Sobre puntos y coordenadas

S. XAMBÓ DESCAMPS

En mathématique aussi, il y a bien entendu des spécialités qu'on nomme analyse, géometrie ou algèbre. Mais ces spécialités n'ont pas d'existence permanente et les lignes de démarcation se décplacent et changent continuellement. Parler de spécialités rigidement établies en mathématique est certainement un non-sens. Les mathématiciens qui se spécialisent étroitement se condamment à une vue incomplète de la mathématique contemporaine.

A. Weil [1961]

INTRODUCCION

En su *Géométrie* Descartes nos reveló, entre otras maravillas, la posibilidad de construir y estudiar entes geométricos, conocidos o nuevos, por medios puramente algebraicos. Se trata de un puente entre álgebra y geometría con tránsito en los dos sentidos, ya que las ideas geométricas condicionan a su vez los conceptos algebraicos que a ellas se asocian. Una ilustración elemental y bien conocida, pero fundamental, de este influjo recíproco es el desarrollo gradual del álgebra lineal en el siglo pasado, como trasunto intrínseco de las coordenadas, hasta perfilarse como el lenguaje natural de las geometrías lineales usuales (afín, métrica, proyectiva e hiperbólica) y llegar a ser, por su versatilidad, en una de las materias matemáticas más básicas, en parte debido a que, en breves y sugestivas palabras de Manin [1981, p. 8 y 9], lo lineal no es más que una idealización de «pequeñas perturbaciones arbitrariamente grandes» y que «a pequeña escala todo puede ser linealizado».

El tema es pues el de las relaciones entre álgebra y geometría, bien sean en la dirección de algebraizar ésta o en la de geometrizar aquélla, e incluso, más en general, el de las relaciones entre sistemas matemáticos dispares, como entre polinomios, cuerpos y grupos en la teoría de Galois de las ecuaciones, o entre revestimientos no ramificados de un espacio topológico y subgrupos del grupo fundamental de la base. Es un tema recurrente cuyo cultivo ha movilizado medios cada vez más refinados. A los ejemplos mencionados (el álgebra lineal, la teoría de Galois y la teoría de Poincaré del grupo fundamental) se podrían añadir muchos otros. Aquí queremos citar los siguientes:

(a) Los trabajos de Boole [1847, 1854] sobre lógica algebraica.

(b) La versión puramente algebraica de la teoría de las superficies de Riemann compactas, debida a Dedeking y Weber [1882] (para una exposición reciente véase Lang [1982]).

(c) Los resultados de Hilbert [1890] sobre anillos de polinomios y que esencialmente constituyen los fundamentos algebraicos sobre los que descansa la teoría moderna de las variedades algebraicas en el sentido de Serre [1955].

(d) Las investigaciones de Stone [1934, 1936, 1937] sobre determinadas relaciones entre la lógica algebraica y la topología, las cuales han evolucionado en la dirección que algunos llaman «algebraización de la topología» y otros «topología sin puntos» (a este respecto se puede consultar el libro Johnstone [1982], o el artículo Johnstone [1983], en los que este tema es considerado con detalle).

(e) La teoría espectral de S. Mazur e I. Gelfand (véase, por ejemplo, Gelfand-Raikov-Chilov [1964], Naimark [1972]).

(f) El desarrollo de la geometría algebraica contemporánea, impulsando principalmente por A. Grothendieck, como una síntesis, abogada ya por Kronecker, de las ideas de geometría algebraica y las de la teoría algebraica de números (Grothendieck-Dieudonné [EGA], Grothendieck *et al* [SGA]).

(g) La teoría de las supervariedades (diferenciables, analíticas o algebraicas) y de los grupos cuánticos (véase, por ejemplo, Manin [1984, 1988 b] y Manin [1988 a]), o, más en general, la llamada *Geometría no conmutativa*(véase Connes [1990]).

Estos puntos, que sin duda son capitales para poder formarse una perspectiva histórica de las interacciones del álgebra con otras materias, aportan, si son tenidos en cuenta, un enriquecimiento substancial del fondo de ideas en el que la docencia y la investigación hallan su último sustento. Pero no es fácil encontrar textos asequibles que nos sirvan de guía en estos territorios, especialmente a los no iniciados. Si consideramos, por ejemplo, la geometría algebraica de Grothendieck, incluso la versión pedagógica de Hartshorne [1977] exige un tiempo muy dilatado de estudio, ya que a las casi 500 páginas del texto se deben añadir, si se quiere asimilar con éxito, un texto previo de variedades algebraicas y otro de álgebra conmutativa. Pero incluso tras arduos estudios pueden aún quedar ocultas las razones profundas por las cuales el espacio de ideales primos de un anillo encierra el secreto de la unificación entre geometría algebraica y aritmética, o las raíces que explican, nutriendo el presente desde el subsuelo de la historia de las ideas, por qué dicho espacio es denominado «espectro» del anillo. ¿Tendrá alguna relación este uso de la palabra espectro con el uso ordinario en física atómica, como en «el espectro del litio»?

En estas páginas discutiremos algunas ideas elementales relativas a las interacciones entre el Algebra y otras ramas de las Matemáticas, principalmente aquéllas que tienen más relieve para la geometría algebraica. Más concretamente, describiremos algunos de los procesos básicos que llevan de un modo natural de objetos geométricos, en un sentido amplio, a objetos algebraicos, especialmente anillos, y también los que nos permiten reproducir aquéllos a partir de éstos, esto es, que nos permiten asociar un objeto geométrico a uno algebraico, digamos un anillo. En la medida de lo posible, discutiremos algunos ejemplos con objeto de

hacer más tangible la potencia, consubstancial con el sueño de Descartes, que estas ideas aportan.

Se ha de advertir que los temas aquí tratados son bien conocidos por los correspondientes expertos, siendo el objeto de estas notas no más que un intento de exponerlos al nivel más elemental y autocontenido que nos ha sido posible alcanzar a fin de que pueda ser útil para el mayor número de lectores, incluyendo, naturalmente, a los estudiantes de Matemáticas. Estos tal vez puedan leerlo con provecho para percibir con más discernimiento la naturaleza de algunos de los estudios que pueden emprender y la de su continuación, si llegare éste a ser el caso, en una carrera de investigación.

Siendo así que alguna de estas cuestiones (como el papel del álgebra en la geometría, la optimización de la docencia y la perspectiva histórica de los conceptos) han sido el objeto de las fructíferas reflexiones del profesor don José J. Etayo Miqueo a lo largo de su carrera científica, quisiera ofrecerle estas páginas como una expresión de mi reconocimiento a su espléndida y ejemplar labor.

Preliminares. Este epígrafe es de referencia y el lector sólo debe consultarlo si se da el caso de que un cierto concepto, para el cual no se da ninguna referencia, no le es familiar. Los requisitos se reducen a nociones elementales de álgebra y topología, e incluso algunas de ellas se revisan brevemente.

Todos los anillos se supondrán no nulos con unidad y por *homomorfismo de anillos* entenderemos un homomorfismo de la suma y del producto que transforma la unidad en la unidad. Si no se dice explícitamente lo contrario, los anillos se supondrán conmutativos. Si A es un anillo y J es un ideal de A, para todo elemento $a \in A$ pondremos $a(I)$ para denotar la clase de restos de a módulo I, de modo que $a \mapsto a(I)$ coincide con la proyección canónica de A en el cociente A/I.

Un *dominio* es un anillo que carece de divisores de cero no nulos, esto es, en el cual $ax = 0$ y $a \neq 0$ implican $x = 0$. Un ideal $\boldsymbol{p}$ de A se dice que es *primo (maximal)* si $A/\boldsymbol{p}$ es un dominio (un cuerpo), esto es, si $ax \in \boldsymbol{p}$ y $a \notin \boldsymbol{p}$ implican $x \in \boldsymbol{p}$ (respectivamente, si para todo $a \in A - \boldsymbol{p}$ existe un $b \in A$ tal que $ab - 1 \in \boldsymbol{p}$).

Como es costumbre, pondremos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ para denotar, respectivamente, el anillo de los números *enteros*, el cuerpo de los números *racionales*, el cuerpo de los números *reales* y el cuerpo de los números *complejos*.

Si $\phi: A \to B$ es un homomorfismo de anillos y J es un ideal de B, $\phi^{-1} J$ es un ideal de A. Puesto que la composición de ϕ con la proyección canónica $B \mapsto B/J$ tiene núcleo $\phi^{-1} J$, vemos que ϕ induce una inclusión

$$A/\phi^{-1} J \hookrightarrow B/J$$

En el caso de que J *sea primo, entonces* $\phi^{-1} J$ también lo es, pues si B/J es un dominio, también lo es $A/\phi^{-1} J$. La inclusión de $\mathbb{Z}$ en $\mathbb{Q}$ y el ideal $\{0\}$ de $\mathbb{Q}$ prueban que la imagen inversa de un ideal maximal no es, en general, un ideal maximal.

Un elemento a de un anillo se dice *nihilpotente* si existe un entero positivo n tal que $a^n = 0$. *El conjunto de elementos nihilpotentes coincide con la intersección de todos los ideales primos.* En efecto, es claro que todo ideal primo $\boldsymbol{p}$ contiene a cualquier nihilpotente a, pues si $a^n = 0$, entonces $a^n \in \boldsymbol{p}$ y por tanto $a \in \boldsymbol{p}$. Viceversa, si a no es nihilpotente, veremos enseguida que el lema de Zorn permite hallar un ideal $\boldsymbol{p}$ que es maximal entre los que no contienen ninguna potencia de a y que este ideal resulta ser primo, con lo cual estamos en presencia de un ideal primo que no contiene a a.

He aquí la línea general de la demostración de los dos últimos asertos. Por hipótesis el ideal $\{0\}$ no contiene ninguna potencia de a, y si una cadena de ideales no contiene ninguna potencia de a, entonces la unión conjuntista de los mismos es un ideal que no contiene ninguna potencia de a. Así pues existe un ideal $\boldsymbol{p}$ que es maximal entre los que no contienen a a. Veamos que $\boldsymbol{p}$ es primo. Si x, $y \notin \boldsymbol{p}$, entonces los ideales $\boldsymbol{p} + (x)$ y $\boldsymbol{p} + (y)$ contienen propiamente a $\boldsymbol{p}$ y por tanto cada uno de ellos contiene una potencia de a. Así pues existen $b,c \in A, s,t \in \boldsymbol{p}$ y enteros positivos n,m tales que $a^n = s + bx$, $a^m = t + cy$, de donde

$$a^{n+m} = z + (bc)(xy),\ z \in \boldsymbol{p}$$

Como $a^{n+m} \notin \boldsymbol{p}$, inferimos que $xy \notin \boldsymbol{p}$.

Un anillo que no tiene elementos nihilpotentes no nulos se dice que es *reducido*.

Usaremos los siguientes *lemas de confinamiento* de ideales: (1) si un ideal está contenido en la unión conjuntista de un número finito de ideales primos, entonces el ideal está contenido en uno de ellos, y (2) si un ideal primo contiene la intersección de un número finito de ideales, entonces dicho ideal primo contiene a uno de ellos.

Si B es un anillo y A un subanillo de B, un elemento $b \in B$ se dice que es *algebraico* sobre A si existen elementos $a_0,...,a_n \in A$, no todos nulos, tales que

$$a_0b^n + a_1b^{n-1} + ... + a_{n-1}b + a_n = 0$$

Si podemos tomar $a_0 = 1$, se dice que b es un elemento *entero* sobre A. Los elementos de B que son enteros sobre A forman un subanillo de B, llamado cierre entero de A en B. Así pues resulta que la suma y el producto de elementos enteros son elementos enteros.

Dado un cuerpo $\boldsymbol{k}$, a los anillos que contienen a $\boldsymbol{k}$ como subanillo los llamaremos $\boldsymbol{k}$-álgebras. Un *morfismo de* $\boldsymbol{k}$-álgebras es un morfismo de anillos que restringido a $\boldsymbol{k}$ es la identidad.

Si A es una $\boldsymbol{k}$-álgebra y $x_1,...,x_r$ son elementos de A, pondremos $\boldsymbol{k}[x_1,...,x_r]$ para denotar el subanillo de A formado por las expresiones polinómicas en $x_1,...,x_r$ con coeficientes en $\boldsymbol{k}$. Diremos que una $\boldsymbol{k}$-álgebra A es *finitamente generada sobre* $\boldsymbol{k}$ si existen $x_1,...,x_r \in A$ tales que $A = \boldsymbol{k}[x_1,...,x_r]$. Si $T_1,...,T_r$ son indeterminadas, pondremos $\boldsymbol{k}[T_1,...,T_r]$ para denotar el anillo de polimonios en las indeterminadas $T_1,...,T_r$ el cual es una $\boldsymbol{k}$-álgebra finitamente generada sobre $\boldsymbol{k}$. Es importante tener presente que dar un morfismo de $\boldsymbol{k}$-álgebras $\varnothing$: $\boldsymbol{k}[T_1,...,T_r] \to A$ equivale a dar un elemento $a = (a_1,...,a_r) \in A^r$: $\varnothing$ es el único morfismo de $\boldsymbol{k}$-álgebras tal que

$\phi(T_i) = a_i$, de modo que ϕ es el *homomorfismo* ϕ_a *de evaluación en* a, $\phi_a(q) = q(a)$ para todo polimonio q.

Si $\boldsymbol{k}$ es un cuerpo y T una indeterminada, es fácil verificar que $\boldsymbol{k}[T]$ coincide con su propio cierre entero en $\boldsymbol{k}(T)$ (el cuerpo de funciones racionales en T con coeficientes en $\boldsymbol{k}$), lo cual se enuncia diciendo que $\boldsymbol{k}[T]$ es *íntegramente cerrado.*

Usaremos el *teorema de la base* de Hilbert, según el cual todo ideal de $\boldsymbol{k}[T_1,...,T_n]$ es finitamente generado.

Se dice que un cuerpo $\boldsymbol{k}$ es *algebraicamente cerrado* si todo $f \in \boldsymbol{k}[T]$ de grado $n > 0$ con coeficientes en $\boldsymbol{k}$ tiene una raíz en $\boldsymbol{k}$, esto es, si existe $t \in \boldsymbol{k}$ tal que $f(t) = 0$. En tal caso existen elementos $a,t_1,...,t_n \in \boldsymbol{k}, t_1 = t$, tales que $f = a(T - t_1)...(T - t_n)$. Si $\boldsymbol{k}$ es un cuerpo algebraicamente cerrado y K es un cuerpo que contiene a $\boldsymbol{k}$ con $\dim_{\boldsymbol{k}} K < \infty$, entonces $K = \boldsymbol{k}$. Es decir, un *cuerpo algebraicamente cerrado no tiene extensiones finitas no triviales.*

El cuerpo C es algebraicamente cerrado (teorema fundamental del álgebra).

1. SOBRE PIXELES Y ANILLOS DE BOOLE

> And again it turns out, as always, that the visible must be explained in terms of the invisible.
>
> Manin [1981], p. 57

Esta sección tiene por objeto mostrar, en un caso particularmente simple, casi de juguete, las relaciones fundamentales que aparecen al analizar ciertos anillos de funciones, sus ideales primos y los puntos sobre los cuales las funciones toman sus valores. En secciones sucesivas veremos que el «paradigma» resultante tiene análogos en contextos tales como la geometría algebraica o el análisis funcional.

Píxeles y estados de una pantalla. Nos podemos imaginar una pantalla gráfica (monocroma y sin otras tonalidades que el claro y el oscuro) como una fina retícula de minúsculas bombillas. A estas bombillas se las denomina, en el argot informático, «píxeles». Si un píxel está apagado, diremos que está en el estado 0 y si está encendido, en el estado 1. Así pues el conjunto de estados posibles de un píxel es $\mathbb{Z}_2 = \{0,1\}$. Nótese que $\mathbb{Z}_2$ tiene una única estructura de anillo para la cual 0 es el neutro de la suma.

Sea ahora X un conjunto. Para estimular la imaginación, podemos pensar que X es el conjunto de píxeles de una determinada pantalla. Como un estado de la pantalla viene determinado por la lista de los píxeles que están encendidos, vemos que dar un tal estado equivale a dar un subconjunto de X. Ahora bien, dar un subconjunto de X equivale a dar una aplicación a: $X \to \mathbb{Z}_2$: si Y es un subconjunto de X, la aplicación que le corresponde es la función característica χ_Y de Y,

$$\chi_Y(x) = \begin{cases} 1 \text{ si } x \in Y \\ 0 \text{ si } x \notin Y \end{cases}$$

e inversamente, si $\alpha: X \to \mathbb{Z}_2$ es una aplicación, el subconjunto de X que ella determina es $D(\alpha) = \{x \in X: \alpha(x) = 1\}$, léase dominio de α, que es el complementario del conjunto $Z(\alpha) := \{x \in X \mid \alpha(x) = 0\}$. Así pues

$$\chi_{D(\alpha)} = \alpha \text{ y } D(\chi_Y) = Y$$

Nótese que si $x \in X$, entonces $\chi_{\{x\}}$ es la función que toma valor 1 en x y 0 en los demás elementos de X y que si $x_1,\dots,x_r$ son elementos distintos de X, entonces $\chi_{\{x1,\dots,xr\}} = \chi_{x1} + \dots + \chi_{xr}$, donde para simplificar ponemos χ_x en lugar de $\chi_{\{x\}}$.

El anillo de estados. El conjunto $F(X,\mathbb{Z}_2)$ de las aplicaciones de un conjunto X en Z_2 tiene estructura de anillo. Recordemos que el conjunto $F(X,A)$ de las aplicaciones de un conjunto X en un anillo A, que siguiendo la costumbre llamaremos *funciones* de X a valores en A, constituyen un anillo que contiene una copia del anillo A. En efecto, la suma y producto de funciones se define por las reglas usuales:

$$(\alpha + \beta)(x) = \alpha(x) + \beta(x),\ (\alpha\beta)(x) = \alpha(x)\beta(x)$$

y un elemento a de A se identifica con la función constante $x \mapsto a$ para todo x de X.

La biyección del epígrafe anterior nos permite transportar la estructura de anillo de $F(X,\mathbb{Z}_2)$ al conjunto $P(X)$ de subconjuntos de X. Puesto que $\chi_Y\chi_Z$ vale 1 exactamente en los elementos de $Y \cap Z$, y que $\chi_Y + \chi_Z$ vale 1 exactamente para los elementos de la diferencia simétrica $Y \Delta Z$ (elementos que están en Y pero no en Z ó en Z pero no en Y), vemos que $P(X)$ es un anillo tomando como suma la diferencia simétrica y como producto la intersección.

Anillos de Boole. Un anillo de Boole es un anillo A para el cual $a^2 = a$ para todo $a \in A$. Por ejemplo, $F(X,\mathbb{Z}_2)$, y por tanto $P(X)$, es un anillo de Boole. Repárese en que todo anillo de Boole es conmutativo, ya que de un lado $a + b = (a + b)^2 = a^2 + ab + ba + b^2 = a + b + ab + ba$, de donde $ab + ba = 0$, cualesquiera que sean $a,b \in A$, y del otro, poniendo $b = a$, hallamos que $a + a = 0$ para todo a (equivale a $-a = a$), de donde $ba = -ab = ab$ para todo a y b.

1.1. *Si A es un dominio de Boole, esto es, un anillo de Boole sin divisores de cero no nulos, entonces A es isomorfo a* $\mathbb{Z}_2$.

En efecto, si $a \in A$, de $a^2 = a$ se deduce que $a(a-1) = 0$. Si A no tiene divisores de 0, entonces será $a = 0$ ó $a - 1 = 0$. □

Como corolario tenemos:

1.2. *Si A es un anillo de Boole y* $\boldsymbol{p}$ *es un ideal primo de A, entonces A/p es canónicamente isomorfo a* $\mathbb{Z}_2$. *En particular, todo ideal primo de* A *es un ideal maximal.*

En efecto, $A/\boldsymbol{p}$ es un anillo de Boole, por serlo A, y es un dominio, por definición de ideal primo. □

La composición $A \to A/\boldsymbol{p} \cong \mathbb{Z}_2$ es el único morfismo υ_p de A en $\mathbb{Z}_2$ cuyo núcleo es $\boldsymbol{p}$,

$$\upsilon_p(a) = \begin{cases} 0 & \text{si } a \in p \\ 1 & \text{si } a \notin p \end{cases}$$

Como la clase módulo $\boldsymbol{p}$ de un elemento $a \in A$ es $a(\boldsymbol{p})$, vemos que $a(\boldsymbol{p})$ se corresponde con $\upsilon_p(a)$ por el isomorfismo del corolario 1.2. En lo sucesivo identificaremos $A/\boldsymbol{p}$ con $\mathbb{Z}_2$ y por tanto nos será permitido escribir la relación

$$a(\boldsymbol{p}) = \upsilon_p(a)$$

Viceversa, un homomorfismo $x: A \to \mathbb{Z}_2$ determina un ideal primo $\boldsymbol{p}_x$ de A, $\boldsymbol{p}_x = ker\,(x)$. Obsérvese que

$$x(a) = \upsilon_{px}(a) = a(\boldsymbol{p}_x)$$

Pongamos $\mathcal{X}(A)$ y $\mathcal{P}(A)$ para denotar el conjunto de homomorfismos de A en $\mathbb{Z}_2$ y el conjunto de ideales primos de A. Entonces tenemos:

1.3. *Dado un anillo de Boole A, la correspondencia* $x \mapsto \boldsymbol{p}_x$ *nos da una biyección entre el conjunto* $\mathcal{X}(A)$ *y el conjunto* $\mathcal{P}(A)$. *La correspondencia inversa es* $\boldsymbol{p} \mapsto \upsilon_p$.

Como se ha dicho, $ker(\upsilon_p) = \boldsymbol{p}$. Por otra parte, $\boldsymbol{p}_x$ es el núcleo de x y de υ_{px}, de donde $x = \upsilon_{px}$ para todo $x \in \mathcal{X}(A)$. □

Teorema de representación. Sea A un anillo de Boole e identifiquemos $\mathcal{X} = \mathcal{X}(A)$ con $\mathcal{P} = \mathcal{P}(A)$ por medio de las biyecciones (1.3). Dado $a \in A$, sea $\hat{a}: \mathcal{X} \to \mathbb{Z}_2$ la aplicación definida de la siguiente manera:

$$\hat{a}\,(x) = x(a) = a(\boldsymbol{p}_x)$$

De este modo tenemos una aplicación $\rho: A \to F(\mathcal{X},\mathbb{Z}_2)$, $a \mapsto \hat{a}$. Se comprueba sin ninguna dificultad que esta aplicación es un homomorfismo de anillos. Veamos que ρ es inyectivo. En efecto, si $\hat{a} = 0$, ello significa que $a \in \boldsymbol{p}$ para todo ideal primo $\boldsymbol{p}$ de A y por tanto a es nihilpotente. Pero entonces la relación $a = a^2$ implica que $a = 0$.

En suma, hemos demostrado que todo anillo de Boole A es isomorfo a un subanillo del anillo $F(X,\mathbb{Z}_2)$, siendo X el conjunto de homomorfismos de A en $\mathbb{Z}_2$, o el conjunto $\mathcal{P}(A)$ de los ideales primos de A. Teniendo en cuenta el isomorfismo entre $F(\mathcal{X},\mathbb{Z}_2)$ y $P(\mathcal{X})$ (por el cual $\hat{a}$ se corresponde con el conjunto $D(\hat{a}) \subseteq \mathcal{X}(A)$), queda demostrado el siguiente «teorema de representación»:

1.4. *Sea A un anillo de Boole y* $\mathcal{X}$ *el conjunto de homomorfismos de A en* $\mathbb{Z}_2$, *o el conjunto de sus ideales primos. Entonces un monomorfismo natural (de anillos)* $A \hookrightarrow P(\mathcal{X})$. □

Observación. Los conjuntos $D(\hat{a}) \subseteq \mathcal{X}(A)$ coinciden con los conjuntos entornados (es decir, simultáneamente abiertos y cerrados) de una topología de $\mathcal{X}(A)$. Con esta topología resulta que $\mathcal{X}(A)$ es un espacio de Boole (un espacio topológico compacto y Hausdorff en el que todo abierto es la unión de los conjuntos entornados que contiene) y que todo espacio de Boole X es homeomorfo al espacio $\mathcal{X}(A(X))$, donde $A(X)$ es el álgebra de Boole de los conjuntos entornados de X (véase Halmos [1962], § 18).

Píxeles e ideales primos. Estudiemos ahora el caso del anillo $F(X,\mathbb{Z}_2)$, X un conjunto. Dado un elemento $x \in X$, podemos considerar el homomorfismo $F(X,\mathbb{Z}_2) \to \mathbb{Z}_2$ dado por $\alpha \mapsto \alpha(x)$. Dado que dos elementos distintos de X dan homomorfismos distintos, podemos identificar X a un subconjunto de $\mathcal{X}(F(X,\mathbb{Z}_2))$. Nótese que el ideal primo $\boldsymbol{p}_x$ que corresponde a un punto x está formado por los elementos $a \in A$ tales que $a(x) = 0$, y que $x(a) = a(x)$, donde a la izquierda x se interpreta como un homomorfismo de A en $\mathbb{Z}_2$ y a la derecha como un elemento de X.

Si nos restringimos a conjuntos finitos, lo cual es el caso para el conjunto de píxeles de una pantalla, entonces se tiene:

1.5. *Las correspondencias $X \mapsto F(X,\mathbb{Z}_2)$ y $A \mapsto \mathcal{X}(A)$, la primera de conjuntos finitos a anillos de Boole finitos y la segunda en sentido contrario, son inversas una de la otra (salvo biyecciones canónicas). Es decir, para todo conjunto finito X, existe una biyección natural entre X y $\mathcal{X}(F(X,\mathbb{Z}_2))$, y para todo anillo de Boole finito A existe una biyección natural entre A y $F(\mathcal{X}(A),\mathbb{Z}_2)$.*

Se trata de ver, si $\boldsymbol{p}$ es un ideal primo de $F(X,\mathbb{Z}_2)$, que existe una $x \in X$ tal que $\boldsymbol{p} = \boldsymbol{p}_x$ (como hemos dicho ya, x es entonces único). A tal fin basta ver, por ser $\boldsymbol{p}$ maximal, que existe $x \in X$ con $\boldsymbol{p} \subseteq \boldsymbol{p}_x$.

Para buscar una x con esta propiedad, notemos primero que si $\boldsymbol{p}$ no está contenido en $\boldsymbol{p}_x$, entonces la función característica $\mathcal{X}_x$ del punto x está en $\boldsymbol{p}$: si α es un elemento de $\boldsymbol{p}$ con $\alpha(x) \neq 0$, entonces $\mathcal{X}_x = \mathcal{X}_x\alpha \in \boldsymbol{p}$. Así pues si $\boldsymbol{p}$ no estuviese contenido en ningún $\boldsymbol{p}_x$, entonces $\boldsymbol{p}$ contendría la suma $\Sigma\mathcal{X}_x$ donde x recorre X, suma que es la unidad del anillo $F(X,\mathbb{Z}_2)$.

También tenemos que comprobar que si A es un anillo de Boole finito, y α una función de $\mathcal{X} = \mathcal{X}(A)$ a valores en $\mathbb{Z}_2$, entonces $\alpha = \hat{a}$ para un cierto a de A. A tal fin basta ver que dado un ideal maximal $\boldsymbol{p}$, existe un elemento a tal que $a \notin \boldsymbol{p}$ y de modo que a pertenece a cualquier ideal maximal distinto de $\boldsymbol{p}$ (es decir, tal que $\hat{a} = \mathcal{X}_{(p)}$. Pero esto es una consecuencia directa del segundo lema de confinamiento de ideales: este lema nos muestra que la intersección de los ideales maximales distintos de $\boldsymbol{p}$ (sólo hay una cantidad finita de ellos) no puede estar contenida en $\boldsymbol{p}$, ya que de otro modo llegaríamos al absurdo de que $\boldsymbol{p}$ contendría uno de dichos ideales. □

Observación. Para todo entero positivo n,

$$\mathbb{Z}_2^n \cong F(\{1,\ldots,n\},\mathbb{Z}_2)$$

es un álgebra de Boole con n ideales primos. La anterior proposición muestra que si A es un álgebra de Boole finita con n ideales primos, entonces A es isomorfa a $\mathbb{Z}_2^n$.

Homomorfismo de anillos de Boole. Si X y X' son conjuntos y $f\colon X \to X'$ es una aplicación, entonces la transformación

$$f^*\colon F(X',\mathbb{Z}_2) \to F(X,\mathbb{Z}_2)$$

definida por la relación $f^*(\alpha') = \alpha' \circ f$, es un homomorfismo de anillos. Pongamos $\phi = f^*$ y veamos que ϕ permite reconstruir f, en el caso en que X y X' sean finitos. En efecto, si interpretamos los puntos de X (respectivamente, X') como homomorfismos de $F(X,\mathbb{Z}_2)$ en $\mathbb{Z}_2$ (respectivamte de $F(X',\mathbb{Z}_2)$, entonces $f = \phi^*$ (por definición $\phi^*x = x \circ \phi$), pues para todo $x \in X$, $\alpha' \in F(X',\mathbb{Z}_2)$,

$$(\phi^*x)(\alpha') = (x \circ \phi)(\alpha') = x(\phi(\alpha')) = x(\alpha' \circ f) = (\alpha' \circ f)(x) = \alpha'(fx) = (fx)(\alpha')$$

Nótese que la reconstrucción de f a partir de ϕ en términos de ideales primos consiste en que la relación $f(x) = x'$ equivale a

$$\phi^{-1}(\boldsymbol{p}_x) = \boldsymbol{p}_{x'}$$

No es ahora difícil ver que la aplicación $f \mapsto \phi$ es una biyección entre el conjunto de aplicaciones $X \to X'$ y el conjunto de homomorfismos de anillos $F(X',\mathbb{Z}_2) \to F(X,\mathbb{Z}_2)$. Junto con el teorema de representación, vemos que las biyecciones de (1.5) son categoriales, en el sentido que inducen biyecciones entre el conjunto de homomorfismos $A' \to A$ entre dos álgebras de Boole finitas A' y A, y el conjunto de aplicaciones de $\mathcal{X}(A) \to \mathcal{X}(A')$. En otros términos, la «geometría» de los conjuntos finitos equivale al «álgebra» de las álgebras de Boole finitas.

2. SOBRE CONJUNTOS CARTESIANOS

> The archetype of an m-dimensional geometrical object is the number space $\mathbb{R}^m$ or, from the time of Descartes, the ring of polynomial functions $\mathbb{R}[x_1, \ldots, x_m]$.
>
> Manin [1984], p. 51

Existe una equivalencia entre, de un lado, conjuntos algebraicos y aplicaciones algebraicas entre los mismos (estos conceptos se definen en los epígrafes que siguen) y, del otro, álgebras finitamente generadas reducidas sobre un cuerpo algebraicamente cerrado $\boldsymbol{k}$ y homomorfismos entre las mismas. Esta equivalencia es análoga a la que hemos establecido en la sección anterior. Se basa en el teorema débil de los ceros de Hilbert (2.2), que juega aquí el papel análogo al que ha jugado antes el enunciado (1.2). Esta correspondencia será usada para establecer que la «geometría» de los conjuntos algebraicos es equivalente al «álgebra» de las $\boldsymbol{k}$-álgebras reducidas finitamente generadas sobre $\boldsymbol{k}$.

Conjuntos algebraicos. Si $\boldsymbol{k}$ es un cuerpo infinito, podemos interpretar el conjunto $\boldsymbol{k}^n$, siguiendo la prescripción de la geometría analítica de Descartes, como un «espacio geométrico» (afín). Los polinomios $q \in \boldsymbol{k}[T_1,\ldots,T_n]$ en las indeterminadas T_i, con coeficientes en $\boldsymbol{k}$, proporcionan funciones $\boldsymbol{k}^n \to \boldsymbol{k}, x \mapsto q(x)$. Siendo k infinito, se puede identificar cada polinomio con la correspondiente función, toda vez que si $q(x) = 0$ para todo $x \in \boldsymbol{k}^n$ entonces $q = 0$. Hablaremos en este caso de polinomios o funciones polinómicas, indistintamente. Por ejemplo, T_i es la i-ésima función de coordenadas, $T_i(x_1,...,x_n) = x_i$.

Las figuras «cartesianas» del espacio k^n son los subconjuntos dados por un número finito de ecuaciones polinómicas. Más precisamente, un subconjunto X de k^n se dice que es *algebraico* si existen polinomios $f_1,...,f_r$ de n variables con coeficientes en k tales que $X = Z(f_1,...,f_r)$, donde

$$Z(f_1,...,f_r) = \{x \in k^n \mid f_1(x) = ... = f_r(x) = 0\}$$

Obsérvese que $Z(f_1,...,f_r) = Z(f_1) \cap ... \cap Z(f_r)$. A los conjuntos de la forma $Z(f)$, $f \neq 0$, se les denomina *hipersuperficies* (*curvas planas* para $n = 2$, *superficies* para $n = 3$). Si el grado total de f es d, se dice también que $Z(f)$ tiene grado d. Las hipersuperficies de grado 1 son los *hiperplanos* (*rectas* para $n = 2$, *planos* para $n = 3$) y las de grado 2 las *hipercuádricas* (*cónicas* para $n = 2$, *cuádricas* para $n = 3$).

Geometría algebraica y geometría diferencial. Si fuese $k = \mathbb{R}$ (ó $\mathbb{C}$), el teorema de la función implítica nos dice que si $d_x f_1,...,d_x f_r$ son linealmente independientes en todos los puntos $x \in X = Z(f_1,...,f_r)$, entonces X es una variedad diferenciable de dimensión $n - r$ (respectivamente una variedad compleja de dimensión (compleja) $n - r$). Claro, la conclusión es válida para funciones mucho más generales que los polinomios: si $f_1,...,f_r$ son funciones C^∞ en un abierto U de $\mathbb{R}^n$ (respectivamente funciones analíticas en un abierto U de $\mathbb{C}^n$), entonces

$$X = Z(f_1,...,f_r): = \{x \in U \mid f_1(x) = ... = f_r = 0\}$$

es una variedad diferenciable de clase C^∞ y dimensión $n - r$ (respectivamente una variedad compleja de dimensión $n - r$) si $d_x f_1,...,d_x f_r$ son linealmente independientes sobre $\mathbb{R}$ (respectivamente sobre $\mathbb{C}$) en todos los puntos de X. He aquí pues un contraste entre los puntos de vista que inicialmente inspiran al geómetra algebraico y al geómetra diferencial: mientras aquel se restringe a la consideración de polinomios, en principio sobre un cuerpo (y aún un anillo, como veremos) cualquiera, como funciones primordiales de su dominio, sin imponer ninguna restricción adicional, éste considera funciones mucho más generales, pero sujetas a condiciones locales de independencia que garanticen la lisitud de los objetos en cuestión. El territorio común visible desde esta perspectiva está formado entonces por los subconjuntos algebraicos *lisos* de $\mathbb{R}^n$ (ó $\mathbb{C}^n$), a los cuales se puede en principio aplicar, como así realmente se hace, cualquiera de las dos metodologías (o ambas a la vez). Entre ambas disciplinas existen muchos otros nexos, más o menos recónditos, pero la exploración de los mismos cae fuera del objeto de estas páginas.

El espíritu del geómetra algebraico clásico. Una buena porción de la filosofía que impulsa al geómetra algebraico al aceptar las anteriores definiciones (relativas a conjuntos algebraicos) se puede adivinar por su modo de tratar analíticamente, por ejemplo, las rectas del espacio. Veámoslo de un modo muy resumido. Sea Γ el conjunto de rectas de k^3 y sea $\ell_0 \in \Gamma$. Tomemos dos planos paralelos distintos π y π', no paralelos a ℓ_0. El subconjunto $\Gamma_0 \subseteq \Gamma$ formado por las rectas que no son paralelas a dichos planos está en correspondencia biyectiva con el producto $\pi \times \pi'$, asignando a cada recta $\ell \in \Gamma_0$ el par $(\ell \cap \pi, \ell \cap \pi')$. Tomando coordenadas afines en cada uno de los planos, hallamos que Γ_0 está en correspondencia biyectiva con $k^2 \times k^2 = k^4$, lo que nos da «coordenadas» para todas las rectas de Γ_0, que a su vez nos permiten tratarlas «analíticamente». Por ejemplo, la condición necesaria y suficiente a fin de que $\ell \in \Gamma_0$ corte a ℓ_0 es que los puntos ($\ell \cap \pi$, $\ell \cap \pi'$, $\ell_0 \cap \pi$, $\ell_0 \cap \pi'$) sean coplanarios, condición que es «algebraica» por cuanto se puede expresar por la anulación de un determinante de orden cuatro formado con las coordenadas (proyectivas) de estos puntos, el cual es un polinomio en dichas coordenadas, con coeficientes en k. Esto significa que las rectas ℓ que cortan a una recta ℓ_0 dada constituyen una hipersuperficie del espacio de todas las rectas. De hecho, haciendo las cuentas se ve que se trata de una hipercuádrica.

En este ejemplo es también manifiesto que si $k = \mathbb{R}$ (ó $k = \mathbb{C}$), entonces el procedimiento descrito muestra que las rectas del espacio tienen estructura de variedad diferenciable (compleja) de dimensión cuatro, puesto que las «coordenadas» dadas por un par de planos se expresan como polimonios en las dadas por otro par.

Funciones polinomiales. Sea X un conjunto algebraico y consideremos la aplicación

$$k[T_1,...,T_n] \to F(X,k)$$

que a cada polinomio q en las indeterminadas $T_1,...,T_n$ le hace corresponder la función $\overline{q}$ de X a valores en k obtenida por restricción de q a X, $\overline{q} = q|X$. Dicha aplicación es un homomorfismo de k-álgebras y su núcleo es un ideal I_C del anillo $k[T_1,...,T_n]$ que claramente contiene el ideal $(f_1,...f_r)$ generado por las «ecuaciones» que definen el conjunto X. Entonces $A(X): = k[T_1,...,T_n]/I_X$ es isomorfo al subanillo de $F(X,k)$ formado por las funciones de X a valores en k que se pueden obtener por restricción de una función polinómica. Los elementos de $A(X)$ se denominan *funciones polinomiales* de X. Es también costumbre representar el anillo $A(X)$ con la notación $k[X]$. Si ponemos $t_i = T_i|X$, es claro que $A(X) = k[t_1,...,t_n]$, de modo que $A(X)$ es una k-álgebra finitamente generada. Como los elementos de $A(X)$ son funciones, es también claro que $A(X)$ es reducida.

El teorema débil de los ceros de Hilbert. Este resultado es la piedra angular de esta sección. Su análogo en la sección anterior es la proposición (1.1), que ha sido la clave del teorema de representación. Incluimos, por su simplicidad conceptual, una adaptación de la demostración de Zariski-Samuel [1960] (vol. 2, lema de la página 165) a nuestro contexto.

2.1. *Sea k un cuerpo algebraicamente cerrado y A una k-álgebra finitamente generada. Si A es un cuerpo, entonces A tiene dimensión finita sobre k.*

Tomemos elementos $x_1,...,x_r \in A$ tales que $A = k[x_1,...,x_r]$. Procederemos por inducción respecto de r. Si $r = 0$, $A = k$ y el aserto es evidente. Supongamos pues que $r > 0$. Como A es un cuerpo, el cuerpo $\boldsymbol{k}' = \boldsymbol{k}(x_1)$, formado por las fracciones racionales en x_1 con coeficientes en $\boldsymbol{k}$, es un subcuerpo de A y $A = \boldsymbol{k}'[x_2,...,x_r]$. Por recurrencia podemos suponer demostrado que A tiene dimensión finita sobre $\boldsymbol{k}'$. Así pues será suficiente demostrar que $\boldsymbol{k}'$ tiene dimensión finita sobre $\boldsymbol{k}$.

A tal fin consideremos una indeterminada T y los homomorfismos

$$\upsilon_i: \boldsymbol{k}'[T] \to \boldsymbol{k}'[x_i] \ (2 \leq i \leq r)$$

tales que $\upsilon_i(T) = x_i$, $\upsilon_i|\boldsymbol{k}' = 1$. Como $\boldsymbol{k}'[x_i]$ tiene dimensión finita sobre $\boldsymbol{k}'$, mientras que $\boldsymbol{k}'[T]$ tiene dimensión infinita sobre el mismo cuerpo, $\mathbf{ker}(\upsilon_i)$ es no nulo y por tanto existe un polinomio no nulo

$$f_i \in \boldsymbol{k}'[T]$$

tal que $f_i(x_i) = 0$. Sin pérdida de generalidad, podemos suponer que el coeficiente de grado máximo de f_i (sea n_i este grado) es la unidad. Además, podemos poner los restantes coeficientes con un denominador común $q \in \boldsymbol{k}[x_1]$, e incluso que este denominador es el mismo para todos los f_i. Multiplicando la relación $f_i(x_i) = 0$ por q^{n_i}, vemos que existen polinomios $g_i[T]$ tales que $g_i(qx_i) = 0$ y de modo que (1) g_i tiene grado n_i y su coeficiente de grado máximo es la unidad, y (2) los restantes coeficientes de g_i pertenecen a $\boldsymbol{k}[x_1]$.

Para ver que $\boldsymbol{k}'$ tiene dimensión finita sobre $\boldsymbol{k}$, sea υ: $\boldsymbol{k}[T] \to \boldsymbol{k}[x_1]$ el homeomorfismo tal que $\upsilon(T) = x_1$, $\upsilon| \boldsymbol{k} = 1$. Si $\mathbf{ker}(\upsilon) \neq 0$, digamos $\mathbf{ker}(\upsilon) = (f)$, $f \in \boldsymbol{k}[T]$ no nulo e irreducible, entonces la conclusión es clara, pues $\boldsymbol{k}[x_1] \simeq \boldsymbol{k}[T]/\mathbf{ker}(\upsilon) = \boldsymbol{k}[T]/(f)$ es un cuerpo de dimensión finita sobre $\boldsymbol{k}$ y *a fortiori* $\boldsymbol{k}' = \boldsymbol{k}[x_1]$.

Para terminar la demostración será suficiente ver que $\mathbf{ker}(\upsilon) = 0$ acarrea una contradicción. En efecto, en tal caso υ sería un isomorfismo $\boldsymbol{k}[T] \simeq \boldsymbol{k}[x_1]$. Consideremos un elemento cualquiera $z \in \boldsymbol{k}' = \boldsymbol{k}(x_1)$. Sabemos que $z = \phi(x_1, ..., x_r)$ para algún polimonio ϕ con coeficientes en $\boldsymbol{k}$. De la propiedad (2), párrafo anterior, se puede deducir sin dificultad que existe una potencia q^s del polinomio q allí definido, con el exponente s dependiente de z, tal que $q^s z$ es entero sobre $\boldsymbol{k}[x_1]$ y por tanto tal que $q^s z \in \boldsymbol{k}[x_1]$, pues $\boldsymbol{k}[x_1] \simeq \boldsymbol{k}[T]$ es íntegramente cerrado. Ello significa que cualquier $z \in \boldsymbol{k}(x_1)$ se puede escribir en la forma p/q^s, $p \in \boldsymbol{k}[x_1]$ (p y s dependientes de z, pero q es independiente del mismo), lo cual no es posible debido al isomorfismo $\boldsymbol{k}[T] \simeq \boldsymbol{k}[x_1]$ y a que $\boldsymbol{k}[T]$ no posee dicha propiedad. □

Como corolario tenemos:

2.2. *Sea* $\boldsymbol{k}$ *un cuerpo algebraicamente cerrado,* A *un álgebra finitamente generada sobre* $\boldsymbol{k}$ *y* $\boldsymbol{m}$ *un ideal maximal de* A*. Entonces el morfismo canónico* $\boldsymbol{k} \to A/\boldsymbol{m}$ *es un isomorfismo.*

En efecto, $A/\boldsymbol{m}$ es un álgebra finitamente generada sobre $\boldsymbol{k}$. Como $A/\boldsymbol{m}$ es un cuerpo, **2.1** nos permite inferir que $A/\boldsymbol{m}$ tiene dimensión finita sobre $\boldsymbol{k}$. Pero la única extensión finita de un cuerpo algebraicamente cerrado $\boldsymbol{k}$ es $\boldsymbol{k}$. □

Pondremos $\upsilon_m: A \to \boldsymbol{k}$ para denotar la composición de la proyección canónica $A \to A/\boldsymbol{m}$ con el isomorfismo $A/\boldsymbol{m} \cong \boldsymbol{k}$. Se comprueba sin dificultad que υ_m *es el único homomorfismo* $A \to \boldsymbol{k}$ *de* $\boldsymbol{k}$*-álgebras cuyo núcleo es* $\boldsymbol{m}$.

> The reader may need an effort of will to perceive mathematics as a tutor of our imagination.
>
> Manin [1981], p. xi

Reconstrucción de los puntos. Sea $\boldsymbol{k}$ un cuerpo algebraicamente cerrado y X un conjunto algeraico de $\boldsymbol{k}^n$. Sea $A = A(X)$ el anillo de funciones polinomiales sobre X e identifiquemos $\boldsymbol{k}$ al subanillo de las funciones constantes.

Dado un punto $x \in X$, la aplicación de evaluación en x, $\alpha \mapsto \alpha(x)$, es un homomorfismo $A \to \boldsymbol{k}$. Puesto que $\alpha(x) = \alpha(x')$ para todo $\alpha \in A$ implica $x = x'$ (basta tomar como α las funciones de coordenadas), podemos identificar X a un subconjunto de $\mathcal{X}(A) := Hom_{k\text{-álg}}(A,\boldsymbol{k})$, $X \subseteq \mathcal{X}(A)$. De este modo nos es permitido escribir

$$x(\alpha) = \alpha(x)$$

para todo $x \in X$ y $\alpha \in A$.

2.3. *Se verifica que* $X = \mathcal{X}(A)$.

En efecto, sea ξ: $A \to \boldsymbol{k}$ un homomorfismo de $\boldsymbol{k}$-álgebras. Pongamos $x_i = \xi(t_i)$ y $x = (x_1,...,x_n)$, donde $t_i = T_i|X$. Sea $q \in \boldsymbol{k}[T_1,...,T_n]$ y $\overline{q} = q|X$. Como $\overline{q} = q(t_1,...,t_n)$, $\xi(\overline{q}) = q(x_1,...,x_n)$ y por tanto $q(x_1,...,x_n) = 0$ para todo $q \in I_X$. Así pues $x \in X$. Por otra parte,

$$x(\overline{q}) = \overline{q}(x_1,...,x_n) = q(x_1,...,x_n) = \xi(\overline{q}),$$

de donde $\xi = x$. □

Puntos e ideales maximales. Ahora si $x \in X = \mathcal{X}(A)$, $\boldsymbol{p}_x := ker(x) = \{a \in A | a(x) = 0\}$ es un ideal maximal de A, pues

$$A/\boldsymbol{p}_x \cong Im(x) = \boldsymbol{k}.$$

Es inmediato verificar que

$$\boldsymbol{p}_x = (t_1 - x_1,...,t_n - x_n)$$

2.4. *La aplicación* $x \mapsto \boldsymbol{p}_x$ *establece una correspondencia biyectiva entre los puntos de* X *y el conjunto* $\mathcal{M}(A)$ *de los ideales maximales de* A*. La correspondencia inversa es* $\boldsymbol{m} \mapsto \upsilon_m$.

Es claro que $x = \upsilon_{px}$, ya que x y υ_{px} tienen ambos núcleo $\boldsymbol{p}_x$. Por otra parte

$$\boldsymbol{p}_{\upsilon_m} = ker(\upsilon_m) = \boldsymbol{m}. \ \square$$

Aplicaciones algebraicas y homomorfismos de anillos. Sea $\boldsymbol{k}$ un anillo. Sean $X \subseteq \boldsymbol{k}^n$ y $X' \subseteq \boldsymbol{k}^m$ conjuntos algebraicos y f: $X \to X'$ una aplicación. Diremos que f es algebraica, o que es una aplicación polinomial de conjuntos algebraicos, si se pueden hallar polinomios $q_1,\dots,q_m$ en las indeterminadas $T_1,\dots,T_n$ tales que $f(x_1,\dots,x_n) = (q_1(x_1,\dots,x_n),\dots,q_m(x_1,\dots,x_n))$ para todo punto $x = (x_1,\dots,x_n)$ de X. Cuando $\boldsymbol{k}$ es algebraicamente cerrado, las aplicaciones polinomiales también se denominan *morfismos* de conjuntos algebraicos.

Supongamos ahora que $\boldsymbol{k}$ es un cuerpo algebraicamente cerrado. Sea $f\colon X \to X'$ un morfismo de conjuntos algebraicos. Entonces la aplicación $f^*\colon A(X') \to F(X,\boldsymbol{k})$, $f^*(\alpha) = \alpha \circ f$, es un homomorfismo de $\boldsymbol{k}$-álgebras y es inmediato verificar que de hecho $f^*(A(X')) \subseteq A(X)$. Así pues f induce un homomorfismo de $\boldsymbol{k}$-álgebras $f^*\colon A(X') \to A(X)$.

Sea $\phi = f^*$. Entonces $\phi^*\colon \mathcal{X}(A) \to \mathcal{X}(A')$, $\phi^*(x) = x \circ \phi$, coincide con f cuando identificamos X con $\mathcal{X}(A)$ y X' con $\mathcal{X}(A')$. Omitimos la demostración puesto que es calcada de la que se ha dado para el caso de los anillo de Boole. En todo caso tenemos:

2.5. *La aplicación $f \mapsto \phi$ establece una correspondencia biyectiva entre el conjunto de morfismos $f\colon X \to X'$ de conjuntos algebraicos y el conjunto de homomorfismos de $\boldsymbol{k}$-álgebras $\phi\colon A(X') \to A(X)$.*

Es de notar que la relación $f(x) = x'$ es equivalente a la relación $\phi^{-1}(\boldsymbol{p}_x) = \boldsymbol{p}_{x}'$, de modo que, en particular, ϕ^{-1} transforma ideales principales de $A(X')$ en ideales maximales de $A(X)$.

3. SOBRE FUNCIONES CONTINUAS EN ESPACIOS COMPACTOS

> *Our purpose is to show... how natural and useful the Banach algebra setting can be in harmonic analysis.*
>
> Y. Katznelson [1968], p. 194.

> *These features, as well as many applications, gave the book* [S. Banach, *Théorie des opérations linéaires,* Warszawa 1932] *a great appeal, and it had on Functional Analysis the same impact that van der Waerden's book* [Moderne Algebra] *had on Algebra two years earlier.*
>
> J. Dieudonné [1981], p. 142.

Si X es un espacio topológico, $A = \mathcal{C}^0(X,\mathbb{C})$, el anillo de funciones continuas de X a valores complejos, es una $\mathbb{C}$-álgebra. En esta sección nos ocuparemos, entre otros, del problema de reproducir X a partir de A, tratando de poner de manifiesto las analogías con los casos estudiados en las secciones anteriores. El resultado clave para este fin es el teorema de Mazur-Gelfand (3.4) y su corolario (3.5), cuyo papel es análogo en el presente contexto al del teorema débil de los ceros de Hilbert.

Algebras topológicas. Si X es un espacio compacto Hausdorff y ponemos, para todo $\alpha \in A$,

$$\|\alpha\|_\infty = \sup_{x\in X} |\alpha(x)|,$$

entonces $\|\cdot\| = \|\cdot\|_\infty$ dota a A de una estructura de *álgebra de Banach* (conmutativa y unitaria), en el sentido de que $\|\cdot\|$ es una norma para A respecto de la cual A es completo (o sea, A es un espacio de Banach respecto de $\|\cdot\|$) y tal que

$$\|\alpha\beta\| \le \|\alpha\|\,\|\beta\|\,.$$

Recordemos que los axiomas para una *norma* (en un espacio vectorial complejo A) son los siguientes: *(positividad)* $\|\alpha\| \ge 0$ y $\|\alpha\| = 0$ sólo si $\alpha = 0$; *(homogeneidad)* $\|\lambda\alpha\| = |\lambda|\|\alpha\|$ para todo $\lambda \in \mathbb{C}$, $\alpha \in A$; y *(desigualdad triangular)* $\|\alpha + \beta\| \le \|\alpha\| + \|\beta\|$. La condición de completitud es que toda sucesión de Cauchy (respecto de la norma) sea convergente en A.

Usaremos más abajo que si *A es un espacio de Banach complejo y $\alpha \in A$ un elemento no nulo, entonces existe una aplicación lineal continua $\omega\colon A \to \mathbb{C}$ tal que $\omega(\alpha) \ne 0$.* Es esta proposión una consecuencia directa del teorema de Hahn-Banach sobre extensión de funcionales (véase Robertson-Robertson [1980], p. 29).

Un álgebra normada A (no necesariamente conmutativa), con la topología dada por la norma, es un *álgebra topológica,* esto es, la suma y el producto son aplicaciones continuas. Si A es unitaria, entonces A tiene además *inverso continuo,* lo que quiere decir que el grupo A^* de elementos invertibles de A es abierto en A y que la aplicación $A^* \to A^*$, $\alpha \mapsto \alpha^{-1}$, es continua.

Esquematicemos la demostración de los dos últimos asertos. En primer lugar, si $\varepsilon \in A$ y $\|\varepsilon\| < 1$, entonces la serie

$$\sigma = 1 + \varepsilon + \varepsilon^2 + \varepsilon^3 + \dots$$

es convergente en A y es inmediato que $(1-\varepsilon)\sigma = 1$. Esto prueba que los elementos de la bola de radio 1 con centro en la unidad son invertibles. A continuación tomemos dos elementos $\alpha,\beta \in A$ y supongamos que α es invertible y que $\|\alpha - \beta\| < \|\alpha^{-1}\|^{-1}$. Entonces

$$\|1 - \alpha^{-1}\beta\| = \|\alpha^{-1}(\alpha - \beta)\| \le \|\alpha^{-1}\|\|\alpha - \beta\| < 1$$

y por tanto

$$\alpha^{-1}\beta = 1 - (1 - \alpha^{-1}\beta)$$

es invertible. Ello prueba que β es invertible y que

3.1. $$\beta^{-1} = \alpha^{-1} \sum_{j\ge 0} (1 - \alpha^{-1}\beta)^j$$

Vemos pues que la bola de centro α y radio $\|\alpha^{-1}\|^{-1}$ está formada por elementos invertibles. Finalmente, de la última igualdad resulta que

$$\beta^{-1} - \alpha^{-1} = \sum_{j\geq 1} (1 - \alpha^{-1}\beta)^j\,\alpha^{-1}$$

de donde

$$\|\beta^{-1} - \alpha^{-1}\| \leq \sum_{j\geq 1} \|\alpha^{-1}\|^{j+1}\|\alpha - \beta\|^j =$$
$$= \|\alpha^{-1}\|^2\|\alpha - \beta\| \sum_{j\geq 0} \|\alpha^{-1}\|^j\|\alpha - \beta\|^j$$

Si ahora tomamos $\|\alpha - \beta\| < \frac{1}{2}\|\alpha^{-1}\|^{-1}$, entonces el segundo factor de la última expresión es inferior a 2, de donde $\|\beta^{-1} - \alpha^{-1}\| < 2\|\alpha^{-1}\|^2\|\alpha - \beta\|$.

To think... means to calculate with critical awareness.

Manin [1981], p. xi

Espectro de un elemento de un álgebra topológica. Para motivar esta definición, consideremos primero el álgebra A de endomorfismos de un espacio complejo E de dimensión finita. Dado $\alpha \in A$, $\lambda I - \alpha$ es no invertible si y sólo si $\ker(\lambda I - \alpha) \neq 0$, es decir, si y sólo si λ es un valor propio de α. Si E es un espacio de Banach complejo, y A es el álgebra de sus operadores (endomorfismos continuos), entonces dado $\alpha \in A$ ocurre que $\lambda I - \alpha$ es no invertible si y sólo si se verifica al menos una de las dos condiciones siguientes: (a) el núcleo de $\lambda I - \alpha$ es no nulo, lo que equivale a que λ sea un valor propio de α, ó (b) la imagen de $\lambda I - \alpha$ no es todo E. En todo caso, se define el espectro de α, $E\alpha$, como el conjunto de los $\lambda \in \mathbb{C}$ tales que $\lambda I - \alpha$ es no invertible. Esta noción fue introducida por Hilbert, escogiendo el término por la analogía, en principio superficial, entre los espectros de emisión de los átomos y los conjuntos de valores propios de operadores conocidos. Esta analogía se convirtió en una sólida teoría en manos de los fundadores de la mecánica cuántica teórica, especialmente Heissenberg y Schrödinger, y en una sólida teoría tras el esfuerzo fundamental de von Neumann [1955].

Es ahora claro que la noción de espectro es válida para los elementos de cualquier álgebra. Pero como esta noción sólo es realmente interesante en el caso de ciertas álgebras topológicas, nos restringimos a este caso para una definición formal. Si A es una $\mathbb{C}$-álgebra unitaria de Banach, y $\alpha \in A$, definimos el *espectro* de α, $E\alpha$, o $E(\alpha)$, como el conjunto de los $\lambda \in \mathbb{C}$ tales que $\lambda - \alpha$ es no invertible en A. Nótese que la misma definición para el álgebra A de funciones polinomiales de una variedad afín es irrelevante, por cuanto $Ea = \boldsymbol{k}$ para todo $\alpha \in A$ no constante.

Resolvente de un elemento. La aplicación R_α: $\mathbb{C} - E\alpha \to A^*$, $\lambda \to (\lambda - \alpha)^{-1}$, se denomina la resolvente de α.

3.2. *El conjunto $\mathbb{C} - E\alpha$ es abierto en $\mathbb{C}$ y la aplicación R_α es analítica en todo $\mathbb{C} - E\alpha$, es decir, $R_\alpha(\lambda)$ es derivable como función de λ para todo $\lambda \in \mathbb{C} - E\alpha$.*

La primera afirmación es inmediata. Para ver la segunda, sea $\lambda_0 \in \mathbb{C} - E\alpha$ y sea λ próximo a λ_0. Entonces $\lambda - \alpha$ es también invertible y de

$$(\lambda - \alpha) - (\lambda_0 - \alpha) = \lambda - \lambda_0$$

deducimos, tras multiplicar por $R(\lambda_0)R(\lambda)$ y efectuar algunas operaciones sencillas, que

$$\frac{R(\lambda) - R(\lambda_0)}{\lambda - \lambda_0} = -R(\lambda_0)R(\lambda),$$

donde $R = R_\alpha$. Tomando límite cuando $\lambda \to \lambda_0$, y teniendo en cuenta que $R(\lambda)$ es continua, vemos que $R(\lambda)$ es derivable en λ_0, con derivada $-R(\lambda_0)^2$. □

Nótese que $R(\lambda)$ se puede desarrollar como una serie de potencias en $\lambda - \lambda_0$, con coeficientes en A y convergente en norma para λ en un entorno de λ_0:

$$R(\lambda) = (\lambda - \alpha)^{-1} = (\lambda_0 - \alpha)^{-1} \sum_{j\geq 0} (1 - (\lambda_0 - \alpha)^{-1}(\lambda - \lambda_0 + \lambda_0 - \alpha))^j =$$
$$= -\sum_{j\geq 0} (\lambda_0 - \alpha)^{-j-1}(\lambda - \lambda_0)^j,$$

donde en el segundo paso hemos usado la fórmula (3.1).

Como corolarios tenemos:

3.3. *Para todo $\alpha \in A$, $\mathbb{C} - E\alpha \neq \mathbb{C}$, es decir, $E\alpha$ es no vacío.*

Veamos primero que $R_\alpha(\lambda)$ es acotada. Si $|\lambda| \geq 2\|\alpha\|$,

$$\|R_\alpha(\lambda)\| \leq \frac{2}{|\lambda|},$$

como se deduce sin dificultad usando la relación

$$R_\alpha(\lambda) = \frac{1}{\lambda}(1 - \alpha/\lambda)^{-1},$$

válida para todo $\lambda \in \mathbb{C} - E\alpha$. Es decir, $R_\alpha(\lambda)$ tiende a cero cuando λ tiende a infinito, de donde el aserto.

Sea ahora ω: $A \to \mathbb{C}$ cualquier aplicación lineal continua y supongamos que $\mathbb{C} - E\alpha = \mathbb{C}$, es decir, que $E\alpha$ es vacío. Entonces $\omega(R_\alpha(\lambda))$ es una función analítica entera, es decir, definida en todo $\mathbb{C}$ (y con valores complejos). Además, es acotada, puesto que su valor tiende a cero cuando λ tiende a infinito. Por el teorema de Liouville, $\omega(R_\alpha(\lambda))$ es constante. Como ω es arbitraria, $R_\alpha(\lambda)$ es constante, lo cual es absurdo. □

Se define el *radio espectral* de $\alpha \in A$, $\rho(\alpha)$, como el supremo de los módulos $|\lambda|$, variando λ en $E\alpha$. Puesto que $\lambda - \alpha$ es invertible para $|\lambda| > ||\alpha||$, como se ha visto en la demostración anterior, resulta que

$$\rho(\alpha) \leq ||\alpha||$$

Vemos pues que $E\alpha$ es compacto, por ser cerrado y acotado.

Teorema de Gelfand-Mazur. Como hemos dicho ya, este teorema es análogo, en el contexto de las álgebras topológicas, al teorema débil de los ceros:

3.4. *Sea A como en el enunciado anterior y supongamos que A es un álgebra de división, esto es, en la que todo elemento no nulo tiene un inverso. Entonces* $A = \mathbb{C}$, *en el sentido que la inclusión de* $\mathbb{C}$ *en A es un isomorfismo.*

En efecto, dado α, existe un $\lambda \in \mathbb{C}$ tal que $\lambda - \alpha$ es no invertible. Como A es un álgebra de división, será $\alpha = \lambda$. □

El teorema anterior fue publicado por primera vez, sin demostración, por S. Mazur (1938). La demostración anterior es esencialmente debida a I. M. Gelfand (hacia 1939) y variaciones de la misma se pueden hallar en muchas fuentes, entre las que podemos destacar Gelfand-Raikov-Chilov [1964], § 4, Th. 2; Naimark [1972], p. 173; Katznelson [1976], p. 200; y Aupetit [1991], p. 39.

La consecuencia más importante para nuestros propósitos es el siguiente resultado:

3.5. *Sea A una* $\mathbb{C}$*-álgebra de Banach y* ***m*** *un ideal maximal de A. Entonces* $A/\boldsymbol{m} = \mathbb{C}$, *en el sentido que el homomorfismo natural* $\mathbb{C} \to A/\boldsymbol{m}$ *(obtenido por composición de la inclusión* $\mathbb{C} \hookrightarrow A$ *con la proyección canónica* $A \to A/\boldsymbol{m}$*) es un isomorfismo.*

Como $\boldsymbol{m}$ es cerrado (ello es una consecuencia de los resultados del primer epígrafe de esta sección), $A/\boldsymbol{m}$ es un álgebra de Banach con la norma del cociente. Siendo $A/\boldsymbol{m}$ es un cuerpo, el teorema de Gelfand-Mazur nos da que la inclusión de $\mathbb{C}$ en $A/\boldsymbol{m}$ es un isomorfismo. □

Pondremos υ_m para indicar la composición de la proyección canónica $A \to A/\boldsymbol{m}$ con el isomorfismo canónico $A/\boldsymbol{m} \cong \mathbb{C}$. Es claro que υ_m es el único morfismo de $\mathbb{C}$-álgebras cuyo núcleo es $\boldsymbol{m}$.

Puntos e ideales maximales. Sea X un espacio topológico compacto y A el anillo de las funciones continuas de X a valores complejos. Como hemos ya dicho, A es un álgebra de Banach con la norma

$$||\alpha|| = \sup_{x \in X} |\alpha(x)|$$

Dado un punto $x \in X$, la aplicación de evaluación $\alpha \mapsto \alpha(x)$ es un homomorfismo de $\mathbb{C}$-álgebras (automáticamente continuo) y es sabido que $\alpha(x) = \alpha(x')$ para todo α implica $x = x'$. Así pues podemos identificar X a un subconjunto de $\mathcal{X}(A) := Hom_{\mathbb{C}\text{-álg}}(A, \mathbb{C})$.

Por otra parte, para cada $\xi \in \mathcal{X}(A)$, $\boldsymbol{p}_\xi := ker(\xi)$ es un ideal maximal de A. Obsérvese que si $x \in X$, entonces $\boldsymbol{p}_x$ está formado por las funciones continuas nulas en x.

3.6. *Se verifica que* $X = \mathcal{X}(A)$. *Además, la correspondencia* $x \mapsto \boldsymbol{p}_x$ *es una biyección entre X y el conjunto* $\mathcal{M}(X)$ *de los ideales maximales de A, siendo* $\boldsymbol{m} \mapsto \upsilon_m$ *la correspondencia inversa.*

Sólo es necesario demostrar el primer aserto, ya que los demás se prueban como en la sección anterior. Sea $\xi \in \mathcal{X}(A)$. Entonces $\boldsymbol{m} = \boldsymbol{p}_\xi$ es un ideal maximal de A. Si pudiésemos hallar un punto $x \in X$ tal que $\boldsymbol{p}_x \subseteq \boldsymbol{m}$, entonces sería $\boldsymbol{p}_x = \boldsymbol{m}$, de lo cual se deduce sin dificultad que $\xi = x$.

Notemos que si $\boldsymbol{m}_x \not\subseteq \boldsymbol{m}$, entonces existe una función $\alpha \in \boldsymbol{m}$ tal que $\alpha(x) \neq 0$ y por tanto tal que α es no nula en un entorno de x. Si la conclusión que queremos establecer fuese falsa, existiría, por compacidad de X, un recubrimiento por abiertos $U_1, \ldots, U_r$ y funciones continuas $\alpha_1, \ldots, \alpha_r \in \boldsymbol{m}$ tales que α_i es no nula en todo punto de U_i. Entonces la función $\beta = \Sigma|\alpha_i|^2$ es una función continua que no se anula en ningún punto de X y $\beta \in \boldsymbol{m}$, pues $|\alpha_i|^2 = \alpha_i\overline{\alpha}_i \in \boldsymbol{m}$. Pero entonces β es invertible en A y esto es una contradicción. □

A un homomorfismo de $\mathbb{C}$-álgebras de A en $\mathbb{C}$ se le denomia también un *carácter* del álgebra A. Es por ello que el conjunto $\mathcal{X}(A) = Hom_{\mathbb{C}\text{-álg}}(A, \mathbb{C})$ se denomina el *espacio de caracteres* de A. Es un subconjunto del espacio A' de todas las aplicaciones lineales continuas de A en $\mathbb{C}$.

The spectrum of a quantity is the set of all values that the quantity can take.

Manin [1981], p. 36

La teoría de Gelfand. Sea A un álgebra de Banach conmutativa. Pongamos $X = \mathcal{X}(A)$ para denotar su espacio de caracteres. Para cada $\alpha \in A$, podemos definir una función $\hat{\alpha} \in F(X, \mathbb{C})$ del mismo modo que en las secciones anteriores:

$$\hat{\alpha}(x) = x(\alpha)$$

La aplicación $\gamma: A \to F(X, \mathbb{C})$, $\alpha \mapsto \hat{\alpha}$, se denomina la *representación de Gelfand* de A.

Para estudiar esta representación en algunos casos, notemos primero que

3.7. *Se verifica la igualdad*

$$\{\hat{\alpha}(x) \,/\, x \in X\} = E\alpha$$

En particular resulta que $\rho(\alpha) = ||\hat{\alpha}||_\infty$. *Como* $\rho(\alpha) \leq ||\alpha||$, *la transformación de Gelfand* $\alpha \mapsto \hat{\alpha}$ *es continua.*

En efecto, si $\lambda - \alpha$ no es invertible, existe un ideal maximal $\boldsymbol{m}$ tal que $\lambda - \alpha \in \boldsymbol{m}$. Pero $\boldsymbol{m} = \boldsymbol{p}_x$, para algún $x \in X$, lo cual significa que $x(\lambda - \alpha) = 0$, es decir, que $\lambda = x(\alpha) = \hat{\alpha}(x)$. Recíprocamente, $x(\alpha) - \alpha \in \ker(x) = \boldsymbol{p}_x$ y por tanto $x(\alpha) - \alpha$ no puede ser invertible. □

Esta proposición nos muestra que X es un *espacio espectral* para A, en el sentido que los elementos de A se representan como funciones complejas de X y ello de modo tal que la imagen de la función $\hat{\alpha}$ coincide con el espectro de α. Nótese que $|x(\alpha)| \leq \rho(\alpha) \leq ||\alpha||$.

> ... if a space under study happens to be either a Banach algebra, or the dual space of one, keeping this fact in mind usually pays dividens.
>
> Katznelson [1968], p. 194

Teoremas Tauberianos. Es éste el título del libro en el que Norbert Wiener publicó su demostración, bastante complicada, según el cual *si* $\alpha: \mathbb{R} \to \mathbb{C}$, *es una función continua no nula en todos los puntos que coincide con la suma de una serie trigonométrica* $\sum_{n\in Z} a_n e^{int}$ *absolutamente convergente, entonces la función inversa* $1/\alpha$ *tiene la misma propiedad.*

En 1940 I. M. Gelfand dio con una demostración sencilla y natural del mismo, y también de un teorema más general de P. Lévy. Veamos las ideas en que se basa su demostración.

En primer lugar, sea A un álgebra de Banach conmutativa y unitaria y α un elemento de A. Dado cualquier polinomio $q \in \mathbb{C}[T]$, es claro que podemos substituir T por α en q, obteniendo un elemento $q(\alpha) \in A$. Puesto que $\widehat{q(\alpha)} = q(\hat{\alpha})$, es claro por (3.7) que $E(q(\alpha)) = q(E\alpha)$. En particular resulta que *si q no se anula en $E\alpha$, entonces $q(\alpha)$ es invertible en A*: si $q = (T-\lambda_1)...(T-\lambda_r)$ y $\lambda_i \notin E\alpha$, entonces los factores $\alpha - \lambda_i$ son invertibles en A. De este modo vemos que se puede definir $f(\alpha)$ sin ambigüedad para cualquier función racional $f \in \mathbb{C}(T)$ cuyo denominador no tenga ceros en $E\alpha$.

Para demostrar el teorema de Wiener será pues suficiente ver que el espectro de una serie trigonométrica absolutamente convergente no puede contener 0 si ella misma no se anula en ningún punto.

A tal fin, sea W el álgebra de las series trigonométricas $\alpha(t) = \sum_{n\in Z} a_n e^{int}$ a valores complejos y que son absolutamente convergentes en $\mathbb{R}$: es un álgebra de Banach (conmutativa y unitaria) con la norma

$$\|\alpha\| = \sum_{n\in Z} |a_n|$$

Para cada $x \in [0,2\pi)$, la aplicación $\alpha \mapsto \alpha(x)$ es un carácter de W (que seguiremos denotando x) y como consecuencia el intervalo $[0,2\pi)$ se puede identificar a un subconjunto del espacio espectral $X = X(W)$. Recíprocamente, si ξ es un carácter de W, entonces $\xi = x$ para algún $x \in [0,2\pi)$ (necesariamente único). En efecto, las relaciones

$$\xi(e^{it})\,\xi(e^{-it}) = 1,\ |\xi(e^{it})| \leq \|e^{it}\| = 1 \text{ y } |\xi(e^{-it})| \leq \|e^{-it}\| = 1$$

prueban que existe un único $x \in [0,2\pi)$ tal que

$$\xi(e^{it}) = e^{ix}$$

y es entonces fácil ver que $\xi = x$

Habiendo identificado el espacio espectral de W, es ahora claro que si $\alpha \in W$ no se anula en ningún punto, entonces $0 \notin E\alpha$ y por consiguiente que α es invertible en W.

Observación. Gelfand se dio cuenta en seguida que la expresión $f(\alpha)$ ($\alpha \in A$, A un álgebra de Banach conmutativa y unitaria) tiene sentido para funciones más generales que las racionales que no tienen polos en $E\alpha$. El secreto es la fórmula de Cauchy de la teoría elemental de funciones analíticas. El punto está en que, como es fácil ver, para funciones racionales sin polos en $E\alpha$ vale la fórmula

$$f(\alpha) = \frac{1}{2\pi i}\int_\gamma \frac{f(\lambda)d\lambda}{\lambda - \alpha},$$

siendo γ cualquier camino liso y simplemente cerrado que contiene a $E\alpha$ en su interior. Pero ahora es claro que esta fórmula tiene sentido para cualquier función analítica en un abierto que contiene a $E\alpha$. Con ello hemos esbozado la demostración de la generalización de Lévy del teorema de Wiener:

3.8. (Wiener-Lévy) *Sea $\alpha \in W$ y se f una función holomorfa en un entorno de $E\alpha$. Entonces $f(\alpha) \in W$.* □

Otro ejemplo interesante es el álgebra de Banach $A = A(K)$ de las funciones continuas en un compacto K de $\mathbb{C}$ y que son holomorfas en el interior de K (con la norma del supremo). Es claro que K se identifica a un subconjunto del espacio espectral de $X = X(A)$, identificando $x \in K$ al homomorfismo de evaluación $\alpha \mapsto \alpha(x)$. Veamos que $K = X$. En efecto, sea $\xi \in X$ y sea $x = \xi(i)$, donde i es la función de inclusión de K en $\mathbb{C}$. Si fuese $x \notin K$, la función β definida por la relación

$$\beta(z) = \frac{1}{z - x}$$

pertenecería a A, lo cual es imposible, ya que $1 = \beta(i - x)$ y $\xi((i - x)\beta) = 0$. Así pues ha de ser $x \in K$. Es ahora claro que ξ y x coinciden sobre los polinomios. Por tanto coinciden sobre límites uniformes de polinomios, de lo cual se puede inferir que $\xi = x$.

Topología de Gelfand. Por otra parte, es natural preguntarse si la norma de A inducirá de modo natural alguna topología en X. Puesto que

$$x(\alpha)| \leq \rho(\alpha) \leq \|\alpha\|,$$

como se ha hecho notar al final del epígrafe sobre la teoría de Gelfand, vemos que todo $x \in X$ es un elemento del espacio A' de las aplicaciones lineales continuas de

A en $\mathbb{C}$ (espacio dual de A) y que por tanto el espacio espectral X heredará cualquier topología de A'. Ahora bien, A' viene dotado de dos topología naturales.

Por ser un espacio de aplicaciones lineales continuas, A' viene provisto de una norma,

$$\|\omega\| = \sup_{\|\alpha\|=1} |\omega(\alpha)|$$

Se tiene entonces que

$$|w(\alpha)| \leq \|w\| \cdot \|\alpha\|$$

para todo $\alpha \in A$, y que $\|w\|$ es la mínima constante real que tiene esta propiedad. Por ejemplo, los elementos $x \in X$ tienen norma 1, por las desigualdades del párrafo anterior, de modo que X está contenido en la bola unidad de la norma de A'.

La segunda topología, más estrechamente relacionada con las propiedades algebraicas de A, es la *débil* (weal-star). Es la topología mínima para la cual los elementos de A dan aplicaciones (lineales) continuas de A' en $\mathbb{C}$, vía el acoplamiento natural $A \times A' \to \mathbb{C}$. A esta topología la denominaremos *topología espectral* o *topología de Gelfand* del espacio espectral $X(A)$.

Para terminar la sección, refiramos el *problema de la corona.* Este problema hace referencia a un abierto U de $\mathbb{C}$, al cual le asociamos el álgebra de Banach $H^\infty(U)$ de las funciones que son holomorfas y acotadas en U. Como en ocasiones anteriores, podemos sumergir U en el espacio espectral X de $H^\infty(U)$. El problema de la corona consiste en determinar si U es denso en X, según la topología de Gelfand, y permanece abierto en general, aunque se conoce que la respuesta es afirmativa (L. Carleson), para un disco (véase Aupetit [1991] para más detalles y referencias).

4. SOBRE LA GEOMETRIZACION DEL ALGEBRA

Several decades had to lapse before the rise of the theory of topological, differentiable and complex manifolds, the general theory of fields, the theory of ideals in sufficiently general rings, and only then it became possible to construct algebraic geometry on the basis of the principles of set-theoretic mathematics. [...]. The basis for this rebuilding of algebraic geometry was algebra.

Shafarevich, preface to *Basic Algebraic Geometry,* Grundlehren 213, Springer 1974

En la sección anterior hemos visto que para todo espacio topológico compacto Hausdorff X existe una biyección natural entre X y el espacio espectral del álgebra $C^0(X,\mathbb{C})$. No es difícil ver que esta biyección es un homeomorfismo, a condición de dotar a dicho espacio espectral de la topología de Gelfand. Recordemos que la topología de Gelfand era la mínima para la cual las funciones $\hat{\alpha}$ son continuas.

Fenómenos parecidos ocurrían para conjuntos algebraicos, aunque hasta este momento no los hemos considerado más que como conjuntos, al no haber detectado todavía ninguna estructura topológica natural en los mismos. El ojetivo de esta sección es mostrar que los conjuntos alegraicos poseen efectivamente una topología natural y extraer de este hecho algunas consecuencias.

Topología de Zariski. Sea k un cuerpo algebraicamente cerrado y sea $X \subseteq k^n$ un conjunto algebraico. La *topología de Zariski* de X es la topología cuyos cerrados vienen dados por la siguiente proposición:

4.1. *Los conjuntos algebraicos contenidos en X forman una familia de cerrados para X.*

Es suficiente ver que la unión de dos conjuntos algebraicos es un conjunto algebraico y que la intersección de una familia arbitraria de conjuntos algebraicos es también un conjunto algebraico. El primer aserto es claro, dado que se verifica la igualdad.

$$Z(f_1,...,f_r) \cup Z(g_1,...,g_s) = Z(f_1g_1,...,F_1g_s,...,f_rg_1,...,f_rg_s).$$

El segundo aserto es algo más delicado. Consideremos una familia $X_i = Z(f_1^i,...,f_{ri}^i)$, $i \in I$. La intersección de los Z_i es el conjunto donde se anulan simultáneamente todos los polimonios f_j^i, $i \in I$, $1 \leq j \leq r_i$. El punto está, pues, en ver que *este conjunto se puede obtener como anulación de un número finito de polinomios.* Pero esto es una consecuencia del teorema de la base de Hilbert. En efecto, si consideramos el ideal J de $k[T_1,...,T_n]$ generado por los polimonios f_j^i ($i \in I$, $1 \leq j \leq r_i$), dicho teorema garantiza que J es finitamente generado, digamos $J = (h_1,...,h_t)$, y por tanto $\bigcap_{i\in I} X_i = Z(h_1,...,h_t)$. □

Es inmediato verificar que la topología de Zariski es consistente con las inclusiones, en el sentido que si $X \subseteq X'$, X y X' conjuntos algebraicos, entonces la topología de Zariski de X' induce en X la topología de Zariski de X.

Nótese también que los cerrados propios de la topología de Zariski de k son los conjuntos finitos. Ello es así porque un polinomio no nulo de grado n en una indeterminada T admite a lo más n raíces distintas, y a que si $t_1,...,t_r \in k$ entonces $f = (T-t_1)...(T-t_r)$ se anula precisamente en $t_1,...,t_r$, $Z(f) = \{t_1,...,t_r\}$. En lo sucesivo k será dotado de esta topología, a la que podemos denominar *cofinita.*

Ahora dado un conjunto algebraico $X \subseteq k^n$, hemos visto que X se identifica con el conjunto $\hat{\alpha}(A)$, donde A es el álgebra de funciones polinomiales de X. Se plantea la cuestión de reconstruir la topología de Zariski de X a partir del álgebra $A(X)$. Puesto que en k tenemos la topología cofinita, podemos pensar, como en la teoría de Gelfand, en la *topología espectral,* esto es, la mínima topología para la cual las funciones de A son continuas.

4.2. *Si X es un conjunto algebraico con álgebra de funciones polinomiales A, la topología de Zariski de X coincide, vía la identificación de X con X(A), con la topología espectral.*

Sea $Z = Z(g_1,...,g_s)$ un cerrado de Zariski de X. Queremos ver que Z es un cerrado espectral. Ahora bien, puesto que $Z = Z(g_1) \cap ... \cap Z(g_s)$, será suficiente ver que si g es un polinomio, entonces $X \cap Z(g)$ es un cerrado espectral. Pero ello es claro, ya que si γ es la restricción de g a X, entonces

$$X \cap Z(g) = \gamma^{-1}(0),$$

que es un cerrado espectral por ser $\{0\}$ cerrado en $\boldsymbol{k}$ y $\gamma \in A$.

Inversamente, queremos ver que un cerrado espectral es un cerrado de Zariski. Puesto que la familia de cerrados de la topología espectral es la generada por las imágenes inversas por elementos de A de subconjuntos finitos de $\boldsymbol{k}$, es suficiente ver que si $\alpha \in A$ y $t \in \boldsymbol{k}$, entonces $\alpha^{-1}(t)$ es un cerrado de Zariski. Pero ello es también claro, ya que si α es un polinomio cuya restricción a X es α, y $f = a - t$, entonces $\alpha^{-1}(t) = X \cap Z(f)$ como se comprueba sin dificultad. □

Caracterización de las álgebras finitamente generadas reducidas. El anillo de funciones polinomiales de un conjunto algebraico es una $\boldsymbol{k}$-álgebra finitamente generada reducida. Recíprocamente:

4.3. *Sea A una* $\boldsymbol{k}$*-álgebra finitamente generada y reducida. Entonces existe un conjunto algebraico X tal que A es isomorfa a A(X).*

En efecto, por ser A finitamente generada, existen elementos $t_1,...,t_n \in A$ tales que $A = \boldsymbol{k}[t_1,...,t_n]$. Sea ϕ: $\boldsymbol{k}[T_1,...,T_n] \to A$ el homomorfismo de $\boldsymbol{k}$-álgebras definido por las relaciones $\phi(T_i) = t_i$. Es claro que ϕ es epiyectivo. Sea $I = ker(\phi)$. Por el teorema de la base, existen polinomios $f_1,...,f_r$ tales que $I = (f_1,...,f_r)$. Sea $X = Z(f_1,...,f_r)$. Habremos terminado si vemos que $I_X = I$, ya que si ello es así, entonces $A \cong \boldsymbol{k}[T_1,...,T_n]/ker(\phi) \cong \boldsymbol{k}[T_1,...,T_n]/I \cong \boldsymbol{k}[T_1,...,T_n]/I_X \cong A(X)$.

Puesto que la inclusión $I \subseteq I_X$ es evidente, bastará ver si f es un polinomio nulo en $X = Z(f_1,...,f_r)$, entonces $f \in I$.

A tal fin, consideremos una indeterminada auxiliar T_0 y formemos (éste es el artificio de Rabinowitz) el conjunto algebraico $Y = Z(1 - fT_0 f_1,...,f_r)$ de $\boldsymbol{k}^{n+1}$. Puesto que por hipótesis f es nulo en los puntos donde se anulan todos los f_i, es claro que Y es vacío. Pero sabemos que ello implica, como una consecuencia inmediata del teorema débil de los ceros, que el ideal $(1 - fT_0 f_1,...,f_r)$ de $\boldsymbol{k}[T_0,...,T_n]$ es todo $\boldsymbol{k}[T_0,...,T_n]$. En particular existen $g_0,...,g_n \in \boldsymbol{k}[T_0,...,T_n]$ tales que

$$1 = g_0(1 - fT_0)g_1 \cdot f_1 + ... + g_r \cdot f_r$$

Sustituyendo T_0 por $1/f$ en esta identidad, hallamos que existe un entero positivo m y polinomios $h_1,...,h_n \in \boldsymbol{k}[T_1,...,T_n]$ tales que

$$f^m = h_1 \cdot f_1 + ... + h_r \cdot f_r$$

Aplicando ϕ a ambos miembros, hallamos que $\phi(f)^m = 0$. Pero por hipótesis A es reducida, de donde $\phi(f) = 0$. Pero ello significa que $f \in ker(\phi) = I$. □

Teorema de los ceros. En la demostración anterior se ha visto que si $f, f_1,...,f_r \in \boldsymbol{k}[T_1,...,T_n]$ y f es nulo sobre $X = Z(f_1,...,f_r)$, entonces existe un entero positivo m tal que $f^m \in (f_1,...,f_r)$. Este hecho es el *teorema fuerte de los ceros de Hilbert.*

Una consecuencia sencilla de este teorema es que *en una* $\boldsymbol{k}$*-álgebra finitamente generada la intersección de sus ideales maximales coincide con el conjunto de los elementos nihilpotentes.* En particular, *si A es finitamente generada sobre* $\boldsymbol{k}$ *y reducida, la intersección de sus ideales maximales es* $\{0\}$.

Señalemos aquí que cuando el cuerpo $\boldsymbol{k}$ no es algebraicamente cerrado existen otras formas del teorema de los ceros, más elaboradas, para las cuales el lector interesado puede consultar McKenna [1980] y Colliot-Thélène [1982]. Para generalizaciones del teorema de los ceros al contexto diferenciable, véase Bochnak [1973]. Recordemos aquí el caso más elemental. Supongamos que U es un abierto de $\mathbb{R}^n$ y que $f_1,...,f_r$ son funciones de clase $\mathcal{C}^\infty$ tales que $d_x f_1,...,d_x f_r$ son linealmente independientes en un punto $x \in X = Z(f_1,...,f_r)$. Sea f una función de clase $\mathcal{C}^\infty$ definida en un entorno V de x y tal que f es nula en $V \cap X$. Entonces existe un entorno $V' \subseteq V$ de x tal que f pertenece al ideal de $\mathcal{C}^\infty(V')$ generado por las restricciones de las f_i a V'.

Geometrización de k-álgebras finitamente generadas reducidas. Ahora nos damos cuenta de que si $X \subseteq \boldsymbol{k}^n$ es un conjunto algebraico, $A(X)$ es algo más que una $\boldsymbol{k}$-álgebra finitamente generada reducida, ya que *viene dotada de un sistema distinguido de generadores.* En correspondencia con ello, X es algo más que un espacio topológico, ya que *viene presentado como un subespacio de* $\boldsymbol{k}^n$. No obstante, el tipo de álgebras que pueden ocurrir como álgebras de funciones polinomiales de conjuntos algebraicos ha quedado caracterizada, en el teorema anterior, en términos que no dependen de tales conjuntos.

Es, pues, natural considerar álgebras finitamente generadas sobre $\boldsymbol{k}$ como objetos primarios y asignarles, de un modo intrínseco, una geometría a cada una de ellas. Si A es una tal álgebra, le podemos asociar su espacio espectral $\mathcal{X} = \mathcal{X}(A)$, dotado de la topología espectral, a la cual la podemos también llamar, apropiadamente por (4.2), topología de Zariski. De este modo, los elementos $\alpha \in A$ se representan como funciones $\hat{\alpha}$ sobre $\mathcal{X}$, a las que podemos llamar *funciones regulares* sobre $\mathcal{X}$. Nótese que si $\hat{\alpha} = 0$, entonces ha de ser $\alpha = 0$, ya que $x(\alpha) = 0$ para todo $x \in \mathcal{X}$ equivale a que α esté en todos los ideales maximales de A.

Los cerrados de Zariski de $\mathcal{X}$ vienen descritos del siguiente modo. Sean $\alpha_1,...,\alpha_r \in A$ y pongamos $V(\alpha_1,...,\alpha_r) \subseteq \mathcal{X}$ para denotar el conjunto de los $x \in \mathcal{X}$ tales que $x(\alpha_i) = 0$ para todo i. Si identificamos $\mathcal{X}$ con el conjunto de los ideales maximales de A, $V(\alpha_1,...,\alpha_r)$ es el conjunto de los ideales maximales $\boldsymbol{m}$ tales que $\alpha_i \in \boldsymbol{m}$. Con estas notaciones tenemos:

4.4. *Los subconjuntos* $V(\alpha_1,...,\alpha_r)$*, con r entero positivo y* $\alpha_1,...,\alpha_r \in A$*, son los cerrados de la topología de Zariski de* $\mathcal{X}$.

Para la demostración se puede representar A como el álgebra de funciones regulares sobre un conjunto algebraico X, en cuyo caso el aserto se demuestra de un modo parecido a (4.2). □

Comportamiento respecto de morfismos. Sean A y B $\boldsymbol{k}$-álgebras finitamente generadas reducidas y pongamos $\mathcal{X} = \mathcal{X}(A)$, $\mathcal{Y} = \mathcal{X}(B)$. Sea $\phi: A \to B$ un homomorfismo de $\boldsymbol{k}$-álgebras. Entonces tenemos una aplicación $\phi^*: \mathcal{Y} \to \mathcal{X}$ dada por $y \mapsto y \circ \phi$. En términos de ideales maximales, $\phi^*(m) = \phi^{-1}(m)$. Nótese que la inclusión

$$A/\phi^{-1}m \hookrightarrow B/m$$

es necesariamente la identidad, pues el anillo de la derecha es $\boldsymbol{k}$ y el de la izquierda contiene $\boldsymbol{k}$.

4.5. *La aplicación $f = \phi^*$ es continua, ya que*

$$f^{-1}Z(\alpha_1,...,\alpha_r) = Z(\phi\alpha_1,...,\phi\alpha_r)$$

En efecto, de las definiciones resulta inmediatamente que

$$(\phi\alpha)y = \alpha(fy)$$

para todo $\alpha \in A$, $y \in \mathcal{Y}$. En particular $(\phi\alpha)y = 0$ si y sólo si $\alpha(fy) = 0$ y de ello se deduce sin dificultad la relación del enunciado. □

Nótese que la fórmula $(\phi\alpha)y = \alpha(fy)$ nos muestra que $f = \phi^*$.

A los espacios de la forma $\mathcal{X}(A)$, A un álgebra finitamente generada y reducida sobre un cuerpo algebraicamente cerrado $\boldsymbol{k}$ los denominaremos *variedades algebraicas afines.* Y a las aplicaciones entre variedades afines inducidas por homomorfismos de $\boldsymbol{k}$-álgebras (en sentido opuesto), *morfismos de variedades algebraicas afines.*

Geometría de un cociente. Sea A una $\boldsymbol{k}$-álgebra finitamente generada reducida, $I = (\alpha_1,...,\alpha_r)$ un ideal de A. El cociente $B = A/I$ es una $\boldsymbol{k}$-álgebra finitamente generada. Un elemento $\alpha(I) \in B$ es nihilpotente si y sólo si existe un entero positivo m tal que $\alpha^m \in I$, lo que muestra que B es reducida si y sólo si el ideal I es un *ideal radical,* esto es, tal que $\alpha^m \in I$, m un entero positivo, implica $\alpha \in I$. Si I es un ideal radical, a la proyección canónica $\pi: A \to B$ le corresponde una inyección $\pi^*: \mathcal{Y} \to \mathcal{X}$ que da un homeomorfismo de $\mathcal{Y}$ con $V(\alpha_1,...,\alpha_r)$.

Hemos intentado dejar claro que $\mathcal{X}(A)$ es un objeto geométrico intrínsecamente asociado a A y que su inclusión en un $\boldsymbol{k}^n$ es equivalente a dar un sistema de n generadores de A como $\boldsymbol{k}$-álgebra. Ello es ahora claro, ya que la distinción de un sistema de n generadores en A equivale a distinguir un epimorfismo de $\boldsymbol{k}[T_1,...,T_n]$ en A, al cual le corresponde una inclusión de $\mathcal{X}(A)$ en $\boldsymbol{k}^n$.

Geometría de una localización. Mencionemos tan sólo el caso de la localización por un elemento. Sea A un $\boldsymbol{k}$-álgebra finitamente generada reducida y $\mathcal{X} = \mathcal{X}(A)$. Sea $\varphi \in A$ un elemento no nulo. Entonces $D(\varphi)$ es un abierto. ¿Es este espacio el espacio espectral de una $\boldsymbol{k}$-álgebra? Es claro, por definición de $D(\varphi)$, que los puntos de este abierto son los homomorfismos de A en $\boldsymbol{k}$ cuyo valor en β es no nulo. Por otra parte, podemos formar el anillo A_β tomando fracciones de la forma α/β^n, donde n es un número natural cualquiera y α un elemento arbitrario

de A. Estas fracciones pueden ser sumadas y multiplicadas como las fracciones de números enteros y de este modo A_β es una $\boldsymbol{k}$-álgebra conmutativa y unitaria. La única diferencia con el caso de los números racionales está en que ahora, si el cálculo ha de ser consistente, una fracción α/β^n se considera nula cuando $\beta^m\alpha = 0$ para algún m natural.

Es además claro que si $t_1,...,t_s$ son generadores de A como $\boldsymbol{k}$-álgebra, entonces $t_1,...,t_s, 1/\beta$ son generadores de A_φ, de modo que A_φ es finitamente generada. Veamos que es reducida. Si α/β^n, fuese nihilpotente, entonces sería $\alpha^N/\beta^{nN} = 0$ en A_β, para un cierto número natural N. Esto significa que existe un m natural tal que $\beta^m\alpha^N = 0$ en A. Multiplicando por una potencia de β o de α, vemos que $\beta\alpha$ es nihilpotente y como A es reducida, ha de ser $\beta\alpha = 0$. Por tanto $\alpha/\beta^n = 0$ en A_β.

Por último, es claro que tenemos un homomorfismo de $\boldsymbol{k}$-álgebras $\lambda: A \to A_\beta$, $\alpha \mapsto \alpha/1$. Pongamos $\mathcal{X} = \mathcal{X}(A)$, $\mathcal{Y} = \mathcal{X}(A^\beta)$. Dado que $\phi/1$ es invertible en $A \to A_\beta$, resulta que $(\lambda^*y)(\beta) = y(\beta/1) \neq 0$ para todo $y \in \mathcal{Y}$. Recíprocamente, si $x(\beta) \neq 0$, $x \in \mathcal{X}$, entonces existe un único homomorfismo $y: A_\varphi \to \boldsymbol{k}$ tal que $y(\alpha/\beta^n) = x(\alpha/)x(\beta)^{-n}$, lo cual prueba que λ^* identifica $\mathcal{X}(A_\beta)$ con $D(\beta)$.

Por último, es claro que tenemos un *homomorfismo de localización* $\lambda: A \to A_\beta$, $\alpha \mapsto \alpha/1$. Pongamos $\mathcal{X} = \mathcal{X}(A)$, $\mathcal{Y} = \mathcal{X}(A_\beta)$. Dado que $\beta/1$ es invertible en A_β, resulta que $(\lambda^*y)(\beta) = y(\beta/1) \neq 0$ para todo $y \in \mathcal{Y}$. Recíprocamente, si $x(\beta) \neq 0$, $x \in \mathcal{X}$, entonces existe un único homomorfismo $y: A_\beta \to \boldsymbol{k}$ tal que $y(\alpha/\beta^n) = x(\alpha/)x(\beta)^{-n}$, lo cual prueba que λ^* identifica $\mathcal{X}(A_\beta)$ con $D(\beta)$.

Se ha de advertir que la localización de A respecto de un subconjunto S cualquiera es una $\boldsymbol{k}$-álgebra A_S cuya construcción, puramente algebraica, no ofrece dificultad. Ahora bien, si S no es finito, entonces A_S no es en general finitamente generada. No obstante, su espacio de caracteres se identifica con el subconjunto del espacio espectral de A formado por los puntos en los que no se anula ningún elemento de S, conjunto que en general no es ni abierto ni cerrado.

Productos o geometría del producto tensorial. Sean A y B $\boldsymbol{k}$-álgebras finitamente generadas reducidas. Entonces podemos formar el álgebra $A \otimes_p B$, cuyos elementos son sumas finitas de elementos de la forma $\alpha \otimes \beta$ y cuyo producto viene caracterizado por la relación $(\alpha \otimes \beta)(\alpha' \otimes \beta') = \alpha\alpha' \otimes \beta\beta'$. Tenemos homomorfismos de $\boldsymbol{k}$-álgebras $A \to A \otimes_p B$, $\alpha \mapsto \alpha \oplus 1$, $B \to A \otimes_p B$, $\beta \mapsto 1 \oplus \beta$, de modo que $\alpha \otimes \beta = (\alpha \oplus 1)(1 \oplus \beta)$. De ello resulta que dar un homomorfismo de $\boldsymbol{k}$-álgebras $A \otimes_p B \to C$, C cualquier $\boldsymbol{k}$-álgebra, es equivalente a dar un par de homomorfismos de $\boldsymbol{k}$-álgebras $A \to C$, $B \to C$.

Es claro además que $A \otimes_k B$ es finitamente generada y se puede ver que es reducida. Así pues podemos considerar el espacio espectral $\mathcal{P} = \mathcal{X}(A \otimes_p B)$. Tenemos morfismos $\mathcal{P} \to \mathcal{X}$, $\mathcal{P} \to \mathcal{Y}$ y además dar un morfismo $\mathcal{Z} \to \mathcal{P}$ equivale a dar un par de morfismos $\mathcal{Z} \to \mathcal{X}$, $\mathcal{Z} \to \mathcal{Y}$. Así pues $\mathcal{P}$ es un *producto* de las variedades afines $\mathcal{X}(\mathcal{A})$ y $\mathcal{X}(B)$.

Es fácil ver que si $X \subseteq \boldsymbol{k}^n$, $Y \subseteq \boldsymbol{k}^m$, entonces su producto coincide, como conjunto, con el producto $X \times Y \subseteq \boldsymbol{k}^{n+m}$. Sin embargo es de observar que la topología de Zariski de la variedad producto es más fina que la topología producto.

Grupos algebraicos. Algebras de Hopf. Identifiquemos el espacio de las matrices $n \times n$ con el espacio k^{n^2}. La función **det**: $k^{n^2} \to k$ es un polinomio (homogéneo) de grado n y el producto de matrices nos da un morfismo algebraico $k^{n^2} \times k^{n^2} \to k^{n^2}$. Como $\mathrm{GL}_n(k)$ está formado por las matrices con determinante no nulo, es una variedad afín, $\mathrm{GL}_n(k) = D(\mathbf{det})$, y el producto de matrices $\mathrm{GL}_n(k) \times \mathrm{GL}_n(k) \to \mathrm{GL}_n(k)$ es un morfismo de variedades. La aplicación $\mathrm{GL}_n(k) \to \mathrm{GL}_n(k)$, dada por $a \mapsto a^{-1}$, es también un morfismo.

Un *grupo lineal* es un subgrupo G de algún $\mathrm{GL}_n(k)$ cerrado por la topología de Zariski. Por ejemplo, los *grupos clásicos:* El mismo $\mathrm{GL}_n(k)$; $\mathrm{SL}_n(k)$, el grupo lineal especial, formado por las matrices con determinante 1, es el lugar de ceros de $\mathbf{det} - 1$, $\mathrm{SL}_n(k) = Z(\mathbf{det} - 1)$; $\mathrm{O}_n(k)$, el grupo ortogonal, formado por las matrices ortogonales, esto es, matrices $a \in \mathrm{GL}_n$ cuya traspuesta coincide con su inversa, $aa^T = a^Ta = I$; $\mathrm{Sp}_n(k)$, el grupo simpléctico, formado por las matrices simplécticas, esto es, matrices $a \in \mathrm{GL}_{2n}$ tales que $a^TJa = J$, siendo

$$J = \begin{pmatrix} & I \\ -I & \end{pmatrix}$$

e I la matriz identidad de orden n.

Si G es un grupo lineal, las aplicaciones μ: $G \times G \to G$ y ι: $G \to G$, dadas por multiplicación y paso a la matriz inversa, son morfismos de variedades. Así que los grupos lineales son en particular *grupos algebraicos.*

Sea A el álgebra de las funciones polinomiales de un grupo lineal G. Entonces tenemos homomorfismos de k-álgebras μ^*: $A \to A \oplus A$, ι^*: $A \to A$ y Δ^*: $A \to A \oplus A$, donde Δ: $G \to G \times G$ es la *aplicación diagonal,* $x \mapsto (x,x)$. Diremos que μ^* es la *comultiplicación,* que Δ^* es la *multiplicación* y que ι^* es la aplicación *antípoda* de A. El elemento neutro I de G es un homomorfismo $A \to k$, al que llamaremos *counidad* de A. A la inclusión η de k en A la llamaremos *unidad.* En correspondencia con la propiedad asociativa de μ, diremos que μ^* es *coasociativa.* La aplicación μ^* no verifica la propiedad de *coconmutatividad,* debido a que G no es en general conmutativo. Sin embargo Δ^* es *conmutativa,* en un sentido natural que no hace falta hacer explícito. La counidad satisface la propiedad que traduce que $I \in G$ es el elemento neutro del grupo. La unidad verifica la propiedad dual.

La estructura $(A, \Delta^*, \mu^*, \eta, I)$, con las propiedades descritas, es un ejemplo de *álgebra de Hopf* con antípoda. Entre la multiplicación y comultiplicación hay una relación de compatibilidad, que se expresa por la conmutatividad del diagrama dual del diagrama conmutativo que sigue:

$$\begin{tikzcd} & G \arrow[dr, "\Delta"] & \\ G \times G \arrow[ur, "\mu"] \arrow[d, "\Delta \times \Delta"'] & & G \times G \\ G \times G \times G \times G \arrow[rr, "S_{(23)}"] & & G \times G \times G \times G \arrow[u, "\mu \times \mu"'] \end{tikzcd}$$

donde $S_{(23)}$ es el morfismo que consiste en trasponer el segundo y tercer factor.

Un morfismo de grupos lineales induce un morfismo entre las correspondientes álgebras de Hopf, y viceversa. De este modo no es difícil ver, por ejemplo, que todo morfismo φ de $\mathrm{GL}_n(k)$ en k^*, el grupo multiplicativo de k, es una potencia entera del determinante, $\varphi(a) = \mathbf{det}(a)^q$, $q \in \mathbb{Z}$.

Nota sobre grupos cuánticos. Las álgebras de Hopf como las descritas, pero admitiendo la posibilidad de que sean no conmutativas, vienen siendo usadas en los últimos años para obtener una generalización de los grupos (algebraicos o de Lie) a lo que se ha dado en llamar *grupos cuánticos.* El objeto primario es el álgebra de Hopf, a la cual se somete a una «geometrización» cuyo resultado es el grupo cuántico. Para este tema, y temas relacionados de geometría no conmutativa, que no podemos tratar aquí, remitimos al lector a las referencias consignadas en el punto (g) de la introducción.

Variedades tóricas. Hemos visto que el lenguaje de los conjuntos algebraicos (o variedades algebraicas afines) es equivalente al de las k-álgebras finitamente generadas reducidas: a cada conjunto algebraico X se le asocia el álgebra $A(X)$ y, viceversa, a cada k-álgebra finitamente generada A se le asocia su espacio espectral $X(A)$.

Por la misma definición, los conjuntos algebraicos vienen definidos por ecuaciones polinómicas, a lo cual corresponde una descripción del álgebra de funciones polinomiales como un cociente de un anillo de polinomios.

El punto que queremos destacar aquí es la construcción de ciertas álgebras finitamente generadas reducidas de las cuales a priori no se conoce explícitamente ningún sistema de generadores. Los espacios espectrales de estas álgebras son ejemplos interesantes de variedades afines que no vienen dadas explícitamente como conjuntos algebraicos.

Para describir estas álgebras, sea S un subconjunto del conjunto $\mathcal{M}$ de monomios en las indeterminadas $T_1, \ldots, T_n$, con exponentes enteros, y formemos el conjunto $k[S]$ de todas las combinaciones lineales de los elementos de S con coeficientes de k. De la misma definición resulta que $k[S]$ es un subanillo de $\mathcal{A} := k[T_1, \ldots, T_n, T_1^{-1}, \ldots, T_n^{-1}]$ si y sólo si S es cerrado con el producto y $1 \in S$, es decir, si y sólo si S es un subsemigrupo del grupo multiplicativo $\mathcal{M}$ (el cual es isomorfo al grupo aditivo $\mathbb{Z}^n$). Si S es un subsemigrupo de $\mathcal{M}$, el anillo $k[S]$ es automáticamente reducido, por ser subanillo de $\mathcal{A}$. Si además S es finitamente generado, entonces $k[S]$ será una k-álgebra finitamente generada. Nótese que $k[\mathcal{M}]$ coincide con $k[T_1, \ldots, T_n, T_1^{-1}, \ldots, T_n^{-1}]$, el anillo de polinomios de Laurent en las indeterminadas T_i.

¿Cómo se pueden construir subsemigrupos finitamente generados S de $\mathcal{M}$? Es claro que un modo de proceder es escoger un conjunto finito $\mu_1, \ldots, \mu_r$ de monomios y definir S como el semigrupo generado por $\mu_1, \ldots, \mu_r$. En este caso $k[S] = k[\mu_1, \ldots, \mu_r]$. Así, por ejemplo, $k[T^2, T^3]$ es el anillo de funciones polinomiales de la curva $Y^2 = X^3$. Nótese además que el anillo de polinomios $k[T_1, \ldots, T_n]$ se obtiene tomando el semigrupo de los monomios con exponentes no negativos.

Pero hay otro modo de proceder y que consiste en partir de un cono racional poliédrico $\sigma = [\upsilon_1, ..., \upsilon_r]$ de $\mathbb{Q}^n$ (es decir, el conjunto de combinaciones lineales $t_1\upsilon_1 + ... + t_s\upsilon_s$ con coeficientes racionales t_i no negativos, siendo los υ_i vectores enteros) y tomar como S el conjunto S_σ de monomios cuyos exponentes $m = (m_1, ..., m_n)$ verifican que $m \cdot x \geq 0$ para todo $x \in \sigma$. Se puede ver que de este modo S_σ es un subsemigrupo finitamente generado y por tanto a σ le podemos asociar una variedad afín X_σ definida como el espacio espectral de $\boldsymbol{k}[S_\sigma]$. A estas variedades se las denomina *variedades tóricas afines* y su estudio tiene actualmente una considerable importancia en varios campos de la geometría algebraica.

Nos remitimos a Oda [1988] para una introducción sistemática a estas variedades y a Procesi-Xambó [1991] para una aplicación de las mismas a un problema clásico de geometría enumerativa.

Geometrización de un anillo conmutativo arbitrario. La geometrización de la $\boldsymbol{k}$-álgebras finitamente generadas se ha hecho vía los ideales maximales de las mismas. Un tal procedimiento no puede ser satisfactorio para anillos conmutativos cualesquiera toda vez que la imagen inversa de un ideal maximal no es en general un ideal maximal, sino sólo un ideal primo. Pero si a cada anillo conmutativo con unidad A le asociamos el conjunto $\mathcal{P}(A)$ de sus ideales primos y a cada ideal I de A le asociamos el subconjunto $V(I)$ de $\mathcal{P}(A)$ formado por los ideales primos $\boldsymbol{p}$ de A tales que $I \subseteq \boldsymbol{p}$ (es decir, tales que $a(\boldsymbol{p}) = 0$ para todo $a \in I$), entonces los conjuntos $V(I)$ son los cerrados de una topología de $\mathcal{P}(A)$, que se denomina también de Zariski, la cual tiene un comportamiento natural respecto de los morfismos arbitrarios de anillos: si $f\colon A \to B$ es un homomorfismo de anillos, la aplicación $\boldsymbol{p} \mapsto f^{-1}(\boldsymbol{p})$ de $\mathcal{P}(B)$ en $\mathcal{P}(A)$ es continua. Vemos pues que el espacio topológico **Spec**(A) (el conjunto $\mathcal{P}(A)$ con la topología de Zariski) juega el papel de un *espacio espectral* para A. A este espacio se le denomina *espectro primo* de A. La noción de álgebra de funciones regulares no es válida tal cual (nótese que si $a \in A$, entonces $a(\boldsymbol{p})$ es un elemento del anillo $A/\boldsymbol{p}$, el cual *varía* al variar $\boldsymbol{p}$), pero se puede substituir por la noción de *haz espectral* de **Spec**(A) (véase Hartshorne [1977]). El *esquema afín* definido por A es entonces el espacio **Spec**(A) dotado de su haz estructural.

Variedades y esquemas. Grosso modo, y calcando la definición usual de variedades diferenciables, las variedades algebraicas se definen como espacios que localmente son isomorfos a variedades afines y los *esquemas* como espacios que localmente son isomorfos a esquemas afines. Las variedades algebraicas son el objeto de estudio de la geometría algebraica clásica, mientras que la geometría algebraica moderna es, en gran medida, el estudio de los esquemas y sus aplicaciones, con frecuencia a problemas que son reformulaciones rigurosas de problemas clásicos. Dado que los esquemas generalizan las variedades (este hecho no es del todo trivial y descansa, en último análisis, en el teorema de los ceros de Hilbert; véase Hartshorne [1977]) y que los ideales primos tienen su origen en cuestiones de aritmética, la teoría de esquemas resulta ser un lenguaje apropiado para expresar no sólo los problemas y métodos de la geometría algebraica clásica, sino también los de teoría de números, especialmente las cuestiones de tipo diofántico. Esta idea es crucial en la filosofía que ha regido la vanguardia de la geometría algebraica en los últimos decenios, dando lugar a numerosos e importantes avances en lo que se puede denominar geometría algebraica aritmética, para distinguirla de la geometría algebraica en el sentido ordinario y que sólo se ocupa del estudio de variedades en un sentido clásico. Para una iniciación al estudio de la geometría algebraica aritmética, véase Xambó [1991] y las referencias que allí se dan.

Epílogo. ¿Qué es el espectro de un anillo? ¿Para qué sirve? ¿Se puede prescindir de un concepto en apariencia tan abstracto? En estas notas en realidad hemos intentado contestar a una baraja de preguntas de esta suerte, mostrando que hay caminos que conducen, sin solución de continuidad en las ideas, de la noción experimental de espectro de un átomo a la noción de espectro de un anillo conmutativo. También se han dado indicaciones de algunas direcciones en las que se está trabajando en la actualidad como continuación natural de las que nos han conducido al presente. Junto a las polaridades entre funciones (o coordenadas) y puntos, entre lógica y realidad, entre álgebra y geometría, en el fondo se han tenido en cuenta otras emparentadas con las mismas, como las existentes entre ondas y partículas o entre matemáticas y física, como lo señalan las numerosas citas a Manin [1981], obra que recomendamos encarecidamente a quienes estén interesados por este tipo de discursos.

Agradecimientos. Es para mi un agradable deber expresar mi gratitud a J. M. Montesinos por el tiempo y la paciencia que ha invertido en muchas discusiones sobre el contenido de estas notas y su presentación, y especialmente por dirigirme las preguntas consignadas en el epílogo, al tiempo que he de dejar claro que los errores, impreciones o defectos que en las mismas subsistan son sólo achacables al autor.

También quiero agradecer los comentarios que Lê-Dũng Tráng y Jesús Ruiz me han hecho a una versión preliminar y que han ayudado a mejorar el contenido de algunos puntos y a eliminar numerosas erratas.

Finalmente quiero dar las gracias a los profesores Javier Etayo y Fernando Etayo, por proporcionarme datos sobre la biografía matemática de don José J. Etayo Miqueo, datos que me permitieron apreciar en un caso próximo y concreto la exactitud de las ideas expresadas por A. Weil en la cita inicial.

BIBLIOGRAFIA

Aupetit, B. [1991]. *A Primer on Spectral Theory.* Universitext, Springer-Verlag, 1991.

Bochnak, J. [1973]. *Sur le théorème des zéros de Hilbert «differentiable»,* Topology 12 (1973), 417-24.

Boole, G. [1847]. *Mathematical Analysis of Logic.* Collected Logical Works (2 vols.), P. Jourdain, Chicago-London, 1916.

Boole, G. [1854]. *An Investigation of the Laws of Thought,* Collected Logical Works (2 vols.), P. Jourdain, Chicago-London, 1916.
Colliot-Thélène [1982]. *Variantes du Nullstellensatz réel et anneaux formellement réels,* en *Géométrie Algébrique Réelle et Formes Quadratiques,* ed. por Colliot-Thélène et al., LN in Math. 959, Springer-Verlag, 1982.
Connes, A. [1990]. *Géométrie non commutative,* InterEditions 1990.
Dedekind, R., Weber, H. [1882]. *Theorie der algebraischen Funktionen einer Veränderlichen,* Jour. für Math. 92 (1882), 181-290.
Dieudonné, J. [1981]. *History of Functional Analysis,* Mathematics Studies, 49. North-Holland, 1981.
Gelfand, I. M., Raikov, D. A., Chilov, G. E. [1964]. *Les anneaux normés commutatives,* Gauthier-Villars 1964 (traducción del texto ruso de 1960).
Grothendieck, A., Dieudonné, J. [EGA]. *Elements de Géométrie Algebrique.* I, II, III y IV. Publ. Math. IHES 1960-64.
Grothendieck, A. et al. [SGA]. *Séminaire de la Géométrie Algebrique,* 1, 2, 3, 4, $4\frac{1}{2}$, 5, 6 y 7. North-Holland 1968. Springer-Verlag LN 1971-77.
Halmos, P. R. [1962]. *Lectures on Boolean algebras,* Van Nostrand 1963.
Hartshorne, R. [1977]. *Algebraic Geometry,* GTM 52, Springer-Verlag 1977 (tercera edición corregida 1983).
Hilbert, D. [1890]. *Über die Theorie der algeraischen Formen,* Math. Ann. 36 (1890), 473-534.
Johnstone, P. T. [1982]. *Stone spaces,* Cambridge Univ. Press 1982.
Johnstone, P. T. [1983]. *The point of pointless topology,* Bull. Amer. Math. Soc., 8-1 (1983), 41-53.
Katznelson, Y. [1968]. *An introduction to harmonic analysis,* Dover 1976 (primera versión 1968).
Lang, S. [1982]. *Introduction to Algebraic and Abelian Functions,* Segunda Ed., Springer-Verlag, 1982.
McKenna, K. [1980]. *Some Diophantine Nullstellensätze,* en *Model Theory of Algebra and Arithmetic,* ed. por Pacholski et al., LN in Math. 834, Springer-Verlag, 1980.
Manin, Y. I. [1981]. *Mathematics and Physics,* Progress in Physics 3, Bi~~e~~rkhäuser 1981.
Manin, Y. I. [1984]. *New directions in geometry,* Russian Math. Surveys 39:6 (1984), 51-83.
Manin, Y. I. [1988 a]. *Quantum groups and Non-Commutative Geometry,* Centre de Recherches Mathématiques, Univ. de Montréal, 1988.
Manin, Y. I. [1988 b]. *Gauge Field Theory and Complex Geometry,* Grundlehren 289, Springer-Verlag, 1988.
Manin, Y. I. [1991]. *Notes on Quantum Groups and Quantum De Rham Complexes,* Preprint MPI/91-60, Max-Planck-Institut für Mathematik, 1991.
Naimark, M. A. [1972]. *Normed algebras,* Wolters-Hoordhoff, 1972.
Oda, T. [1988]. *Convex Bodies and Algebraic Geometry,* Springer-Verlag, 1988.
Procesi, C., Xambó, S. [1991]. *On Halphen's first formula,* aparecerá en los Proceedings del Simposio Zeuthen (Copenhague, 1989), editados por S. Kleiman y A. Thorup.
Robertson, A. P., Robertson, W. J. [1980]. *Topological vector spaces,* Cambridge Univ. Press, edición de 1980.
Serre, J. P. [1955]. *Faisceaux algébriques cohérents,* Ann. of Math. 61 (1955), 197-278.

Stone, M. H. [1934]. *Boolean algebras and their applications to topology,* Proc. Nat. Acad. Sci. U.S.A. 20 (1934), 197-202.
Stone, M. H. [1936]. *The theory of representations of Boolean algebras,* Trans. Amer. Math. Soc. 40 (1936), 37-111.
Stone, M. H. [1937]. *Topological representation of distributive lattices and Browerian logics,* Časopis pešt. mat. fys. 67 (1937), 1-25.
Von Neumann, J. [1955]. *Mathemathical Foundations of Quantum Mechanics,* Investigations in Physics 2, Princeton Univ. Press 1955.
Weil, A. [1961]. *Organisation et désorganisation en mathématique,* Obras completas, Springer-Verlag.
Xambó, S. [1991]. *Introducción a la Geometría Algebraica Aritmética,* Notas para el curso de doctorado 90/91, Departamento de Algebra, Universidad Complutense de Madrid.
Zariski, O., Samuel J. P. [1960]. *Commutative Algebra,* Springer-Verlag 1960.