Boletín de Matemáticas
Vol. VIII , pp. 56-73

EL 17º PROBLEMA DE HILBERT(*)

PAULO RIBENBOIM

En 1900, en París, David Hilbert, invitado a dictar una conferencia, propone 23 problemas abiertos de matemáticas [10] . La solución de estos problemas era difícil; podemos citar, por ejemplo, los trabajos de Montgomery, Zippin y Gleason para resolver el 5º, aquellos de Julia Robinson y Matijasevich para el problema 10 y la respuesta negativa de Nagata al problema 14.

Expliquemos ahora en qué consistía el 17º de estos problemas.

Sea $\mathbb{R}$ el cuerpo de los números reales, $\mathbb{R}[X_1, \ldots, X_n]$ el *anillo de los polinomios en* n *variables* con coeficientes en $\mathbb{R}$, $\mathbb{R}(X_1, \ldots, X_n)$ su cuerpo de fracciones, es decir, el *cuerpo de fracciones racionales en* n *variables* con coeficientes en $\mathbb{R}$.

Toda fracción racional $f \in \mathbb{R}(X_1, \ldots, X_n)$ puede escribirse en la forma $f = f_1/f_2$ donde $f_1, f_2 \in \mathbb{R}[X_1, \ldots, X_n]$. Diremos que una fracción f está definida en $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$ si es posible escribir $f = f_1/f_2$ donde $f_2(x_1, \ldots, x_n) \neq 0$. Diremos que f es *positiva-definida* si en todo punto $x \in \mathbb{R}^n$ donde f está definida se tiene que $f(x) \geq 0$. Es claro que una

(*) El original, en francés, de este artículo lo publica la Sociedad Brasileña de Matemáticas. El texto corresponde a la conferencia que sobre este tema dictó el autor en el IV Coloquio Colombiano de Matemáticas. La versión castellana estuvo a cargo de Jesús H. Pérez. N. del E.

suma de cuadrados Σf_i^2, donde $f_i \in \mathbb{R}(X_1, \ldots, X_n)$ es positiva-definida. Hilbert trató de buscar otros ejemplos. En el caso $n=0$, $\mathbb{R}(X_1, \ldots, X_n) = \mathbb{R}$ y $f \in \mathbb{R}$ es positiva definida si y sólo si f es positiva en $\mathbb{R}$ y en consecuencia, si y sólo si f es un cuadrado.

En el caso $n=1$, $f \in \mathbb{R}(X)$ es positiva definida si y sólo si f es suma de dos cuadrados.

En el caso $n=2$, $f \in \mathbb{R}(X,Y)$ es definida positiva si y solamente si f puede escribirse como suma de cuatro cuadrados; pero Hilbert no pudo determinar si existía o no una suma de cuatro cuadrados que no fuera suma de tres cuadrados.

Enunciemos entonces el 17º problema de Hilbert en el caso de n variables:

Sea $f \in \mathbb{R}(X_1, \ldots, X_n)$ definida positiva. ¿Es f suma de cuadrados de fracciones racionales? y en el caso de que lo sea, ¿de cuántos cuadrados? Nótese que para estudiar este problema podemos suponer $f \in \mathbb{R}[X_1, \ldots, X_n]$, positiva sobre $\mathbb{R}^n$ (multiplicando por el cuadrado del denominador). Una solución cualitativa a este problema fue dada en 1927 por Artin en [1].

I. REPASO DE ALGUNAS NOCIONES QUE INTERVIENEN EN EL ESTUDIO [15]

Cuerpo ordenado $\mathbb{K}$: Es un cuerpo provisto de una relación de orden total, compatible con las operaciones.

Cuerpo ordenable $\mathbb{K}$: Es un cuerpo que puede dotarse de una relación de orden total compatible con las operaciones. Recordemos el teorema de Artin-Shreier que caracteriza estos cuerpos: un cuerpo $\mathbb{K}$ es ordenable si y solamente si -1 no es suma de cuadrados de elementos de $\mathbb{K}$.

Extensiones ordenadas de un cuerpo ordenado: Sea $\mathbb{K}$ un cuerpo ordenado, $\mathbb{L}$ una extensión de $\mathbb{K}$; $\mathbb{L}$ es *extensión ordenada* de $\mathbb{L}$ si $\mathbb{L}$ está provisto de

un orden que prolonga el de $\mathbb{K}$.

Cuerpo ordenado maximal : Un cuerpo ordenado $\mathbb{K}$ se dice *ordenado maximal* si no admite extensiones algebraicas ordenadas diferentes de $\mathbb{K}$.

Clausura real de un cuerpo ordenado $\mathbb{K}$: Es una extensión ordenada $\tilde{\mathbb{K}}$ de $\mathbb{K}$ que es a la vez extensión algebraica y tal que $\tilde{\mathbb{K}}$ es un cuerpo ordenado maximal. $\tilde{\mathbb{K}}$ es única salvo $\mathbb{K}$ - isomorfismos.

Caracterización de los cuerpos ordenados maximales : Un cuerpo $\mathbb{L}$ es ordenado maximal si y sólo si

(i) $\mathbb{L} = \mathbb{L}^2 \cup (-\mathbb{L}^2)$

(ii) para todo $f \in \mathbb{L}[X]$ de grado impar, f tiene una raiz en $\mathbb{L}$. Anotamos que un tal cuerpo posee un solo orden y podemos citar como ejemplos el cuerpo $\mathbb{R}$ de los números reales y el cuerpo de los números reales algebraicos.

Obsérvese también que (ii) hace pensar que los cuerpos ordenados maximales están cercanos a los cuerpos algebraicamente cerrados. De hecho, si $\mathbb{L}$ es ordenado maximal, entonces $L[i]$ es algebraicamente cerrado (donde $i^2 = -1$).

Elementos totalmente positivos de un cuerpo ordenable : Sea $\mathbb{K}$ un cuerpo ordenable, $\mathbb{K}$ es entonces suceptible de admitir varios órdenes totales compatibles con las operaciones. Llamaremos elemento totalmente positivo de $\mathbb{K}$ un elemento que es positivo en *cada uno* de estos órdenes. Existe una caracterización de estos elementos : $x \in \mathbb{K}$ es totalmente positivo si y sólo si x es suma de cuadrados de elementos de $\mathbb{K}$.

II. SOLUCION CUALITATIVA DEL 17º PROBLEMA DE HILBERT

El cuerpo $\mathbb{R}(X_1, \ldots, X_n)$ es ordenable.

Hemos visto que toda suma de cuadrados de elementos de $\mathbb{R}(X_1, \ldots, X_n)$ es

positiva definida y queremos estudiar el problema recíproco, o sea, vamos a demostrar la implicación :

$f \in \mathbb{R}[X_1, \ldots, X_n]$ *definida positiva* $\Rightarrow$ f *es un elemento totalmente positivo de* $\mathbb{R}(X_1, \ldots, X_n)$.

La primera demostración de este teorema, larga y difícil, fué dada por Artin [1] . Se pueden encontrar otras presentaciones en [15] y [11] .

Después de la solución de Artin, otras demostraciones que hacen uso de la lógica (la Teoría de Modelos) han sido obtenidas; al respecto se puede consultar [17], [12] ó [7] .

Expondremos aquí una presentación de estos métodos lógicos. Recordemos antes una serie de elementos de lógica .

1. *Repaso de nociones de Lógica*

Los enunciados matemáticos se expresan por medio de un lenguaje. Un tal lenguaje está formado de símbolos de diferente tipo :

- los símbolos de constantes (como *0* ó *1*)
- los símbolos lógicos (ó : $\vee$, y : $\wedge$, no : $\neg$, existe : $\bigvee$, para todo: $\bigwedge$[1] y otros definidos a partir de estos, como por ejemplo la equivalencia lógica: $\Longleftrightarrow$)
- los símbolos relacionales (como $\leq$ ó $=$)
- los símbolos funcionales (como $+$, $\cdot$)
- las variables .

Para expresar los enunciados de la teoría de los cuerpos conmutativos, em-

(1) En lugar de $\bigvee$ y de $\bigwedge$ se usan también $\exists$, $\forall$, respectivamente . N. del T.

plearemos un lenguaje que comprende 0 y 1 como símbolos de constantes, $+$ y $\cdot$ como símbolos funcionales, y $=$ como símbolo relacional.

En este lenguaje $\mathfrak{L}$ escribimos los axiomas de la teoría de los cuerpos conmutativos y todo conjunto tal que los axiomas sean proposiciones verdaderas será un *modelo* de la teoría de los cuerpos conmutativos.

Aquí, lo que nos interesa es la teoría de los cuerpos conmutativos ordenados. Citemos los elementos del lenguaje y enunciemos los axiomas de esta teoría. El lenguaje estará formado por 0 y 1 como símbolos de constantes, $+$ y $\cdot$ como símbolos funcionales en dos variables, $-$ como símbolo funcional en una variable y $=$, $>$ como símbolos relacionales.

Los axiomas de la teoría de cuerpos conmutativos ordenados son :

$\wedge x \quad \wedge y \quad \wedge z \quad ((x+y)+z = x+(y+z))$

$\wedge x \quad \wedge y \quad (x+y = y+x)$

$\wedge x \quad (x+0 = x)$

$\wedge x \quad (x+(-x) = 0)$

$\wedge x \quad \wedge y \quad \wedge z \quad ((x \cdot y) \cdot z = x \cdot (y \cdot z))$

$\wedge x \quad \wedge y \quad (x \cdot y = y \cdot x)$

$\wedge x \quad (x \cdot 1 = x)$

$\wedge x \quad \vee y \quad ((x = 0) \vee (x \cdot y = 1))$

$\wedge x \quad \wedge y \quad \wedge z \quad (x \cdot (y+z) = x \cdot y + x \cdot z)$

$\neg \quad (0 = 1)$

$\wedge x \quad \wedge y \quad ((x > 0) \wedge (y > 0) \Rightarrow x+y > 0)$

$\wedge x \quad \wedge y \quad ((x > 0) \wedge (y > 0) \Rightarrow x \cdot y > 0)$

$\wedge x \quad (x = 0 \vee x > 0 \vee -x > 0)$

$\wedge x \quad \neg \quad ((x > 0) \wedge (-x > 0))$

Para obtener los axiomas de la teoría de los cuerpos conmutativos ordenados maximales utilizaremos el mismo lenguaje y añadiremos a los axiomas precedentes los axiomas siguientes :

$$\wedge x \quad \vee y \qquad ((x = y^2) \wedge (-x = y^2))$$

y para cada $n \geq 0$, el axioma

$$\wedge x_1 \wedge x_2 \ldots \wedge x_{2n+1} \vee x \qquad (x^{2n+1} + x_1 x^{2n} + \cdots + x_{2n+1} = 0)$$

Trabajaremos por ahora en la teoría relativa a un cuerpo de base fijo $\mathbb{K}$ ordenado maximal. Consideramos entonces el lenguaje $\mathfrak{L}'$ que se obtiene a partir del lenguaje $\mathfrak{L}$ precedente al cual añadimos a los símbolos constantes los símbolos correspondientes a los elementos de $\mathbb{K}$.

Consideramos el sistema de axiomas $\mathfrak{A}'$ que se obtiene añadiendo al sistema precedente $\mathfrak{A}$ todos los enunciados que ligan las constantes (y en consecuencia, los elementos de $\mathbb{K}$).

Los modelos del sistema $\mathfrak{A}'$ son entonces los cuerpos ordenados maximales $\mathbb{L}$ que contienen $\mathbb{K}$. Los cuerpos $\mathbb{L}$ son entonces las extensiones ordenadas de $\mathbb{K}$, extensiones que son no algebraicas en general.

Expliquemos ahora el método de eliminación de cuantificadores.

Se dice que un sistema de axiomas $\mathfrak{A}$, del lenguaje $\mathfrak{L}$ permite la *eliminación de cuantificadores* si para toda fórmula F del lenguaje $\mathfrak{L}$ existe una fórmula F' del mismo lenguaje, sin cuantificadores tal que $F \Longleftrightarrow F'$ es una consecuencia de $\mathfrak{A}$.

Volvamos a los cuerpos conmutativos ordenados maximales. Esta teoría permite la eliminación de cuantificadores (véase [12]).

Como consecuencia de este teorema, si $\mathfrak{A}'$ es el sistema de axiomas de-

finidos anteriormente, expresados en el lenguaje $\mathfrak{L}'$, entonces, el sistema de axiomas $\mathfrak{A}'$ (de la teoría de los cuerpos ordenados maximales que contienen a $\mathbb{K}$) es saturado.

Esto significa que si F es una fórmula del lenguaje $\mathfrak{L}'$, entonces F ó $\neg F$ es una consecuencia de $\mathfrak{A}'$. Es decir, podemos a partir de los axiomas de $\mathfrak{A}'$ demostrar F o su negación. Apliquemos ahora estos resultados al 17º problema de Hilbert.

2. *Solución por métodos de la lógica del 17º problema.*

Escribimos la hipótesis que $f \in \mathbb{R}[X_1, \ldots, X_n]$ es positiva definida. Tenemos la fórmula F :

$$\Lambda x_1 \, \Lambda x_2 \ldots \Lambda x_n \qquad (f(x_1, x_2, \ldots, x_n) \geq 0)$$

Esta fórmula F es verdadera en $\mathbb{R}$.

Sea $\mathfrak{A}'$ el conjunto de axiomas precedentes con $\mathbb{K} = \mathbb{R}$.

Sabemos que $\mathfrak{A}'$ es saturado y entonces F o $\neg F$ puede demostrarse a partir de $\mathfrak{A}'$. Puesto que F es verdadera en $\mathbb{R}$, $\neg F$ no puede demostrarse a partir de $\mathfrak{A}'$ y entonces es F que se demuestra a partir de $\mathfrak{A}'$.

Tenemos entonces $\mathfrak{A}' \vdash F$. Esto implica que F es verdadera en todos los modelos de $\mathfrak{A}'$.

En particular, F es verdadera en $\mathfrak{R}$ clausura real de $\mathbb{R}(X_1, \ldots, X_n)$ provisto de un orden cualquiera. Escogemos como elementos de $\mathfrak{R}$: $x_1 = X_1, \ldots, x_n = X_n$. De acuerdo con F deducimos que $f(X_1, \ldots, X_n) \geq 0$ en $\mathfrak{R}$ y por lo tanto en $\mathbb{R}(X_1, \ldots, X_n)$. Siendo esto verdadero para todo orden de $\mathbb{R}(X_1, \ldots, X_n)$, $f(X_1, \ldots, X_n)$ es un elemento totalmente positivo de $\mathbb{R}(X_1, \ldots, X_n)$ y por lo tanto, f es suma de cuadrados de elementos de

$\mathbb{R}(X_1, \ldots, X_n)$.

III. ESTUDIO CUANTITATIVO DEL 17º PROBLEMA DE HILBERT

Tenemos entonces el resultado, según el cual, $f \in \mathbb{R}(X_1, \ldots, X_n)$ definida positiva es suma de un número finito m de cuadrados de elementos de $\mathbb{R}(x_1, \ldots, X_n)$; este m depende de f y de n. Es posible encontrar $m(n)$, cota superior de los $m(n, f)$ para todas las funciones definidas positivas de $\mathbb{R}(x_1, \ldots, X_n)$.

Examinemos los casos para los primeros valores de n.

Si $n=0$, se tiene $m(0) = 1$

Si $n=1$, se tiene $m(1) = 2$

Si $n=2$, se tiene $m(2) \leq 4$

En un trabajo no publicado de Ax en 1968 se demostró que $m(3) \leq 8$; Pero, Pfister demostró independientemente que para todo n se tiene $m(n) \leq 2^n$ [13].

Llamaremos entonces constante de Pfister y lo notamos $Pf(K)$ al más pequeño entero m (si existe) tal que toda suma de cuadrados de elementos de $\mathbb{K}$ sea una suma de a lo más m cuadrados ; si un tal entero no existe definimos $Pf(K) = \infty$. Con esta notación el resultado de Pfister se escribe $Pf(\mathbb{X}_1,\ldots,X_n) \leq 2^n$.

Por otra parte, Cassels estableció el resultado siguiente : $n + 1 \leq Pf(K(\mathbb{X}_1, \ldots, X_n))$ para todo cuerpo K [2].

Deducimos entonces que si $n = 2$, $3 \leq Pf(\mathbb{R}(X_1, X_2)) \leq 4$. Pero, en un artículo, [3], Cassels, Ellison y Pfister demostraron que un cierto polino-

mio de $\mathbb{R}[X,Y]$, positivo definido y por tanto suma de cuatro cuadrados, no es suma de 3 cuadrados y entonces $Pf(\mathbb{R}(X_1, X_2)) = 4$.

Para $n \geq 3$, el problema permanece sin resolver y lo único que sabemos es que $n + 1 \leq Pf(\mathbb{R}(X_1, \ldots, X_n)) \leq 2^n$.

Anotamos que podemos considerar estos problemas para otros cuerpos diferentes de $\mathbb{R}$ y que Pourchet [14] demostró recientemente que $Pf(\mathbb{Q}(X)) = 5$. Hasta ese momento se conocía únicamente el resultado de Landau $Pf(\mathbb{Q}(X)) \leq 8$. Obsérvese entonces que la constante de Pfister de un cuerpo nó es siempre una potencia de 2.

El parágrafo que sigue está consagrado al estudio de las nociones que intervienen en la demostración del bonito resultado de Pfister.

Sumas de cuadrados. Nivel y dimensión diofántica de un cuerpo.

En primer lugar, recordemos la identidad clásica :

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2 .$$

Tenemos seguidamente la identidad de Lagrande : el producto de dos sumas de cuatro cuadrados es una suma de cuatro cuadrados.

Podemos demostrar esta identidad utilizando la norma multiplicativa sobre los cuaterniones definida por la suma de los cuadrados de las cuatro componentes.

Tenemos también la identidad de Cayley : el producto de dos sumas de ocho cuadrados es nuevamente una suma de ocho cuadrados ; lo cual se demuestra utilizando el álgebra no asociativa y no conmutativa de Cayley. En este caso, también tenemos una norma multiplicativa definida por la suma de los cuadrados de las ocho componentes.

En cada uno de estos tres casos, las componentes del producto son las for-

mas bilineales de las componentes de las sumas dadas. Pero, Hurwitz demostró que esto no es posible sino para los productos de sumas de $1, 2, 4$ ú 8 cuadrados.

Sinembargo, Pfister logró demostrar que si consideramos sumas de cuadrados de elementos de un cuerpo (y no solamente de álgebras), el producto de dos sumas de 2^n cuadrados es una suma de 2^n cuadrados de elementos del cuerpo. Además, el resultado no es suceptible de mejorarse, pues si consideramos un entero q tal que en todo cuerpo, el producto de dos sumas de q cuadrados es una suma de q cuadrados, entonces q necesariamente es una potencia de 2.

Este teorema se utiliza en el estudio de los niveles de los cuerpos.

Recordemos lo que es el nivel de un cuerpo $\mathbb{K}$: Si K es ordenable, entonces -1 no puede ser una suma de cuadrados de elementos de $\mathbb{K}$ y tomamos como nivel de $\mathbb{K}$: $\nu(K) = \infty$.

Si $\mathbb{K}$ no es un cuerpo ordenable, entonces -1 es una suma de cuadrados de elementos de $\mathbb{K}$ y llamaremos nivel de $\mathbb{K}$ al entero m más pequeño tal que -1 sea una suma de m cuadrados en $\mathbb{K}$. El resultado sobre las sumas de cuadrados le permitió a Pfister demostrar que si $\mathbb{K}$ no es ordenable, entonces $\nu(K)$ es una potencia de 2. Recíprocamente, dada una potencia de 2 es posible encontrar un cuerpo $\mathbb{K}$ que tenga como nivel dicha potencia de 2.

Por ejemplo, en el caso en el cual $\mathbb{K}$ es finito, todo elemento, es suma de dos cuadrados y entonces $\nu(K)$ es 1 ó 2. Con ayuda de los símbolos de Legendre, se puede mostrar que $\nu(\mathbb{K}) = 1$.

Es más interesante buscar el nivel de los cuerpos de números algebraicos no ordenables es decir, totalmente imaginarios. Para esto, se utiliza el principio de localización-globalización en la forma del teorema de Minkowski-Hasse que permite reducir el problema al caso del cuerpo de los números complejos

(trivial) y de las extensiones algebraicas finitas de los cuerpos p-ádicos.

El problema está resuelto ahora por un teorema de Hasse que dice que "" toda forma cuadrática en cinco variables y con coeficientes en un cuerpo que es extensión algebraica finita de un cuerpo p-ádico, tiene un cero no trivial "".

Entonces, localmente, -1 es suma de 4 cuadrados y esto también es verdadero globalmente. En conclusión, el nivel de todo cuerpo de números totalmente imaginario es $1, 2$ ó 4. Un artículo de Connell [5], permite decidir cuál es el nivel de un cuerpo en cada caso.

Estos problemas, conducen a problemas de existencia de ceros no triviales para polinomios homogéneos. Esto es, en realidad la determinación de la dimensión diofántica de un cuerpo. Si K es un cuerpo dado, se trata de encontrar condiciones sobre el número de variables y sobre el grado de polinomios homogéneos para que estos tengan un cero no trivial. Sobre esto, se puede consultar [15].

IV. ALGUNOS DESARROLLOS RECIENTES DEL 17° PROBLEMA DE HILBERT

Hablaremos primero sobre un teorema de Dubois cuya demostración utiliza el resultado de Artin sobre el 17° problema de Hilbert y que es el análogo del teorema de los ceros de Hilbert [6].

Seguidamente, expondremos algunos resultados sobre problemas semejantes al 17° problema de Hilbert, para las variedades reales [8], y para las matrices simétricas [9], considerados últimamente por Gondard y por el autor.

1. *Teorema de Dubois.*

Comenzamos por recordar el teorema de los ceros de Hilbert.

Si $\mathbb{K}$ es un cuerpo y $S \subseteq \mathbb{K}[X_1, \ldots, X_n]$, $n \geq 1$, asociamos a S el conjunto $V(S)$.

$$V(S) = \{ x = (x_1, \ldots, x_n) \in \mathbb{K}^n \mid f(x_1, \ldots, x_n) = 0 \quad \text{para todo} \quad f \in S \}$$

Se dice que $V(S)$ es el *$\mathbb{K}$-conjunto algebraico asociado a S*.

Recíprocamente, si $T \subset \mathbb{K}^n$; definimos

$$Id(T) = \{ f \in K[X_1, \ldots, X_n] \mid f(x_1, \ldots, x_n) = 0, \text{ para todo } x \in T \}$$

$Id(T)$ es un ideal de $\mathbb{K}[X_1, \ldots, X_n]$. Anotemos algunas propiedades :

(i) Sea I el ideal engendrado por S. Entonces $V(I) = V(S)$. Podemos considerar entonces únicamente ideales de $\mathbb{K}[X_1, \ldots, X_n]$.

(ii) $Id(V(I)) \supseteq I$

(iii) $V(Id(T)) \supseteq T$

(iv) $V(Id(V(I))) = V(I)$

Un problema importante es la determinación de $Id(V(I))$ y de los ideales tales que $Id(V(I)) = I$. En el caso en el cual K es un cuerpo algebraicamente cerrado, el problema se resuelve por el teorema de los ceros de Hilbert.

Teorema de los ceros de Hilbert.

Sea K un cuerpo algebraicamente cerrado, I un ideal de $K[X_1, \ldots, X_n]$ entonces $Id(V(I)) = \sqrt{I}$ (radical de I) definido por $\sqrt{I} = \{ f \in K[X_1, \ldots, X_n]$ existe $m \geq 1$ tal que $f^m \in I \}$.

Tenemos entonces una correspondencia biunívoca entre los ideales radicales tales que $I = \sqrt{I}$ y los K-conjuntos algebraicos.

Además, los ideales radicales I se caracterizan por que son intersección de ideales primos, más exactamente, de un número finito de ideales primos.

$V(I)$ es entonces reunión de un número finito de K-conjuntos algebraicos correspondientes a estos ideales primos. Estos K-conjuntos algebraicos irreducibles se llaman entonces variedades de K^n.

El estudio de estas variedades es equivalente al estudio de los ideales primos de $K[X_1, \ldots, X_n]$. Cada ideal primo P se asocia biyectivamente al anillo de coordenadas de $V(P)$ es decir, a

$$K[X_1, \ldots, X_n] / P = K[\xi_1, \ldots, \xi_n] .$$

Este anillo, es una K-álgebra entera de tipo finito y un álgebra cualquiera de estas puede obtenerse a partir de un ideal primo.

El teorema de los ceros de Hilbert permite entonces reducir el estudio geométrico de las variedades al estudio algebraico de las K-álgebras enteras de tipo finito.

En el caso donde K no es algebraicamente cerrado, el teorema de Hilbert ya no es válido. Sinembargo los cuerpos ordenados maximales, estando tan cercanos a los cuerpos algebraicamente cerrados, tienen una propiedad análoga. Este es el teorema de Dubois, descubierto por otro lado en forma ligeramente diferente por Risler [16].

Teorema de Dubois.

Sea K un cuerpo ordenado maximal. I un ideal de $K[X_1, \ldots, X_n]$ entonces $Id(V(I)) = \sqrt[R]{I}$ (radical real de I) definido por

$$\sqrt[R]{I} = \{ f \in K[X_1, \ldots, X_n] \mid \exists\, m \geq 1 , \quad \exists\, u_1, \ldots, u_r \in K[X_1, \ldots, X_n],$$

$$f^m (1 + \Sigma u_i^2) \in I \}$$

Es claro que $\sqrt[R]{I} \supseteq \sqrt{I}$; pero, es posible que estos ideales sean diferentes;

por ejemplo, si I es el ideal principal de $\mathbb{R}[X]$ engendrado por $1+X^2$, entonces $\sqrt{I} = I$ mientras que $\sqrt[R]{I}$ contiene 1 y por lo tanto es igual a $\mathbb{R}[X]$.

Un ideal tal que $\sqrt[R]{I} = I$ se llamará *ideal real*. Los ideales primos reales de $K[X_1, \ldots, X_n]$ están entonces en biyección con las variedades irreducibles de $K[X_1, \ldots, X_n]$ (K es naturalmente ordenado maximal) e igualmente en biyección con las K-álgebras enteras de tipo finito de la forma $K[X_1, \ldots, X_n]/P$ donde $P = \sqrt[R]{P}$ es un ideal primo. Estas álgebras se caracterizan porque su cuerpo de fracciones es ordenable. Los anillos de coordenadas de las variedades irreducibles de K^n tienen entonces la propiedad de que su cuerpo de fracciones es ordenable.

La demostración del teorema de Dubois utiliza el teorema de Artin. Esto hace creer que Hilbert, quien tenía el teorema de los ceros para los complejos, quería un teorema análogo para los reales y presentía que la demostración exigiría una respuesta previa al problema 17º.

2. *17º problema de Hilbert para las variedades reales.*

Sea K un cuerpo ordenado maximal, P un ideal primo real y $V = V(P)$. Sea $K(V)$ el cuerpo de fracciones de $K[X_1, \ldots, X_n]/P = K[\xi_1, \ldots, \xi_n]$.

Todo elemento de $K(V)$ se escribe f_1/f_2 donde $f_1, f_2 \in K[\xi_1, \ldots, \xi_n]$. Todo elemento $f \in K[\xi_1, \ldots, \xi_n]$ puede considerarse como una aplicación de V hacia K o como la restricción a $V \in K^n$ de una función polinomial $F \in K[X_1, \ldots, X_n]$.

Diremos que $f \in K(V)$ está definida en $x = (x_1, \ldots, x_n) \in V$ si f puede escribirse como $f = f_1/f_2$ donde $f_1, f_2 \in K[\xi_1, \ldots, \xi_n]$ y $f_2(x) \neq 0$.

De la misma manera, diremos que $f \in K(V)$ es *definida positiva sobre un*

conjunto si es positiva en todo punto de este conjunto donde está definida.

Podemos entonces preguntarnos si $f \in K(V)$ definida positiva sobre V es suma de cuadrados en $K(V)$.

Podemos mostrar que existen funciones $f \in K[\xi_1, \ldots, \xi_n]$ definidas positivas sobre V que no son restricción a V de funciones polinomiales $F \in K[X_1, .., X_n]$ definidas positivas sobre K^n. La respuesta no puede ser entonces una aplicación directa del teorema de Artin.

Utilizando un método de lógica análogo al expuesto anteriormente podemos demostrar que el problema admite una respuesta afirmativa : una función $f \in K(V)$ definida positiva es suma de cuadrados en $K(V)$.

Nosotros nos hemos interesado en el problema cuantitativo correspondiente.

Utilizando un lema de Pfister, se puede demostrar que $Pf(K(V)) \leq 2^d$ siendo d la dimensión de la variedad.

De otro lado, hacemos la conjetura siguiente :

$$d + 1 \leq Pf(K(V))$$

Esta conjetura ha sido demostrada en muchos casos por ejemplo, si $d = 1$, cuando V es una variedad racional o sea $K(V) = K[n_1, \ldots, n_d]$; cuando $K(V) = K[n_1, \ldots, n_d][\alpha]$ con $[K(V) : K[n_1, \ldots, n_d]]$ impar, o cuando V es una esfera real en el espacio $\mathbb{R}^3$.

3. 17º *problema de Hilbert, para las matrices simétricas.*

Ante todo, precisemos algunas definiciones.

Sea K un cuerpo ordenado y R una clausura real de K ; sea $A = (A_{ij})$ una matriz simétrica de orden n con coeficientes en K ; diremos que A es *positiva*

cuando la forma cuadrática asociada a A sobre R es positiva, es decir, cuando

$$\forall\ u = (u_1, \ldots, u_n) \in R^n\ ,\qquad \sum A_{ij}\, u_i\, u_j \geq 0\ .$$

Esta definición no depende de la escogencia de la clausura real R de K y permite definir una relación de orden sobre el grupo aditivo de las matrices simétricas de orden n con coeficientes en K. Este orden lo llamaremos *extensión natural* del orden de K.

Consideremos ahora un cuerpo cualquiera K. Una matriz simétrica A de orden n, con coeficientes en K se dirá *naturalmente positiva* si A es positiva para todo orden extensión natural de un orden de K.

Nosotros obtuvimos primeramente una generalización de un resultado de Ciampi [4] que puede expresarse gracias a las definiciones anteriores de la manera siguiente :

Sea K un cuerpo de característica diferente de 2. Una matriz simétrica con coeficientes en K es naturalmente positiva si y sólo si es suma de cuadrados de matrices simétricas con coeficientes en K. (resultado trivial si K es no ordenable).

Consideremos entonces matrices simétricas $F = (F_{ij})$ donde $F_{ij} \in K(X_1, .., X_m)$ siendo K ordenado maximal. Diremos que F es definida en el punto $x = (x_1, ..., x_m) \in K^m$ si podemos escribir para todo i, j

$$F_{ij} = \frac{G_{ij}}{H_{ij}}\ ;\quad G_{ij}, H_{ij} \in K[X_1, \ldots, X_m] \quad \text{y}$$

$$H_{ij}(x_1, \ldots, x_m) \neq 0\ .$$

Diremos que F es definida positiva sobre K^m si la matriz $F(x) = (F_{ij}(x))$ es

positiva en todo punto x donde está definida.

Utilizando nuevamente métodos de lógica análogos a los utilizados anteriormente, hemos demostrado que una matriz simétrica con coeficientes en $K(X_1, \ldots, X_m)$ (K ordenado maximal) es positiva definida si y sólo si es suma de cuadrados de matrices con coeficientes en $K(X_1, \ldots, X_m)$.

En el caso $n = 1$, encontramos nuevamente el teorema de Artin.

Podemos considerar entonces las cuestiones cuantitativas correspondientes y definir la constante de Pfister $Pf(n, m)$ para las matrices simétricas de orden n con coeficientes en el cuerpo $K(X_1, \ldots, X_m)$, K cuerpo ordenado maximal.

Es posible demostrar el resultado siguiente : $m + 1 \leq Pf(n, m) \leq 2^m$; la cota inferior se obtiene fácilmente, la cota superior es más difícil de obtener y para ello se utilizan los resultados del parágrafo 2 de esta parte.

Bibliografía

[1] E. Artin, "Uber die Zerlegung definiter Funktionen in Quadrate", Ann. Math. Sem. Hamburg 5 (1927) - p. 100-115.

[2] J. W. S. Cassels, "On the representation of rational functions as sums of squares", Acta Arithmetica IX (1964) - p- 79-82.

[3] J. W. S. Cassels - W. J. Ellison - A. Pfister, "On sums of squares and on elliptic curves over function fields" Journal of number theory - mai 1971-vol. 3 - nº 2.

[4] J. R. Ciampi, "Characterization of a class of matrices as sums of squares", Linear Algebra and its Applications 3, 1970, 45-50.

[5] J. G. Connel, "The Stufe of Number Fields", Math. Z. 124-20-22 (1972).

[6] D. W. Dubois - G. Efroymson, "Algebraic Theory of real varieties", Studies and Essays presented to Yu-Chen on his Sixtieth Birthday, 1970.

[7] D. Gondard "Sur le 17 eme probleme de Hilbert", These (3 eme cycle) - 1973- Orsay.

[8] D. Gondard - P. Ribenboim, "Fonctions définies positives sur les variétés réelles", (a paraître - Bulletin Soc. Math. 1974).

[9] D. Gondard - P. Ribenboim, "17 eme probleme de Hilbert pour les matrices", (a paraître, Bull. Sc. Math. 1974).

[10] D. Hilbert, "Mathematische Probleme", Gottinger Nach. (1900) p. 284-285.

[11] N. Jacobson, *Abstract Algebra*, vol. III.

[12] G. Kreisel et J. L. Krivine, *Eléments de logique mathématique - Théorie des modeles*, Dunod - Paris - 1967.

[13] A. Pfister, "Zur Darstellung definiter Funktionen als Summe von Quadraten", Invent. Math. 16 (1965) p. 363-370.

[14] Y. Pourchet, "Sur les représentations en sommes de carrés des polynômes a une indéterminée sur un corps de nombres algébriques", 1971 - Acta Arithmetica Wars. Zawa. t. 19 - p. 89-104.

[15] P. Ribenboim, *L'arithmétique des corps*, Hermann - 1972.

[16] J. J. Risler, "Une caractérisation des idéaux des variétés algébriques réelles", C. R. A. S. 271 - 1171-73 - 9 décembre 1970.

[17] A. Robinson, *Model Theory*.

Queen's University
Kingston, Ontario
Canadá