Un esempio di noce di Grothendieck: la soluzione di Artin-Schreier del 17^{mo} problema di Hilbert. [1]

Fabrizio Broglia [2]

Non so se il teorema che presento sia *il teorema piú bello* ma, a mio avviso, è un bel teorema e la sua bellezza, per me, risiede nel metodo usato per dimostrarlo: scopo infatti di questa seminario non è tanto illustrare un teorema in particolare ma piuttosto una procedura, un metodo in cui, per dare risposte a un problema invece di affrontarlo direttamente lo si pone in un contesto più vasto, magari creato apposta, e la risposta la si ottiene come conseguenza di questo allargamento di orizzonte.

Il teorema che ho scelto, e che ritengo un esempio significativo di questa procedura, è la soluzione data da Emil Artin nel 1927 ad uno dei problemi che Hilbert aveva posto nella sua celebre lista, il 17-esimo.

Il 17^{mo} problema di Hilbert.

Il problema è il seguente.

Un polinomio in n variabili a coefficienti reali non negativo su tutto $\mathbb{R}^n$ ammette una rappresentazione come somma di quadrati di funzioni razionali?

In altri termini

$$p(x) \in \mathbb{R}[x_1, \dots, x_n] \text{ e } \forall x \in \mathbb{R}^n \; p(x) \geqslant 0 \Longrightarrow p(x) = \Sigma_{i=1}^{p} f_i^2 \text{ con } f_i \in \mathbb{R}(x_1, \dots, x_n)?$$

Il problema nacque in occasione della discussione della tesi di Minkowski nel 1885, durante la quale egli asserí che gli sembrava improbabile che ogni forma non negativa potesse essere rappresentata come somma di quadrati di forme.

Come si vede, il problema nasce inizialmente come rappresentazione di polinomi (per *forma* si intende un polinomio omogeneo) come somma di quadrati di polinomi. Hilbert ci lavorò a lungo e arrivò a provare la seguente caratterizzazione.

Indichiamo con $P_{(n,m)}$ l'insieme delle forme in n variabili di grado m che sono non-negative su $\mathbb{R}^n$ e con $\Sigma_{(n,m)}$ il sottoinsieme di $P_{(n,m)}$ di quelle forme che sono somme di quadrati di polinomi. Chiaramente il confronto tra $P_{(n,m)}$ e $\Sigma_{(n,m)}$ è interessante solo nel caso che il grado m sia pari, altrimenti $P_{(n,m)} = \varnothing$.

Hilbert mostrò che l'uguaglianza $P_{(n,m)} = \Sigma_{(n,m)}$ valeva se e solo se $n \leqslant 2$ o $m = 2$ o $(n, m) = (3, 4)$ e altre proprietà come ad esempio che passando al campo delle funzioni razionali ogni $p \in \mathbb{R}[x, y]$ maggiore o uguale di zero è somma di 4 quadrati in $\mathbb{R}(x, y)$. Si noti che il caso delle forme di grado 2 segue direttamente dalla teoria

[1] Il titolo fa riferimento ad una frase di Grothendieck che, rispondendo a una domanda, disse che per aprire una noce la si può colpire con un martello e schiacciarla direttamente o immergerla in un liquido opportuno e lasciare che il liquido faccia l'opera e questo secondo era il modo da lui preferito.

[2] Conferenza tenuta al Dipartimento di Matematica di Pisa il 22 marzo per il ciclo "Il teorema più bello"

delle forme quadratiche: ogni forma quadratica in $P_{(n,2)}$ è somma di quadrati di forme lineari.

Hilbert non aveva però un controesempio esplicito che venne solo nel 1967 ad opera di Motzkin.

Il caso in una variabile

Nel caso dei polinomi in 1 variabile, ovverosia delle forme in 2 variabili, la soluzione discende direttamente dalla fattorizzazione in $\mathbb{R}[x]$. Ricordiamo che in $\mathbb{R}[x]$ i polinomi irriducibili hanno al più grado 2 e che un polinomio $p(x) = ax^2+bx+c, a \neq 0$ può sempre scriversi come $a\left((x+\frac{b}{2a})^2 - \frac{b^2-4ac}{4a^2}\right)$ e quindi, se $p(x) \geqslant 0 \quad \forall x \in \mathbb{R}$, allora $b^2 - 4ac \leqslant 0$ per cui o $p(x) = a(x+\alpha)^2$ o $p(x) = a\left((x+\frac{b}{2a})^2 + \left(\frac{\sqrt{4ac-b^2}}{2a}\right)^2\right)$, cioè $a > 0$ e il polinomio o è un quadrato o una somma di due quadrati.

Quindi, poiché un polinomio qualsiasi è prodotto di fattori lineari l_i con esponenti m_i e di fattori di grado 2 q_j con esponenti n_j cioè $p(x) = \Pi l_i^{m_i} \Pi q_j^{n_j}$, se $p(x) \geqslant 0$ si ha che tutti gli esponenti m_i sono pari e quindi il primo prodotto è un quadrato e il secondo una somma di quadrati. Val la pena di osservare che anche il numero totale di quadrati che interviene nell'espressione di p è limitato ed è 2, poiché il prodotto di due somme di 2 quadrati è ancora una somma di 2 quadrati: $(a^2+b^2)(c^2+d^2) = (ac-db)^2 + (ad+bc)^2$.

Il polinomio di Motzkin

L'esempio di polinomio maggiore o uguale a zero non somma di quadrati dato da Motzkin è il polinomio $m(x,y) = 1 + x^2y^2(x^2+y^2-3)$ che è positivo su tutto $\mathbb{R}^2$ in quanto la media aritmetica dei polinomi $1, x^2y, xy^2$ è maggiore o uguale della loro media geometrica. Il fatto che non sia somma di quadrati di polinomi discende da una verifica diretta: se infatti il polinomio m si potesse esprimere come somma di quadrati di polinomi s_i, questi dovrebbero avere al più grado 3. Inoltre in ogni s_i non potrebbero comparire monomi con x^3 o y^3 perché i coefficienti risultanti sarebbero positivi in quanto somme di quadrati e il polinomio m non contiene termini in x^6 o y^6. Analogamente si vede che negli s_i non possono esserci monomi puri del tipo x^2 o y^2 e x o y. Quindi ogni s_i è della forma $a_i + xy\ l_i$, con l_i di grado 1. Ma allora $\Sigma s_i^2 = \Sigma a_i^2 + x^2y^2\Sigma l_i^2 + ...$ e questo è impossibile perché il termine in $m(x,y)$ che moltiplica x^2y^2 cambia segno.

Anche se l'esempio di Motzkin è di molto posteriore, ben si presta ad illustrare la richiesta di Hilbert: un calcolo esplicito mostra infatti che il polinomio è in effetti somma di quadrati di funzioni razionali:

$$(x^2+y^2+1)m(x,y) =$$
$$= (x^2y-y)^2 + (xy^2-x)^2 + (x^2y^2-1)^2 + \frac{1}{4}(xy^3-x^3y)^2 + \frac{3}{4}(xy^3+x^3y-2xy)^2$$

Soluzione di Emil Artin.

Il problema di Hilbert fu risolto nel 1927 da Emil Artin che lo affrontò non direttamente ma nel contesto della teoria dei campi ordinabili, teoria creata da lui e Otto Schreier probabilmente a questo scopo. In questa classe di corpi risulta infatti possibile caratterizzare gli elementi che sono somme di quadrati.

Teorema 1. *In un corpo ordinabile le somme di quadrati sono gli elementi positivi in tutti gli ordini.*

Il corpo delle funzioni razionali, come vedremo, è un corpo ordinabile, e lo è in vari modi, pertanto al fine di rispondere alla domanda di Hilbert si tratta di mettere in relazione per un polinomio l'essere positivo come funzione da $\mathbb{R}^n$ a $\mathbb{R}$ con l'essere positivo in ogni ordine del corpo $\mathbb{R}(X)$ delle fuzioni razionali, e questo è appunto il contenuto del prossimo teorema.

Teorema 2. *Se $K = \mathbb{R}(x_1, \ldots, x_n)$ è il corpo delle funzioni razionali e p un polinomio, esiste un ordine β in K in cui p è positivo se e solo se esiste un punto $y \in \mathbb{R}^n$ tale che $p(y) > 0$.*

Questo basta a risolvere il problema di Hilbert, perché se esistesse un ordine del corpo delle funzioni razionali in cui p non fosse positivo, esisterebbe un punto $y \in \mathbb{R}^n$ dove p sarebbe negativo e questa sarebbe una contraddizione.

Un verso del teorema 2 è ovvio: se $\overline{y}$ è un punto di $\mathbb{R}^n$ e $p(\overline{y}) \geqslant 0$ allora p è positivo nell'ordine generato dal cono dei polinomi positivi in $\overline{y}$. La parte delicata è il viceversa e per questo esaminiamo rapidamente la teoria di Artin-Schreier.

Campi reali

Un *campo reale* è un campo ordinabile cioè con almeno una relazione d'ordine totale $\leqslant$ compatibile con la struttura di campo, ovverosia tale che

- Se $x \leqslant y$ allora $\forall z \in K \; x + z \leqslant y + z$
- Se $x \geqslant 0$ e $y \geqslant 0$ allora $xy \geqslant 0$

In un campo reale indubbiamente i quadrati sono positivi poiché o $x \geqslant 0$ e quindi $x^2 \geqslant 0$ o $-x \geqslant 0$ e quindi ancora $x^2 = (-x)(-x) \geqslant 0$.

Inoltre un campo ordinabile ha caratteristica 0: infatti 1, essendo un quadrato, è positivo e, poiché $1 \neq 0$, $1 > 0$. Quindi $1 + \ldots + 1 > 1 > 0$. Pertanto un campo ordinabile contiene il campo dei razionali $\mathbb{Q}$.

In definitiva in un campo reale K, il sottoinsieme P degli elementi non negativi in un determinato ordine verifica

(1) $P + P \subset P$, $P \cdot P \subset P$
(2) $K^2 \subset P$
(3) $-1 \notin P$
(4) $P \cup (-P) = K$

Chiameremo *cono proprio* un sottoinsieme di K che verifichi (1),(2) e (3) in quanto la condizione (3) assicura la non banalità del cono P; infatti se -1 fosse in P anche

ogni elemento di K sarebbe in P dato che $\forall a \in K$ si ha $4a = (a+1)^2 - (a-1)^2$ e quindi, poiché un corpo ordinabile ha caratteristica 0, a sarebbe somma di quadrati.

Chiameremo *cono d'ordine* un cono proprio che verifichi anche (4).

Per provare il primo dei risultati enunciati ci saranno utili le seguenti proposizioni.

Proposizione 0.1. *Sia P un cono proprio. Se $-a \notin P$ allora $P[a] = \{x + ay, x, y \in P\}$ lo è.*

Prova Il fatto che $P[a]$ sia un cono è una verifica diretta. Se P non fosse proprio allora $-1 \in P$, cioè $-1 = x + ay$ con $x, y \in P$. Poiché P è proprio, $-1 \notin P$ quindi $y \neq 0$, il che implica che $-a = \frac{x+1}{y} = \frac{y(x+1)}{y^2}$ da cui si avrebbe che $-a \in P$. Contraddizione. □

Proposizione 0.2. *Se un campo contiene un cono proprio allora è ordinabile.*

Dimostrazione. Poiché i coni propri sono un insieme parzialmente ordinato per inclusione e ogni catena contiene un elemento massimale, esiste un cono massimale Q. Occorre provare che tale cono è un ordine, cioè $Q \cup (-Q) = K$.

Sia pertanto $k \in K$: se $k \notin Q$, $Q[-k]$ è un cono proprio che contiene Q. Per la massimalità di Q si ha $Q = Q[-k]$ cioè $-k \in Q$. □

In definitiva, riassumendo, abbiamo la seguente caratterizzazione dei campi reali.

Teorema Sia K un campo. Le seguenti proprietà sono equivalenti

(1) K è ordinabile
(2) K ha un cono proprio
(3) $-1 \notin \Sigma K^2$
(4) Per ogni $x_1, \ldots, x_n \in K$

$$\Sigma x_i^2 = 0 \Rightarrow x_1 = \ldots = x_i = 0$$

Possiamo quindi provare il Teorema 1 che caratterizza le somme dei quadrati in un campo, cioè che in un campo ordinabile K l'insieme delle somme dei quadrati ΣK^2 è l'intersezione di tutti i coni positivi di tutti gli ordini.

Dimostrazione. Ovviamente $\Sigma K^2 \subset P$ per ogni cono proprio e quindi $\Sigma K^2 \subset \bigcap P$. Per mostrare l'uguaglianza sia $a \in \bigcap P \setminus \Sigma K^2$. Poiché ΣK^2 è un cono proprio e $a \notin \Sigma K^2$ per la proposizione 01 $\Sigma K^2[-a]$ è un cono proprio e quindi K ha un cono d'ordine che non contiene a, cioè esiste un ordine in cui a non è positivo. □

Qualche esempio.

Ovviamente $\mathbb{R}$ è un campo reale con un solo ordine dove tutti i positivi sono quadrati mentre $\mathbb{C}$ non lo è poiché in particolare -1 è un quadrato:$-1 = i^2$

Anche il campo delle funzioni razionali $\mathbb{R}(x)$ è un campo reale, ma non ammette un solo ordine. Per dare un ordine in tale campo è sufficiente darlo sull'anello $\mathbb{R}[x]$ poiché $\frac{p}{q} = \frac{pq}{q^2}$. Poiché $\mathbb{R} \subset \mathbb{R}[x]$ un ordine su $\mathbb{R}[x]$ deve estendere l'ordine di $\mathbb{R}$,

quindi per dare un ordine occorre conoscere la posizione di x rispetto a $\mathbb{R}$. Poniamo ad esempio $0 < x < a \ \forall a > 0, a \in \mathbb{R}$

Risulta ovviamente $0 < \ldots < x^n < \ldots < x^2 < x < 1$ e il segno di un polinomio resta determinato dal segno del suo monomio di grado minimo.

Questo procedimento si può ripetere in molti modi, per esempio ponendo x a sinistra di 0 o rimpiazzare 0 con qualsiasi numero reale a o anche porre $x < a \forall a \in \mathbb{R}$ o $x > a \forall a \in \mathbb{R}$

Naturalmente con tutti questi ordinamenti $\mathbb{R}(x)$ non è archimedeo.

In più variabili vi sono anche altri modi per dare ordinamenti su $\mathbb{R}[x_1, \ldots, x_n]$ che non si riducono semplicemente allo stabilire ricorsivamente la posizione delle veriabili. Per maggiori dettagli si può vedere ad esempio [BCR].

Campi reali chiusi

La nozione di campo reale è ancora troppo generale: al fine di aumentare la somiglianza con il campo dei reali poniamo una richiesta di massimalità.

Definizione 0.3. Un campo reale si dice *reale chiuso* se è massimale rispetto alle estensioni algebriche ordinate, cioè K reale chiuso $\Longrightarrow$ se K_1 è una estensione algebrica di K allora K_1 non è ordinabile.

Per i campi reali chiusi vale la caratterizzazione seguente

Teorema 0.4. *Per un campo K sono fatti equivalenti*

(1) *K è reale chiuso.*
(2) *K ammette un solo ordine in cui i positivi sono quadrati e ogni polinomio di grado dispari ha uno zero.*
(3) *L'estensione $K[i] = \dfrac{K[X]}{(x^2+1)}$ è algebricamente chiusa.*

Osservazione 0.5.
(1) Ovviamente il campo dei reali è un campo reale chiuso, ma non è il più piccolo. Ad esempio il suo sottocampo $\mathbb{R}_{\text{alg}}$ dei numeri reali algebrici è anche lui reale chiuso per la proprietà (3): infatti $\mathbb{R}_{\text{alg}}[i] = \mathbb{C}_{\text{alg}}$ che è la chiusura algebrica di $\mathbb{Q}$.
(2) La proprietà (3) dice in particolare che per i polinomi a coefficienti in un corpo reale chiuso vale una fattorizzazione perfettamente analoga a quella per i polinomi a coefficienti in $\mathbb{R}$.

Una ulteriore osservazione da fare è che per i polinomi a coefficienti in un campo reale chiuso valgono gli usuali teoremi dell'analisi, in particolare vale il teorema di Rolle, del valor medio, degli zeri e della permanenza del segno. Per le dimostrazioni si veda [BCR].

Chiusura reale

Il risultato importante di Artin-Schreier è che per un campo reale, fissato un ordine, esiste una estensione algebrica reale chiusa.

Teorema. Sia K un campo ordinato da un ordine β. Esiste un campo reale chiuso, estensione algebrica di K il cui unico ordine induce l'ordine β su K.

Si dimostra inoltre che tale campo è unico a meno di isomorfismi che conservano l'ordine e viene detto *chiusura reale di K rispetto all'ordine β.*

L'idea della prova è la seguente. Sia $\overline{K}$ una chiusura algebrica di K. Si consideri la famiglia dei campi F contenenti K e contenuti in $\overline{K}$ che siano ordinati con un ordine che estende β. A tale famiglia si può applicare il lemma di Zorn e si verifica che un elemento massimale è una chiusura reale.

Il teorema di Artin

Il risultato che porta alla risposta per il 17^{mo} problema di Hilbert è il Teorema 2 che riformuliamo in questo modo

Teorema (A_n) Sia $\mathbb{R}(X) = \mathbb{R}(x_1, \ldots, x_n)$ il campo delle funzioni razionali, β un ordine su tale campo e $p_1, \ldots, p_k$ polinomi. I polinomi p_i sono positivi nell'ordine β se e solo se esiste un punto $y \in \mathbb{R}^n$ tale che $p_i(y) > 0 \forall i$.

Osservazione 0.6. Se A è una algebra di polinomi in n variabili, un omomorfismo di algebre $\varphi : A \to \mathbb{R}$ è la valutazione dei polinomi dell'algebra nel punto $(\varphi(x_1), \ldots, \varphi(x_n)) \in \mathbb{R}^n$.

Per provare il teorema utilizzeremo il seguente risultato ausiliario.

Teorema (B_n) Sia A un'algebra finitamente generata su $\mathbb{R}$ di dimensione n integra e ordinabile e sia $f \in A$ non nullo. Allora esiste un omomorfismo di $\mathbb{R}$-algebre $\varphi : A \to \mathbb{R}$ tale che $\varphi(f) \neq 0$.

Vediamo come il risultato ausiliario in dimensione $n-1$ implichi il teorema di Artin in dimensione n, cioé $B_{n-1} \Rightarrow A_n$.

Dimostrazione. Indichiamo rispettivamente con $\mathbb{F}_n$ e $\mathbb{F}_{n-1}$ le chiusure reali dei corpi $\mathbb{R}(x_1, \ldots, x_n)$ e $\mathbb{R}(x_1, \ldots, x_{n-1})$ rispetto all'ordine β e all'ordine indotto. I polinomi p_i, che non è restrittivo supporre monici, pensati come elementi di $\mathbb{F}_{n-1}[x_n]$, ammettono per quanto detto nell'osservazione (2) CITARE una fattorizzazione del tipo

$$p_i = \Pi(x_n - a_{i,j})^{n_{i,j}} \Pi((x_n + b_{i,j})^2 + c_{i,j}^2)^{m_{i,j}}$$

dove, per ogni i le $a_{i,j}$ sono le radici in F_{n-1} del polinomio p_i e i $b_{i,j}$ e $c_{i,j}$ sono la parte reale e la parte immaginaria delle radici di p_i in $\mathbb{F}_{n-1}[i]$.

Sia $\{\alpha_s\}$ l'insieme delle radici in $\mathbb{F}_{n-1}$ dei p_i ordinato secondo l'ordine β, nel senso che $\alpha_s <_\beta \alpha_{s+1}$. Quindi il segno dei polinomi nell'ordine β è determinato dalla posizione di x_n rispetto alle radici α_s.

Supponiamo che nell'ordine β si abbia $\alpha_h < x_n < \alpha_{h+1}$ e sia θ un elemento di $\mathbb{F}_{n-1}$ nella stessa posizione di x_n rispetto alle radici, cioè $\alpha_h < \theta < \alpha_{h+1}$. Risulta quindi per ogni s, $\theta - \alpha_s = \pm e_s^2$.

Consideriamo la $\mathbb{R}$-algebra A generata da $\mathbb{R}[x_1, \ldots, x_{n-1}]$ e dai numeri $\theta, a_{i,j}, b_{i,j}, c_{i,j}, e_s$ che appaiono nelle rappresentazioni dei p_i. Sia f il prodotto in A di tutti gli elementi

$c_{i,j}, e_s$. L'algebra A è contenuta in $\mathbb{F}_{n-1}$ perché gli elementi con cui abbiamo esteso $\mathbb{R}[x_1, \ldots, x_{n-1}]$ appartengono a $\mathbb{F}_{n-1}$ e quindi sono algebrici su $\mathbb{R}(x_1, \ldots, x_{n-1})$. Pertanto l'algebra A è integra, ordinata e di dimensione $n-1$ e quindi per B_{n-1} esiste un morfismo di $\mathbb{R}$-algebre $\varphi : A \to \mathbb{R}$ tale che $\varphi(f) \neq 0$. Possiamo costruire $\psi : \mathbb{R}[x_1, \ldots, x_n] \to \mathbb{R}$ ponendo

- $\psi(x_j) = \varphi(x_j)$ per $j = 1, \ldots, n-1$
- $\psi(x_n) = \varphi(\theta)$

Osserviamo che la condizione $\varphi \neq 0$ implica $\varphi(\theta) - \varphi(\alpha_s) = \pm\varphi(e_s)^2 \neq 0$ e $\varphi(\alpha_s) < \varphi(\theta)$ e quindi $\psi(p_i) = p_i(\psi(x_1), \ldots, \psi(x_{n-1}), \psi(x_n))$ ha per costruzione lo stesso di p_i rispetto a *beta*. □

Siamo quindi ricondotti a provare il risultato ausiliario.

Esso può essere ottenuto come conseguenza dello stesso teorema di Artin nella stessa dimensione, cioè $A_n \Rightarrow B_n$.

In definitiva avremo provato $A_n \Rightarrow B_n \Rightarrow A_{n+1}$. Poiché A_0 e B_0 risultano banalmente veri, il teorema di Artin, che implica una risposta positiva alla questione posta da Hilbert, risulta provato per induzione.

Per provare il teorema ausiliario utilizzeremo un ulteriore strumento: il teorema di Sturm.

Il teorema di Sturm.

Il teorema di Sturm è un teorema di localizzazione delle radici di un polinomio in una variabile a coefficienti reali. Se $p(T) \in \mathbb{R}[T]$, la successione di Sturm di $p(T)$ è la successione di polinomi cosí definita.

- $f_0 = p$
- $f_1 = p'$
- f_2 il resto della divisione euclidea tra f_0 e f_1 cambiato di segno
- ....
- $f_{k-2} = f_{k-1}q - f_k$
- ....
- Ultimo polinomio: il Massimo Comun Divisore tra f_0 e f_1

Per ogni numero reale c consideriamo la successione numerica $f_i(c)$ e indichiamo con $V(p, c)$ il numero delle variazioni di segno in questa successione, trascurando gli zeri.

Teorema (Sturm) Sia $p(T) \in \mathbb{R}[T]$ un polinomio a coefficienti reali, a, b due numeri reali con $a < b$ tali che $p(a) \cdot p(b) \neq 0$. Allora il numero di zeri del polinomio p nell'intervallo (a, b) è pari alla differenza $V(p, a) - V(p, b)$

Per dare una idea della prova supponiamo che il polinomio non abbia fattori multipli e quindi che il MCD $(p, p') = \text{cost} \neq 0$.

Osserviamo che allora due termini consecutivi della successione di Sturm non possono annullarsi nello stesso punto c, altrimenti tutti quelli seguenti si annullerebbero compreso il MCD.

Quindi si verifica agevolmente che il passaggio attraverso uno zero di un f_i con $i > 0$, per la permanenza del segno, non comporta variazioni in V perché i segni di $f_{i-1}((c))$ e $f_{i+1}(c)$ sono opposti. Nel caso invece che lo zero sia di $f_0 = p$ si vede, per il fatto che $f_1(c) \neq 0$, che a prescindere dal suo segno il numero delle variazioni cala di 1 passando attraverso c.

Nel caso in cui il MCD tra p e p' non sia costante la prova è simile.

Osservazione. La prova del teorema di Sturm si basa essenzialmente sul teorema di Rolle e le sue conseguenze. Poiché in un campo reale chiuso vale ancora il teorema di Rolle, ne segue che anche il teorema di Sturm resta valido per polinomi a coefficienti in un campo reale chiuso.

Prova $A_n \Rightarrow B_n$**.**

Sia A una $\mathbb{R}$-algebra finitamente generata cioè $A = \dfrac{\mathbb{R}[x_1, \ldots, x_d]}{\mathfrak{a}}$. Supponiamo A integra e ordinabile, quindi $\mathfrak{a}$ deve essere primo e deve verificare $a_1^2 + \ldots + a_k^2 \in \mathfrak{a} \Rightarrow a_i \in \mathfrak{a}\ \forall i$, perché q.f.$A$, il campo dei quozienti di A, deve essere reale.

Poiché A ha dimensione n, è noto **CITARE** che a meno di un cambio lineare di coordinate si può supporre

- $\mathbb{R}[x_1, \ldots, x_n] \subset A$.
- A intera su $\mathbb{R}[x_1, \ldots, x_n]$.
- q.f.A è generato su $\mathbb{R}(x_1, \ldots, x_n)$ da un elemento $\theta \in A$.
- Sia $p(T)$ il polinomio minimo di θ e δ il suo discriminante, cioè il risultante tra p e la sua derivata p'. Allora si ha $\delta A = R[x_1, \ldots, x_n][\theta]$.

Sia ora f un elemento di A diverso da 0. Pertanto δf è un polinomio in θ: $\delta f = q(\theta)$. Per l'irriducibilità di p, q e p sono coprimi e quindi per il teorema di Bézout esistono polinomi $a(t)$, $b(t)$ tali che si ha $a(t)p(t) + b(t)q(t) = h$, dove h è un polinomio non nullo in $x_1, \ldots . x_n$.

Calcolando questa relazione in θ si ottiene $b(\theta)\delta f = h$. Se vogliamo trovare un morfismo di $\mathbb{R}$-algebre φ da A a $\mathbb{R}$ ci serve che

- $\varphi(h) \neq 0$
- $\varphi(\delta) \neq 0$
- $\varphi(\theta)$ sia una radice di $\varphi(p)$.

A tal fine usiamo il teorema di Sturm per il polinomio $p(t)$ pensato a coefficienti nella chiusura reale F del campo $\mathbb{R}(x_1, \ldots, x_n)$ ordinato dall'ordine di A. Fissata una successione di Sturm $f_1, \ldots, f_k$ per $p(t)$ e $M \in \mathbb{R}$ tale che $-M < \theta < M$ si ha che per tale successione $V(p, -M) - V(p, M) \neq 0$ perché p ha una radice in $(-M, M)$.

Consideriamo quindi la lista $\delta, h, f_1(-M), \ldots, f_k(-M), f_1(M), \ldots, f_k(M)$: per A_n esiste un morfismo di $\mathbb{R}$ algebre $\psi : \mathbb{R}[x_1, \ldots x_n]$ $to\mathbb{R}$ che conserva il segno di tutti questi polinomi. Dunque $\psi(f_1), \ldots, \psi(f_k)$ è una successione di Sturm per $\psi(p((t)))$ e poiché $V(\psi(p), -M) - V(\psi(p), M) \neq 0$ il polinomio $\psi(p)$ deve avere una radice T in $(-M, M)$.

Ricordando che $A = \delta^{-1}R[x_1, \ldots, x_n][\theta]$, possiamo definire $\varphi : A \to \mathbb{R}$ ponendo

$\varphi(x_i) = \psi(x_i)$ per $i = 1, \ldots, n$
$\varphi(\delta^{-1}) = (\psi(\delta))^{-1}$
$\varphi(\theta) = T$

Per costruzione risulta $\varphi(f) \neq 0$

Considerazioni finali.

Del teorema di Artin si possono dare molte prove, quasi tutte basate più o meno sullo stesso ordine di idee.

Quella riportata non è quella originaria ma ha il pregio di essere molto vicina a quella del teorema degli zeri (Nullstellensatz), che in effetti si può ottenere con lievi modificazioni degli argomenti. Il Nullstellensatz che si ottiene ha una forma simile a quella complessa: precisamente, nel caso dell'anello A dei polinomi a coefficienti reali in n variabili, si ha per l'ideale $I(V(\mathfrak{a}))$ dei polinomi che si annullano sul luogo di zeri $V(\mathfrak{a})$ di un ideale $\mathfrak{a} \subset A$ la caratterizzazione seguente

$$I(V(\mathfrak{a})) = \{p \in A | \exists q_i \in A \; p^{2m} + \Sigma q_i^2 \in \mathfrak{a}\} = \sqrt[\mathbb{R}]{\mathfrak{a}}\}$$

.

La parte a destra del segno = viene usualmente detta radicale reale di $\mathfrak{a}$e indicata con $\sqrt[\mathbb{R}]{\mathfrak{a}}\}$.

Un tale risultato va nella direzione di svincolare lo studio della geometria algebrica sul corpo $\mathbb{R}$ da quella complessa. In effetti la geometria algebrica reale nel secolo scorso ha avuto un grande sviluppo, entrando anche in relazione con altri settori tra cui in particolare la logica e la teoria delle forme quadratiche.

Un altro aspetto del 17$^{\text{mo}}$ problema di Hilbert è quello quantitativo, nel senso se sia possibile o meno dare una maggiorazione uniforme sul numero dei quadrati necessari nella rappresentazione di una funzione positiva come somma di quadrati. Ad esempio, abbiamo visto che nel caso di polinomi in una variabile ogni polinomio non negativo si può rappresentare come somma di al più 2 quadrati.

La rappresentazione di funzioni non negative come somme di quadrati ha senso per un gran numero di algebre di funzioni: ad esempio Fefferman e Phong hanno provato che ogni funzione $C^{3,1}$ non negativa si può rappresentare come somma di quadrati di funzioni $C^{1,1}$.**metterci Bony**

Parlando di funzioni analitiche, nell'affrontare un problema è conveniente distinguere il caso locale dal caso globale: in genere il caso locale, cioè quello per l'algebra dei germi di funzioni, non differisce molto da quello algebrico per via del teorema di preparazione di Weierstrass, mentre quello globale generalmente presenta difficoltà maggiori. Il 17$^{\text{mo}}$ problema di Hilbert non fa eccezione e infatti il caso locale, proprio facendo leva sul teorema di preparazione di Weierstrass, è risolto mentre quello globale è ancora aperto.

Nel caso analitico globale però, a fronte di una carenza di risultati si hanno in compenso enunciati più precisi.

Per un'algebra A si chiama *numero di Pitagora* il numero, se esiste, $p(A)$ tale che ogni somma di quadrati si può esprimere come somma di $p(A)$ quadrati. Se tale numero non esiste si pone $p(A) = +\infty$.

Per il numero di Pitagora dell'algebra dei polinomi si hanno soltanto stime; in ogni caso il problema quantitativo è del tutto indipendente dal quello qualitativo.

Nel caso analitico globale si ha invece un legame tra i due aspetti qualitativo e quantitativo del 17^{mo} problema di Hilbert dato dal seguente risultato.

Teorema Se ogni ogni funzione analitica globale su $\mathbb{R}^n$ maggiore o uguale di 0 ammette una rappresentazione come somma di un numero finito di quadrati di funzioni meromorfe, allora esiste un numero p per cui ogni funzione non negativa è somma di al più p quadrati di funzioni meromorfe.

Cioè se il problema di Hilbert ammette una soluzione finita per ogni funzione analitica non negativa su $\mathbb{R}^n$ allora il numero di Pitagora del campo delle funzioni meromorfe è finito.

Riferimenti bibliografici

[ABF] Acquistapace, F.; Broglia, F.; Fernando, J. F.: On Hilbert's 17th problem and Pfister's multiplicative formulae for the ring of real analytic functions. *Ann. Sc. Norm. Super. Pisa Cl. Sci. (5) 13 (2014), no. 2, 333–369.*

[A] Artin, E.: Über die Zerlegung definiter Funktionen in Quadrate. *Abh. Math. Sem. Univ. Hamburg 5 (1927), no. 1, 100–115.*

[AS1] Artin, E.; Schreier, O.: Algebraische Konstruktion reeller Körper. *Abh. Math. Sem. Univ. Hamburg 5, (1927) no. 1, 85–99.*

[AS2] Artin, E.; Schreier, O.: Eine Kennzeichnung der reell abgeschlossenen Körper. *Abh. Math. Sem. Univ. Hamburg 5 (1927), no. 1, 225–231.*

[BCR] Bochnak, J. and Coste, M. and Roy, M.-F.: Géométrie algébrique réelle, *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*,**12**, Springer-Verlag, Berlin,

[M] Motzkin, T. S.: The arithmetic-geometric inequality. *1967 Inequalities (Proc. Sympos. Wright-Patterson Air Force Base, Ohio, 1965) pp. 205–224 Academic Press, New York*

[T] Tataru, D.: On the Fefferman-Phong inequality and related problems. *Comm. Partial Differential Equations 27, no. 11-12, 2101–2138.*