos una sucesión sin ceros y de la clase de q_n, que en este caso tendrá la forma:

$$q_1, \quad q_2, \quad \frac{1}{3}, \quad \frac{1}{4}, \quad \ldots\ldots$$

Ahora estamos ya en el primer caso y podemos encontrar la clase inversa de la dada.

El conjunto $A/I = R$ es, pues, un cuerpo. Es llamado *cuerpo de los números reales*. Por tanto, un número real es una clase de sucesiones.

Llegados a este punto hagamos un esquema para comparar la introducción en la Matemática de los dos cuerpos tan importantes de números como son Q y R.

Racionales

En Z la división es posible en algunos casos:

$$\frac{a}{b} = c \in Z.$$

Cuando a no es múltiplo de b creamos un nuevo tipo de número y llamamos número al par a/b.

Pero en el caso de división posible existen otros pares:

$$\frac{m}{n} = c, \quad \ldots\ldots$$

a/b, m/n tienen de común que

$$an = bm, \quad \ldots\ldots$$

Generalizando esto a todos los casos establecemos la equivalencia:

$$\frac{a}{b} \backsim \frac{c}{d} \quad \text{si} \quad ad = bc,$$

y llamamos *número racional* al conjunto

$$\left\{ \frac{a}{b}, \quad \frac{c}{d}, \quad \ldots\ldots \right\}$$

de pares equivalentes.

Reales

En las sucesiones convergentes de números racionales el paso al límite es posible en algunos casos: $\lim q_n = q \in Q$.

Cuando la sucesión convergente q_n no tiene límite, creamos un nuevo tipo de número y llamamos número a la sucesión q_n.

Pero en el caso de existencia de límite, existen otras sucesiones:

$$q'_n \longrightarrow q, \quad \ldots\ldots$$

q_n, q'_n tienen de común que

$$\lim (q_n - q'_n) = 0, \quad \ldots\ldots$$

Generalizando esto a todos los casos establecemos la equivalencia:

$$q_n \backsim q'_n \quad \text{si} \quad \lim (q_n - q'_n) = 0,$$

y llamamos *número real* al conjunto

$$\{q_n, \ q'_n, \ \ldots\}$$

de sucesiones equivalentes.

12. CUERPO DE LOS NUMEROS COMPLEJOS

Consideremos el anillo de polinomios en una indeterminada x con coeficientes sobre el cuerpo de los números reales:

$$R[x].$$

Sea I un ideal principal de este anillo, formado por todos los polinomios que son múltiplos de $x^2 + 1$:

$$I = \{(x^2 + 1)P \mid P \in R[x]\}.$$

Tomemos las clases de restos de este anillo $R[x]$ respecto del ideal I. Estas clases de restos $R[x]/I$ se forman de un modo completamente análogo a como se hace con el anillo Z de los enteros, es decir, cada clase está representada por el resto de la división de cualquier polinomio $P \in R[x]$ por $x^2 + 1$. Como el resto ha de ser de grado menor que el divisor, será, a lo más, de grado 1.

Queda asi, pues, establecido en el anillo $R[x]$ el homomorfismo canónico:

$$R[x] \longrightarrow R[x]/I.$$

La correspondencia establecida por este homomorfismo la podemos representar esquemáticamente para cada $P \in R[x]$:

$$P \longrightarrow (ax + b) + I.$$

Veamos ahora que el conjunto de estos restos $\{ax + b\}$ equivale al conjunto de los números complejos.

En efecto, dados P y $P' \in R[x]$, siendo

$$P' \longrightarrow (cx + d) + I,$$

definimos la correspondencia de suma y producto que existe entre los elementos de $R[x]$ y sus imágenes en $R[x]/I$, correspondencia de operaciones que existe por tratarse de un homomorfismo:

$$\begin{aligned} P + P' &\longrightarrow [(a + c)x + (b + d)] + I. \\ PP' &\longrightarrow [acx^2 + (ad + bc)x + bd)] + I. \end{aligned} \qquad |6|$$

Como el polinomio producto de restos que aparece en |6| es de grado 2, podemos hallar un representante de grado 1 sin más que dividirlo por $x^2 + 1$. Resulta en definitiva:

$$PP' \longrightarrow [(ad + bc)x + (bd - ac)] + I.$$

Podemos advertir, sin pasar más adelante que las operaciones suma y producto, así definidas en las clases de restos, son los mismas

que se efectúan con los números complejos, que manejamos habitualmente.

Para simplificar la notación de las clases de restos vamos a representar sencillamente la clase correspondiente al polinomio x por la letra i:

$$x \longrightarrow x + I = i.$$

Entonces, a la clase correspondiente al polinomio $x^2 + 1$, que es la clase $0 + I = (x^2 + 1) + I$, lo representaremos por $i^2 + 1$. Pero como $x^2 + 1$ pertenece al núcleo del homomorfismo canónico, su imagen es la clase cero (el resto de la división de $x^2 + 1$ por $x^2 + 1$ es, en efecto, nulo), y entonces expresamos esta condición mediante esta igualdad fundamental:

$$i^2 + 1 = 0.$$

Supuesto, por tanto, que tenemos los polinomios P, P', ... $\in R[x]$, representemos sus clases respectivas ahora:

$$P \longrightarrow ai + b.$$
$$P' \longrightarrow ci + d.$$

Entonces, a

$$P + P' \longrightarrow (a + c)i + (b + d)$$

y a

$$PP' \longrightarrow (ad + bc)i + (bd - ac),$$

donde

$$a,\ b,\ c,\ d,\ \ldots \in R.$$

Concluimos, en definitiva, que cada clase de $R[x]/I$ se puede representar por un binomio en la variable I, con la condición $i^2 + 1 = 0$, y cuyas reglas de suma y multiplicación sean las antedichas.

El conjunto de estas clases de restos tiene ya estructura de anillo, como cualquier otra clase de restos respecto de un ideal del anillo. Para ver que es además un cuerpo, demostraremos que cada elemento tiene inverso.

En efecto, dado un elemento del anillo

$$ai + b \neq 0i + 0 \Rightarrow a^2 + b^2 \neq 0,$$

si construyo el elemento

$$\frac{-ai}{a^2 + b^2} + \frac{b}{a^2 + b^2},$$

que también es un número complejo por ser $a, b \in R$, aplicando la regla del producto se sigue:

$$(ai + b)\left[\frac{-ai}{a^2 + b^2} + \frac{b}{a^2 + b^2}\right] = 1.$$

Como esta demostración es completamente general, de aquí se sigue que todo número complejo tiene inverso. Por consiguiente, el conjunto de los números complejos es un cuerpo, el cuerpo C:

$$C = R[x]/I.$$

13. HOMOMORFISMOS Y AUTOMORFISMOS EN EL CUERPO COMPLEJO

El cuerpo R está contenido en el C: R es un subcuerpo de C. Asimismo, Q está contenido en R y, por la propiedad transitiva de la inclusión, en C y es también un subcuerpo de C.

Todas las nociones de homomorfismo, isomorfismo y automorfismo son perfectamente aplicables a los cuerpos.

En particular, existe en C un automorfismo muy interesante: el que hace corresponder a cada número complejo su conjugado

$$a + bi \longrightarrow a - bi.$$

Veamos que se trata, en efecto, de un automorfismo, para lo cual es preciso demostrar que se conservan las operaciones de suma y producto:

$$a + bi \longrightarrow a - bi.$$
$$c + di \longrightarrow c - di.$$

A $(a + c) + (b + d)i$ debe corresponderle $(a + c) - (b + d)i$ y esta última expresión puede descomponerse:

$$(a - bi) + (c - di),$$

que coincide con la expresión suma de conjugados.

De igual modo puede verse que conserva el producto.

Hasta aquí hemos demostrado que se trata de un homomorfismo; si ahora demostramos que el núcleo del homomorfismo sólo consta del elemento cero, quedará demostrado que es automorfismo.

La imagen de dicho núcleo es, desde luego, $0 - 0i$ y su original sólo puede ser (por definición de "conjugación") el $0 + 0i = 0$, luego se trata de un automorfismo.

14. NUMEROS ALGEBRAICOS Y TRASCENDENTES

Volviendo ahora sobre el homomorfismo del anillo $R[x]$ sobre el cuerpo C, podemos expresarlo también de esta otra forma:

$$P(x) \longrightarrow P(i),$$

con la condición $i^2 = -1$; de manera que $P(i)$ es siempre un binomio de la forma $ai + b$ con $a, b \in R$.

El núcleo de este homomorfismo es el ideal:

$$N = \{P(x)\ (x^2 + 1)\},$$

ya que sus imágenes, por ser $x^2 + 1 \longrightarrow 0$,

$$P(i)\ (i^2 + 1) = 0.$$

En todos estos pasos hemos sustituído la x por i. Vemos, por tanto, que el cuerpo C puede considerarse como engendrado por el conjunto de polinomios $R[i]$ con la condición de que $i^2 = -1$.

La i es un "número", tal que si sustituímos $P(x)$ por $P(i)$, lo que era un anillo es ahora ya un cuerpo y el núcleo del homomorfismo es el conjunto

$$\{P(x)\ (x^2 + 1)\} \in R[x].$$

Pero, entonces, i verifica la ecuación $x^2 + 1 = 0$, o cualquier otra de la forma $P(x)\ (x^2 + 1) = 0$, con coeficientes reales. Esto se expresa diciendo que i es un número algebraico sobre R.

En general, dado un cuerpo K, se dice que α es algebraico sobre K si en el homomorfismo

$$K[x] \longrightarrow K[\alpha]$$

el núcleo es distinto de cero. Ello equivale a afirmar que α verifica una ecuación en x con coeficientes de K.

La equivalencia es inmediata de demostrar. En efecto, decir que

$$a_0 + a_1 x + a_2 x^2 + \ldots\ldots + a_n x^n \in N$$

es lo mismo que afirmar que su imagen por el homomorfismo (que consiste en sustituir las x por las α) es el elemento cero, o sea, que

$$a_0 + a_1 \alpha + a_2 \alpha^2 + \ldots\ldots + a_n \alpha^n = 0.$$

Si esto no ocurre, es decir, que se trata de un isomorfismo, y, por tanto, el núcleo coincide con el polinomio 0, α no sería solución de

ninguna ecuación con coeficientes en K, y se dice entonces que α es *trascendente* sobre K.

Ejemplo.—El cuerpo Q es un subcuerpo de R y, por tanto, hay elementos que pertenecen a Q, pero no todos los elementos de R (los irracionales) pertenecen a Q.

Pues bien, dado $\alpha \in R$, siendo α irracional, decimos que es *irracional algebraico* cuando satisface una ecuación con coeficientes en Q. $\sqrt{2}$ es un irracional algebraico, pues es raíz de la ecuación

$$x^2 - 2 = 0, \qquad 1, 2 \in Q.$$

Y si, dado $\beta \in R$, β no satisface ninguna ecuación con coeficientes en Q, diremos que β es *irracional trascendente* sobre Q. Tal es el caso de los célebres números π y e, lo que dentro de las ideas anteriormente expuestas, equivale a afirmar que el homomorfismo

$$a_0 + a_1 x + \ldots\ldots + a_n x^n \longrightarrow a_0 + a_1 \pi + \ldots\ldots + a_n \pi^n$$

es un isomorfismo.

15. GRADO DE UN NUMERO ALGEBRAICO

Dado un número algebraico α sobre un cuerpo K, se llama grado de α al menor de los grados de todos los polinomios de $K[x]$, de los que α sea una raíz.

El concepto de grado algebraico incide con el problema clásico de los números construibles con regla y compás. Dado el cuerpo Q de números racionales y una unidad de segmentos, con la regla y el compás se pueden construir segmentos cuya longitud sea un número racional cualquiera. Esto se expresa diciendo que el cuerpo Q es un *cuerpo construible*.

Todo irracional algebraico de grado 2 sobre Q, como $\sqrt{2}$ por ejemplo, es también construible con regla y compás, lo que, como sabemos, es un ejercicio elemental. Y no solamente él, sino todo elemento de $Q(\sqrt{2})$ se puede también construir. El proceso es general, esto es: haciendo la adjunción de un elemento algebraico de grado 2 a un cuerpo construible se obtiene otro cuerpo también construible. Así podíamos formar una cadena de cuerpos obtenidos cada uno al hacer la adjunción al anterior de un irracional algebraico de grado 2, y como el cuerpo Q de partida es construible, lo son todos los demás cuerpos. Para que un número irracional cualquiera sea, pues, construible con regla y compás será necesario que pertenezca a alguno de los cuerpos construibles, tal como los hemos definido.

Ya desde la geometría griega se plantearon algunos problemas, que han dado en llamarse los problemas clásicos de esa geometría: la trisección del ángulo, la duplicación del cubo, la construcción del eptágono regular y la cuadratura del círculo. En todos ellos se trataba de obtener esos resultados sin más ayuda que la regla y el compás. Conviene insistir en que los mismos griegos los habían re-

suelto ya por otros métodos, pero lo que realmente interesaba a aquella geometría era la resolución con regla y compás.

Pues bien, los tres primeros problemas desembocan, en su resolución de tipo analítico, en sendas ecuaciones de tercer grado, con coeficientes racionales. Esto es, se trataría de construir un elemento algebraico de grado 3, no reducible a ninguno de grado 2, es decir, no perteneciente a ningún cuerpo construible. En consecuencia, los tres primeros problemas no son resolubles con regla y compás, aunque sí, por ejemplo, con ayuda de cúbicas o curvas de tercer grado.

Mayor dificultad supone el problema de la cuadratura del círculo o su equivalente de construir con regla y compás el número π. Es un problema en general dificultoso, y en ocasiones prácticamente imposible, decidir si un número irracional es algebraico o trascendente. Hasta el siglo pasado no se consiguió demostrar que π era trascendente, por lo que sin saber si no es algebraico, menos aún se podía asegurar que no era construible. El problema, pues, estaba pendiente de resolución. Con la demostración de la trascendencia de π, queda resuelto totalmente: el problema de la cuadratura del círculo no puede realizarse exclusivamente con la regla y el compás.

16. ESPACIOS VECTORIALES

La operación de multiplicar los números complejos por los números reales es la aplicación $C \times R \longrightarrow C$, que es una ley de composición externa, donde R es el dominio de operadores. La operación es:

$$(a + bi)c = ac + bci.$$

Esta operación goza de las siguientes propiedades:

1.ª Distributiva respecto de C:

$$[(a + bi) + (a' + b'i)]c = (a + bi)c + (a' + b'i)c.$$

2.ª Distributiva respecto de R:

$$(a + bi)(c + c') = (a + bi)c + (a + bi)c'.$$

3.ª $cc'(a + bi) = c[c'(a + bi)]$.

4.ª $1 \cdot (a + bi) = a + bi$.

Por ser C grupo aditivo y tener esta operación que goza de las cuatro propiedades anteriores, el conjunto C es llamado espacio vectorial sobre el cuerpo R. También se dice que R es el dominio de operadores o multiplicadores de ese espacio vectorial.

Notemos que en todo lo anterior solamente interviene la parte aditiva de los números complejos. Solamente los consideramos como grupo aditivo.

Generalicemos ahora el concepto de espacio vectorial.

El conjunto V es un *espacio vectorial* sobre el cuerpo K cuando se verifica:

1.º V es grupo aditivo.

2.º Existe en V una ley de composición externa, siendo K el dominio de operadores, que cumple las condiciones:

a) $a(\mathbf{v} + \mathbf{v}') = a\mathbf{v} + a\mathbf{v}'$ $\quad a \in K; \quad \mathbf{v}, \mathbf{v}' \in V.$

b) $(a + b)\mathbf{v} \quad a\mathbf{v} + b\mathbf{v}$ $\quad b \in K.$

c) $ab(\mathbf{v}) = a(b\mathbf{v})$

d) $1 \cdot \mathbf{v} = \mathbf{v}$ $\quad$ 1 unidad de K.

Hemos visto ya que C es un espacio vectorial sobre R.

El ejemplo más común y que ha dado el nombre a esta estructura es el conjunto de vectores libres con las operaciones suma de vectores y producto de un vector por un número real ya conocidas.

Otro ejemplo es el conjunto de pares de números reales (a, b), definiendo:

$$(a, b) + (c, d) = (a + c, b + d).$$
$$c(a, b) \quad (ca, cb).$$

Igual sucedería tomando en lugar de pares el conjunto de n-tuplas $(a_1, \ldots, a_n)$ con definiciones análogas de las operaciones.

El subconjunto $W \subset V$ se llama *subespacio vectorial* o *variedad lineal*, cuando es un espacio vectorial respecto de las mismas operaciones que tiene V.

Por ejemplo: Recta vectorial $\subset$ plano vectorial $\subset$ espacio vectorial.

Veamos un criterio de suficiencia para ser W subespacio vectorial.

1.º Para ser W subgrupo basta la condición:

Si $\mathbf{v}, \mathbf{v}' \in W \Rightarrow \mathbf{v} - \mathbf{v}' \in W$.

2.º Para la condición de la operación externa es suficiente que si

$$\mathbf{v} \in W, \ a \in K \Rightarrow a\mathbf{v} \in W.$$

Luego en consecuencia, si

$$\mathbf{v}, \mathbf{v}' \in W, \ a \in K \Rightarrow \mathbf{v} - \mathbf{v}' \in W, \ a\mathbf{v} \in W,$$

entonces W es subespacio vectorial de V, y esta condición es necesaria y suficiente.

17. HOMOMORFISMOS E ISOMORFISMOS

Dados dos espacios vectoriales, V, V' sobre un mismo cuerpo K, se llama homomorfismo de V en V' una aplicación $V \xrightarrow{h} V'$ que verifique:

Si

$$\left.\begin{array}{l}\mathbf{v} \longrightarrow \mathbf{v}' \\ \mathbf{w} \longrightarrow \mathbf{w}'\end{array}\right\} \Rightarrow \begin{array}{l}\mathbf{v} + \mathbf{w} \longrightarrow \mathbf{v}' + \mathbf{w}' \\ a\mathbf{v} \longrightarrow a\mathbf{v}'\end{array}$$

o bien $\left\{\begin{array}{l} h(\mathbf{v} + \mathbf{w}) = h(\mathbf{v}) + h(\mathbf{w}) \\ h(a\mathbf{v}) = a \cdot h(\mathbf{v}).\end{array}\right.$

El núcleo del homomorfismo $N \subset V$ es el conjunto de vectores de V que se representan en el vector $\mathbf{0}'$ de V'.

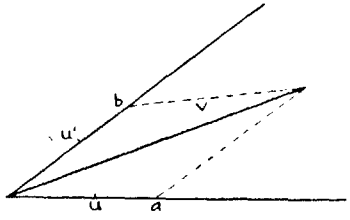
Es fácil ver que N es un subespacio vectorial. En efecto, aplicando el criterio anterior, tenemos:

$$\mathbf{v},\ \mathbf{v}' \in N \Leftrightarrow h(\mathbf{v}) = h(\mathbf{v}') = \mathbf{0}' \Rightarrow h(\mathbf{v} - \mathbf{v}') = \mathbf{0}' \Rightarrow \mathbf{v} - \mathbf{v}' \in N.$$
$$\mathbf{v} \in N \Leftrightarrow h(\mathbf{v}) = \mathbf{0}' \Rightarrow ah(\mathbf{v}) = h(a\mathbf{v}) = \mathbf{0}' \Rightarrow a\mathbf{v} \in N.$$

Análogamente a las anteriores estructuras se dirá: $h : V \longrightarrow V'$ isomorfismo cuando $N = \{\mathbf{0} \in V\}$.

Cuando dos estructuras algebraicas son isomorfas, son matemáticamente equivalentes, pudiéndose estudiar las propiedades que se deducen de las operaciones que definen la estructura indistintamente en cualquiera de las dos estructuras. En general, se elegirá la más cómoda.

En el caso del espacio vectorial V, formado por los vectores libres del plano, si elegimos en el mismo un par de ejes con sus respectivas unidades y hacemos corresponder a cada vector el par de números que son sus componentes, obtenemos un isomorfismo entre el espacio vectorial V y el espacio vectorial de pares de números a que antes nos hemos referido.



Este segundo espacio es, en general, más cómodo para operar que el V.

Por otra parte, también existe un isomorfismo entre el espacio vectorial de los complejos C y el de los pares de números reales, definido por la correspondencia:

$$a + bi \longrightarrow (a,\ b).$$

Pues si

$$c + di \longrightarrow (c,\ d),$$

se sigue:

$$(a + bi) + (c + di) \longrightarrow (a,\ b) + (c,\ d),$$

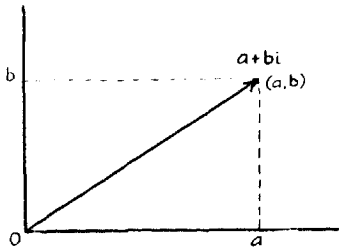
ya que

$$(a + c) + (b + d)i \longrightarrow (a + c,\ b + d);$$

y

$$(a + bi)c = (ac + bci) \longrightarrow (a,\ b)c = (ac,\ bc),$$

resultando como consecuencia de lo anterior que son isomorfos los espacios vectoriales V y C. Esto nos permite representar los números complejos mediante vectores en la forma acostumbrada en los tratados elementales de Matemáticas.



Por eso, en la representación gráfica, a la suma de complejos corresponde la suma de vectores, e igualmente al producto de un número real por un complejo corresponde el producto de dicho número real por el vector correspondiente. Pero lo que no puede decirse es que al producto de complejos corresponda el producto de vectores, pues no olvidemos que el isomorfismo establecido entre ambos conjuntos no afecta a la operación interna del producto que no se considera en la estructura de espacio vectorial. En consecuencia, solamente se podrá hablar del vector que corresponde al complejo producto, pero no del vector producto.

Conviene insistir en la incorrección de algunos textos, que al tratar de este tema hablan del producto y cociente de vectores, cuando en realidad se están refiriendo al producto y cociente de complejos. Los complejos sólo se "parecen" a los vectores, o, dicho con precisión, sólo son isomorfos a los vectores, en cuanto haga referencia a su suma y al producto por números reales. La otra operación interna de producto entre complejos no tiene correspondencia con una operación análoga entre vectores, ya que en los espacios vectoriales no se define esta operación.

Hemos visto que el conjunto de números complejos C tiene dos operaciones internas, respecto las cuales es cuerpo, y una externa,

siendo el dominio de operadores un cuerpo R. Además, C es un espacio vectorial respecto de la operación externa y la suma. Pues todo conjunto que como el C cumple estas condiciones se llama un *álgebra*.

Otro ejemplo notable es el conjunto de matrices cuadradas de un orden dado.

18. BASE Y DIMENSION

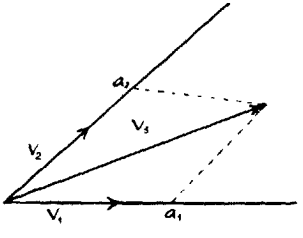
Dado un espacio vectorial V se dice que un conjunto $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$ es un sistema de *generadores* de V cuando dado cualquier $\mathbf{w} \in V$ existen elementos $a_1, \ldots, a_n \in K$ tales que $a_1\mathbf{v}_1 + \ldots + a_n\mathbf{v}_n = \mathbf{w}$. Por ejemplo, en el plano vectorial forma sistema de generadores el conjunto de dos vectores en distinta dirección.

Los elementos $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$ son *linealmente dependientes* cuando existen elementos $a_1, \ldots, a_n \in K$, no todos nulos, tales que

$$a_1\mathbf{v}_1 + \ldots + a_n\mathbf{v}_n = \mathbf{0}.$$

Por ejemplo, en el plano los tres vectores $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ del dibujo cumplen:

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 - 1 \cdot \mathbf{v}_3 = \mathbf{0}.$$



Un conjunto $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$ son *linealmente independientes* cuando no son dependientes, es decir, cuando siempre que se verifique

$$a_1\mathbf{v}_1 + \ldots\ldots + a_n\mathbf{v}_n = \mathbf{0}$$

sean forzosamente:

$$a_1 = \ldots\ldots = a_n = \mathbf{0}.$$

Por ejemplo, en el plano los dos vectores $\mathbf{v}_1, \mathbf{v}_2$, de distinta dirección, son linealmente independientes. En efecto, sea

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 = \mathbf{0}.$$

Si establecemos un isomorfismo entre V y los pares de componentes respecto a $\mathbf{v}_1$, $\mathbf{v}_2$, vemos que:

$$\mathbf{v}_1 \longrightarrow (1, 0).$$
$$\mathbf{v}_2 \longrightarrow (0, 1).$$

Por tanto,

$$a_1\mathbf{v}_1 \longrightarrow a_1(1, 0) = (a_1, 0).$$
$$a_2\mathbf{v}_2 \longrightarrow a_2(0, 1) = (0, a_2).$$
$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 \longrightarrow (a_1, 0) + (0, a_2) = (a_1, a_2);$$

y por ser

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 = \mathbf{o} \longrightarrow (0, 0)$$
$$\Longrightarrow (a_1, a_2) = (0, 0) \Rightarrow a_1 = a_2 = 0.$$

Base de un espacio vectorial V es un conjunto de vectores de V, $\mathbf{v}_1, \ldots, \mathbf{v}_n$ que sean linealmente independientes y a la vez sistema de generadores de V.

Por ejemplo, en el plano un par de vectores de distinta dirección.

Daremos un teorema sin demostración: *Todas las bases de un espacio vectorial* V *tienen el mismo número de elementos.* Dicho número se llama *dimensión* de V.

Sea el espacio vectorial de tres dimensiones: Si $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ es una base del mismo y elegimos $\{\mathbf{v}_1, \mathbf{v}_2\}$, lo que éstos engendran mediante combinaciones lineales es un plano vectorial o espacio vectorial de dimensión 2. Igualmente el $\mathbf{v}_1$ engendra una recta vectorial o espacio de dimensión 1. Representando por $(\mathbf{v}_1, \ldots, \mathbf{v}_n)$ el espacio vectorial engendrado por los vectores $\mathbf{v}_1, \ldots, \mathbf{v}_n$, tenemos en el caso anterior la siguiente escala de contenidos:

$$(\mathbf{v}_1) \subset (\mathbf{v}_1, \mathbf{v}_2) \subset (\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3).$$

Si definimos la unión e intersección entre variedades lineales, como ya se hizo al hablar de los retículos, es decir, la unión de dos variedades lineales es el conjunto de todas las rectas definidas por cada dos puntos, uno de cada variedad, y la intersección de dos variedades, es el conjunto de puntos que pertenecen a ambas, se ve que el conjunto de variedades lineales de un espacio vectorial es un retículo, llamado de las variedades lineales del espacio.

Notemos que la unión $\cup$ e intersección $\cap$ entre variedades equivalen a las dos operaciones fundamentales de la Geometría proyectiva, proyectar y cortar. Luego la Geometría proyectiva puede considerarse como el estudio del retículo de las variedades lineales del espacio.

Los espacios vectoriales pueden considerarse los espacios básicos,

sobre los que construir después el estudio de los espacios afines, proyectivos, métricos...

Cuando en un espacio se introduce la noción de distancia se convierte en un *espacio métrico*.

En un espacio vectorial u originado a partir de él, este concepto puede ser introducido mediante el producto escalar de vectores. Dados los puntos A, B del espacio, llamando $\mathbf{v}$ el vector de origen A y extremo B se define:

$$\text{dist. } (A, B) = \sqrt{\mathbf{v} \cdot \mathbf{v}}.$$

Esta es la llamada métrica euclídea, que transforma el espacio en un *espacio euclídeo*.

EJERCICIOS

1. Estudiar el anillo de restos $Z/(6)$ indicando si tiene o no divisores de cero, unidades y elementos asociados.

2. Idem id. con el anillo $Z/(5)$. Compárese con el anterior.

3. Demostrar que las unidades de un anillo forman grupo abeliano multiplicativo.

4. Demostrar que si dos elementos de un anillo verifican:

$$a \mid b \qquad y \qquad b \mid a,$$

a y b son asociados.

5. Demostrar que en el anillo de los enteros las expresiones

$$ma + nb,$$

donde a, b son fijos y m, n variables, forman un ideal.

6. Dados a y $b \in Z$ y un número d tal que:

$$d = \alpha a + \beta b,$$

y tal que $g(d)$ sea mínimo, demostrar que d divide simultáneamente a a y a b.

Sugerencia.—Si no fuese $d \mid a$ se tendría:

$$a = dc + r, \qquad g(r) < g(d),$$

y como

$$r = a - dc = a(1 - \alpha c) - \beta cb,$$

resultará que por ser r combinación lineal de a y b y ser $g(d)$ mínimo para estas combinaciones,

$$g(d) \leq g(r),$$

en contradicción con lo anterior. Luego

$$r = 0 \Rightarrow a = dc.$$

7. Demostrar, basándose en el resultado anterior y en forma distinta a como se ha hecho en la teoria, que d así construído es el máximo común divisor de a y b.

8. Aplicando el algoritmo de Euclides, hallar la forma lineal (ver problema 6) que nos da el m. c. d. de 120 y 32. Generalizar el resultado.

9. En el conjunto $Z \times Z$ definimos dos leyes internas: si

$$z = (a, b) \qquad \text{y} \qquad z' = (a', b')$$
$$z + z' = (a + a', b + b')$$
$$zz' = (aa' - bb', ab' + ba'),$$

y llamamos «norma» de z:

$$N(z) = a^2 + b^2.$$

Demostrar que

$$N(zz') = N(z) \cdot N(z).$$

10. En el anillo de polinomios $R[X]$, demostrar que el núcleo del homomorfismo $P(X) \longrightarrow P(z)$ es un ideal.

11. ¿Cuál es el núcleo del homomorfismo definido por la aplicación «derivada» sobre el grupo aditivo de los polinomios en una indeterminada X?

12. ¿Cuál es el núcleo del homomorfismo $P(x) \longrightarrow P(z)$? Dar una interpretación gráfica para $P(x)$ de primero y segundo grados.

13. Consideremos los pares de números racionales ordenados (a, b) que representaremos por $z = (a, b)$, con las siguientes leyes:

$$\alpha + \alpha = (a + a', b + b')$$
$$\alpha z' = (aa' + 2bb', ab' + ba').$$

Demostrar que forman cuerpo.

14. Demostrar que el conjunto de los complejos cuyo mod. = 1 forman grupo multiplicativo.

15. Demostrar, observando que $z \longrightarrow \bar{z}$ es un automorfismo, que las raíces complejas de una ecuación polinómica con coeficientes reales, aparecen a pares, es decir, cada una con su conjugada.

16. Demostrar que el conjunto de todas las funciones $\{f(x)\}$ definidas en un punto $x = a$ forman un espacio vectorial sobre el cuerpo de los números reales.

17. Las funciones derivables en $x = a$ constituyen un subespacio vectorial del anterior.

18. Un homomorfismo entre dos espacios vectoriales se llama también un *operador lineal*. Demostrar que la operación *derivada* es un operador lineal definido en el espacio vectorial del ejercicio 17.

IV. NOCIONES DE TOPOLOGIA

1. INTRODUCCION

La idea directriz que presidió la génesis de los espacios topológicos fué la de encontrar un espacio, generalización natural de todos los espacios conocidos o imaginables. Para ello era preciso ante todo discriminar cuáles eran las nociones básicas que convienen a todo espacio. Y se llegó a precisar que la idea fundamental subyacente en la de espacio, de cualquier tipo que éste fuese, era la de *proximidad*. Es, en efecto, necesario que en todo espacio podamos saber decir cuándo un elemento del espacio (punto) está próximo a otro. Entonces la Topología trata fundamentalmente de precisar y formalizar la idea de proximidad.

Según esto, un espacio topológico será un conjunto de entes entre los cuales se puede definir la idea de proximidad.

Esta idea de proximidad se ha supeditado en los espacios ordinarios (espacio euclídeo, espacio físico...) a la de métrica, o sea, a la de medida de una distancia, a la idea de distancia. Por ejemplo, definir el límite de una sucesión de puntos en la recta real, es decir, de puntos que se "aproximan" a otro, es dar una noción de distancia entre los elementos de la sucesión l_i y el límite l y asegurar que dicha distancia se hace cada vez menor y tiende hacia cero.

Utilizamos, según esto, la noción de límite en el conjunto de los números reales. Algunas propiedades, en cambio, son independientes de los números reales y, por otra parte, la misma idea intuitiva de proximidad parece encerrar ya una noción más general que la mera noción de distancia. Esto impone, pues, que consideremos el concepto de proximidad desde un punto de vista más amplio y general.

Para ello vamos a pasar revista a los conceptos elementales de topología. Los ejemplos ilustrativos los tomaremos de un tipo muy sencillo de espacio: la recta real.

2. INTERVALOS Y ABIERTOS

Dados en una recta dos puntos, a, b, llamamos *intervalo* al conjunto de puntos que pertenecen al segmento ab, excluídos los extremos:

$$(a, b) = \{x \mid a < x < b\}.$$

Se consideran también como intervalos los de los tipos siguientes:

$$(-\infty, a) = \{x \mid x < a\},$$

conjunto de puntos situados a la izquierda de a;

$$(a, \infty) = \{x \mid a < x\},$$

conjunto de puntos a la derecha de a.

Entre estos intervalos se definen las operaciones:

Unión de intervalos o conjunto de puntos que pertenecen a uno u otro de los mismos.

Intersección de intervalos o conjunto de puntos que pertenecen a ambos a la vez.

La posibilidad que hay de formar conjuntos más amplios de intervalos y de uniones de intervalos nos lleva a introducir el concepto de abierto.

Abierto es el conjunto formado por la unión de un número cualquiera, finito o infinito, de intervalos.

Los abiertos tienen las siguientes propiedades:

1.ª La unión de un número finito o infinito de abiertos es un abierto.

2.ª La intersección de un número finito de abiertos es un abierto.

La razón de que sea número finito es que de lo contrario podría la intersección no ser un abierto. Por ejemplo, en la recta real el conjunto de intervalos $(-1, 1)$, $(-\frac{1}{2}, \frac{1}{2})$, ..., $(-1/n, 1/n)$, ..., tiene como intersección, cuando n tiende a infinito, el punto 0, que evidentemente no es un abierto.

3.ª La recta real R es un abierto, pues siempre podemos hallar una unión de abiertos que nos da R; por ejemplo: $(-\infty, b)$ (a, ∞) para $a < b$. El conjunto vacío también se considera abierto, pues podemos definirlo como intersección de dos intervalos disjuntos.

Pues bien, si en un conjunto cualquiera se han elegido unos subconjuntos que gocen de estas propiedades de los abiertos, se dice que en ese conjunto se ha introducido una topología, o bien que el conjunto es un *espacio topológico*.

La topología que hemos introducido en la recta por medio de los intervalos se llama topología *ordinaria* de la recta.

3. ESPACIO TOPOLOGICO

En general, pues, dado un conjunto E y el retículo de las partes o subconjuntos de E, $\mathcal{P}(E)$, si en ese retículo se ha elegido un cierto número de partes, $\mathcal{A}$, tales que verifiquen las propiedades de los abiertos:

1.ª $\bigcup_i A_i \in \mathcal{A}$, para cualesquiera $A_i \in \mathcal{A}$, siendo i de un dominio de índices finito o infinito.

2.ª $\bigcap_n A_n \in \mathcal{A}$, para $A_n \in \mathcal{A}$, n, número finito.

3.ª $E, \emptyset \in \mathcal{A}$.

Se dice que E es un *espacio topológico* respecto de la topología introducida por los elementos de $\mathcal{A}$, que son los *abiertos* de este espacio topológico.

La topología introducida en un conjunto E cuando $\mathcal{A} = \mathcal{P}(E)$, es decir, cuando elegimos como abiertos todos los subconjuntos, es la topología más sencilla y la que más abiertos tiene; se llama topología *discreta*. La topología que posee menos abiertos es la definida en el conjunto E, tomando exclusivamente como abiertos E y $\emptyset$ y se conoce con el nombre de topología *grosera*. Una topología es tanto más fina cuantos más abiertos tiene.

Definir una *topología* en un conjunto no es, pues, otra cosa que hacer una elección de partes de ese conjunto que cumplan las tres propiedades anteriores. Para cada elección tendremos, por lo tanto, una topología distinta. Un mismo conjunto puede ser, pues, estructurado de modo que se convierta en distintos espacios topológicos, según las topologías definidas en él.

Dado un espacio topológico, llamamos *cerrado* al complementario de un abierto respecto del espacio total. Si $A \subset E$, se llama *complementario* de A en E al conjunto de puntos de E que no pertenecen a A:

$$A' = \{x \in E \mid x \notin A\}.$$

Entre las partes A, B de un conjunto E y sus respectivos complementos A', B' se cumplen las siguientes propiedades:

$$(A \cup B)' = A' \cap B' \qquad E' = \emptyset$$
$$(A \cap B)' = A' \cup B' \qquad \emptyset' = E.$$

Entonces las propiedades de los abiertos se traducen dualmente en propiedades de los cerrados en la forma siguiente:

1.ª La intersección de un número finito o infinito de cerrados es un cerrado.

2.ª La unión de un número finito de cerrados es cerrado.

3.ª $\emptyset$ y E son cerrados.

En la recta un intervalo cerrado es el segmento cerrado $[a, b]$, incluidos sus extremos:

$$[a, b] = \{x \mid a \leq x \leq b\}.$$

En este caso se verifica que $[a, b]$ es el complementario de la unión de los dos abiertos $(-\infty, a)$ y (b, ∞).

Adviértase que puede haber subconjuntos que no sean ni abiertos ni cerrados, lo cual quiere decir que ambos conceptos no son excluyentes ni clasifican tampoco los subconjuntos de un espacio topológico. El segmento abierto (a, b) más el extremo a, conjunto que se denota $[a, b)$, no es, por ejemplo, ni abierto ni cerrado. En cambio, E y $\emptyset$ son a la vez abiertos y cerrados.

Si en un conjunto se ha introducido una topología, y es, por tanto, ya un espacio topológico, llamaremos, por extensión, *punto* de dicho espacio a cada elemento del conjunto.

Sea x un punto del espacio topológico E. Se llama *entorno* de x y se representa por $U(x)$, a todo conjunto de puntos del espacio que contiene a un abierto, al cual pertenece x.

En la topología de la recta cualquier punto de un abierto posee como entorno el mismo abierto, ya que, en particular, si $x \in A$, podemos tomar $U(x) = A$, y se verifica lo antedicho. No ocurre lo mismo con los cerrados, puesto que un segmento cerrado $[a, b]$ no puede ser entorno de ninguno de sus extremos.

Las nociones de abiertos y entornos son, pues, reducibles la una a la otra, de tal modo que, dados los abiertos, se pueden definir los entornos, y viceversa. Y puede definirse la topología mediante los entornos.

La idea de proximidad se puede ahora establecer basándonos en el concepto de entorno, diciendo que un punto es próximo a otro cuando pertenece a un entorno de éste. Reducimos así la noción de proximidad a un concepto topológico en lugar de un concepto métrico. Tendremos que ver que ese concepto es más general o equivalentemente que la métrica del espacio nos produce una topología de tal modo que lo que eran puntos próximos, según la métrica, sigan siéndolo según la topología.

4. TOPOLOGIA SUBORDINADA POR UNA METRICA

La generalización de que hablábamos estará vista en cuanto comprobemos que una de las topologías que se pueden definir sobre un espacio métrico es la subordinada por la métrica.

Para ello vamos a introducir una métrica en el conjunto E mediante la aplicación

$$E \times E \longrightarrow R^+$$

(R^+, conjunto de números reales positivos más el cero), que llamamos *distancia*, y que goza de las tres propiedades:

dist. $(a, b) = 0 \Leftrightarrow a = b$.

dist. $(a\ b) =$ dist. (b, a) (propiedad simétrica).

dist. $(a, b) +$ dist. $(b. c) \geq$ dist. (a, c) (propiedad triangular).

Lo que equivale a decir que esta distancia posee las propiedades de la distancia que el producto escalar introduce en un espacio vectorial y, por lo tanto, es una generalización de la distancia euclídea. Entonces, todo conjunto dotado de esta noción de distancia diremos que es un *espacio métrico*.

Veamos cómo en un espacio en el que se ha definido esta métrica se puede introducir una topología.

En efecto, llamamos intervalo de centro a y radio r al conjunto de puntos $x \in E$, tales que dist. $(a, x) < r$. En el plano sería un círculo abierto (excluídos los puntos de su circunferencia) de centro a y radio r; en el espacio una esfera abierta y en la recta un segmento abierto.

Entonces, llamando abierto a la unión de un número finito o infinito de intervalos, queda introducida una topología. En ella, un entorno de un punto de E es, como siempre, un conjunto de puntos de E que contenga un abierto al que pertenezca el punto.

De modo que todo espacio métrico es un espacio topológico, y a la topología inducida en ese espacio por su métrica se le llama la topología *natural* de un espacio métrico.

Vista así la posibilidad de generalizar ideas proporcionadas por una métrica a ideas topológicas, vamos a precisar, como ejemplo, el concepto topológico de límite. En la recta real llamábamos límite l de una sucesión l_i, o bien decimos que l_i converge a l si, dado un número cualquiera, $\varepsilon > 0$, se puede encontrar un $n_0 \in N$, tal que para todo $n > n_0$ sea $|l - l_n| < \varepsilon$.

Esto lo expresaremos topológicamente definiendo un intervalo de centro l y radio ε, que es, desde luego, un entorno de l. La idea de límite va a consistir ahora en imponer que todos los puntos de la sucesión l_i, a partir de uno de ellos, el siguiente a l_{n_0}, están dentro de dicho entorno. Es decir, la sucesión de puntos l_i converge hacia l cuando, dado un entorno de l con radio ε cualquiera, todos los puntos de la sucesión, salvo un número finito, pertenecen a ese entorno.

La generalización a un espacio topológico cualquiera es ya inmediata; diremos que una sucesión de elementos de un espacio topológico tiene por límite un punto de él cuando, para cualquier entorno de este punto, todos los términos de la sucesión, salvo a lo más un número finito, pertenecen al entorno.

Resulta, pues, que la estructura métrica es más útil que necesaria en el planteamiento de todas las cuestiones de proximidad.

En una topología general, definida en un espacio, puede ocurrir que una sucesión tenga más de un límite, y aun infinitos. Por ejemplo, en la topología grosera de la recta el único entorno posible para cualquier punto de la recta es toda la recta; entonces, dada una sucesión de puntos en ella, cualquier punto de la recta es límite de esa sucesión, de acuerdo con la definición de límite. Esto hace que sea interesante considerar un tipo especial de espacios topológicos en los que el límite sea único.

Diremos que un espacio topológico es *separado* o de HAUSDORFF cuando, dados en él dos puntos distintos cualesquiera, x, y, se pueden encontrar para ambos sendos entornos $U(x)$ y $U(y)$ que sean disjuntos:

$$U(x) \cap U(y) = \emptyset.$$

En un espacio topológico separado toda sucesión convergente tiene límite único. Se puede ver con facilidad que la condición de separación es equivalente a la imposición de que el límite sea único.

5. HOMEOMORFISMOS

La idea fundamental de la topología es la de *continuidad*. Una aplicación

$$E \xrightarrow{f} E',$$

en la que

$$a \xrightarrow{f} a' = f(a) \in E';$$

diremos, de una manera todavía un poco vaga, que es continua en a cuando los puntos próximos al a se transforman mediante f en puntos próximos al a'. Pero la topología llama punto próximo a a a todo punto perteneciente a un entorno de a. Podemos entonces precisar más diciendo que f es continua en a si todo punto $x \in U(a)$ se transforma en un $x' = f(x) \in U(a')$.

Dando un paso más, equivale esto a decir que para cada entorno $U[f(a)]$ de $f(a)$ podemos encontrar un entorno $U(a)$ de a tal que

$$f[U(a)] \subset U[f(a)],$$

o sea, que f es continua en a si, dado un entorno de $f(a)$ se puede encontrar un entorno de a tal que todos sus puntos se transforman mediante f en los del entorno dado de $f(a)$.

Si particularizamos esta definición al caso de un espacio métrico nos encontramos con la definición clásica de continuidad. En él, los entornos $U[f(a)]$ y $U(a)$ serán, respectivamente, intervalos de centros $f(a)$ y a, y radios ε y η, por ejemplo. Es decir:

$$U[f(a)] = \{x' \mid \text{dist. } [x',\ f(a)] < \varepsilon\}.$$
$$U(a) = \{x \mid \text{dist. } (x,\ a) < \eta\}.$$

Entonces, la traducción literal sería:

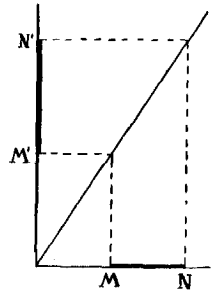
Dado un entorno de $f(a)$ (es decir, dado un número $\varepsilon > 0$), podemos encontrar un entorno de a (podemos encontrar un número η), tal que para todo punto perteneciente a este entorno (para todo x, tal que $|x - a| < \eta$) se verifique que $f(x)$ pertenece al de $f(a)$ (se verifique que $|f(x) - f(a)| < \varepsilon$). Esta es, precisamente, la definición usual.

La aplicación será continua en un intervalo cuando lo sea en cada uno de sus puntos.

Si esta aplicación es además biunívoca y bicontinua en el intervalo, llamando bicontinua a toda aplicación continua f cuya inversa f^{-1} sea también continua, se dice que se trata de un *homeomorfismo* o *transformación topológica*.

Mediante un homeomorfismo, todos los puntos próximos de E se transforman en puntos próximos de E' y, recíprocamente, puntos próximos de E' tienen por originales puntos próximos de E.

Intuitivamente, en el caso de la función representada en el dibujo, es como si la transformación de MN en $M'N'$ fuese una deformación elástica, de modo que adaptásemos el primer segmento al segundo "estirándolo".



Esta es la idea gráfica mediante la cual podríamos describir un homeomorfismo: si suponemos que una figura, una superficie, por ejemplo, es deformable, y pasamos de la superficie dada a una de-

formación suya estirándola o contrayéndola, como si fuera de goma, pero sin rasgar la superficie original, la superficie obtenida es homeomorfa con la dada.

Todas las figuras que se pueden transformar entre sí mediante homeomorfismos son topológicamente equivalentes. Es decir, las propiedades topológicas se conservan en el homeomorfismo. Los homeomorfismos vienen a ser los "isomorfismos" de la estructura topológica; es decir, dos figuras homeomorfas se consideran una misma cosa desde el punto de vista de la topología.

Son, por ejemplo, topológicamente iguales el toro y una esfera con un asa, pues hay un conjunto de deformaciones homeomórficas que nos convierten la primera superficie en la segunda. No son, en cambio, topológicamente equivalentes una superficie esférica y un toro o cualquiera de ellas y un plano; una superficie esférica es topológicamente distinta de ella misma si le hacemos un agujero.

Cursillo de Matemáticas en Valencia

ORGANIZADO por el Seminario de Orientación Didáctica de la Inspección de Enseñanza Media del Estado de Valencia, se celebró del 15 al 30 de abril, en los locales del Instituto «Luis Vives» de dicha ciudad, un cursillo de Profesores de Matemáticas de Bachillerato, que tuvo una asistencia muy numerosa.

Estuvo dirigido por los Profesores don José Ramón Pascual Ibarra, catedrático del Instituto «Cervantes» de Madrid e Inspector excedente, y don José García García, catedrático del Instituto «Luis Vives», que fueron presentados a los asistentes por el Inspector Jefe del distrito don José Pisa Leza.

Se trabajó, por la mañana, en dos sesiones de 10 a 13,30, sobre temas de fundamentación de la Matemática Moderna, y por la tarde, en dos clases prácticas de 4 a 7, sobre Didáctica de la Matemática de Grado Elemental, alguna de ellas con alumnos de los primeros cursos del Bachillerato

El cursillo resultó muy interesante y en la sesión de clausura se manifestó la conveniencia de que todos los años se celebren reuniones de este tipo.

El Centro de Orientación Didáctica entregó a los cursillistas un certificado de asistencia.