Un'applicazione della 'geometria diofantea non-standard' al teorema di irriducibilità di Hilbert

Vincenzo Mantova

21/04/2010

Teorema di irriducibilità di Hilbert

Teorema 1 (Hilbert [Hil92])**.** *Sia $f(X,T)$ un polinomio in $\mathbb{Q}[X,T]$ irriducibile su $\mathbb{Q}(T)$. Esistono allora infiniti $t \in \mathbb{Q}$ tali che $f(X,t)$ è irriducibile su $\mathbb{Q}$.*

Esempio 2. Il polinomio $X^2 - T$ è irriducibile su $\mathbb{Q}(T)$, e per ogni $t \in \mathbb{Q} \setminus \mathbb{Q}^2$ anche $X^2 - t$ è irriducibile su $\mathbb{Q}$.

Questa proprietà vale anche per campi di numeri e campi di funzioni. Dunque scriviamo la generalizzazione:

Definizione 3. Un campo k si dice *Hilbertiano* se per ogni polinomio in $k[X,T]$ irriducibile e separabile su $k(T)$, esistono infiniti $t \in k$ tali che $f(X,t)$ è irriducibile su k.

Esempio 4. Oltre a campi di numeri e campi di funzioni, altri campi sono Hilbertiani: ad esempio, $\mathbb{Q}^{\mathrm{ab}}$ (l'estensione di $\mathbb{Q}$ con tutte le radici dell'unità). Campi evidentemente non Hilbertiani sono i campi algebricamente chiusi. Un esempio più sottile di campo non Hilbertiano è $\mathbb{Q}^{\mathrm{solv}}$ (la massima estensione risolubile di $\mathbb{Q}$, poiché risolve tutti i radicali e quindi tutti i polinomi di grado fino a 4).

Lemma 5. *Se k è Hilbertiano, allora per ogni collezione finita di polinomi $f_1, \dots, f_n$ in $k[X,T]$, irriducibili su $k(T)$, esistono infiniti $t \in k$ tali che gli $f_1(X,t), \dots, f_n(X,t)$ sono tutti irriducibili su k.*

Sia ora k un campo e sia ${}^*k$ una qualsiasi estensione $|k|^+$-satura nel linguaggio $\{0,1,+,\cdot\}$.

Osservazione 6. L'estensione ${}^*k/k$ è regolare (o anche detta geometrica), ossia k è algebricamente chiuso in ${}^*k$.

Teorema 7 (Roquette [Roq75])**.** *Il campo k è Hilbertiano se e solo se esiste un $t \in {}^*k \setminus k$ tale che $k(t)$ è separabilmente chiuso in ${}^*k$.*

Dimostrazione. L'insieme $p(y)$ delle formule $\varphi_f(y)$ che dicono che $f(X,y)$ è irriducibile, al variare di f tra i polinomi indicati nella Definizione 3, è finitamente soddisfacibile per il Lemma 5 ed è quindi un tipo. Dato che è un tipo a parametri in k, è realizzato da un t in ${}^*k$, e dire che $f(X,t)$ è sempre irriducibile su ${}^*k$ significa esattamente che $k(t)$ è separabilmente chiuso in ${}^*k$. □

Definizione 8. Se t è un elemento in $^*k \setminus k$, sia Ω_t la chiusura separabile di $k(t)$ in k.

Teorema 9 (Weissauer [Wei82])**.** *Il campo k è Hilbertiano se e solo se esiste un $t \in {}^*k \setminus k$ ed un posto di $k(t)/k$ che ha solo un numero finito di estensioni a Ω_t.*

Dimostrazione. Se k è Hilbertiano, il Teorema 7 dà un t tale che $k(t) = \Omega_t$, per cui la conseguenza è banale.

Se invece non lo è, si prenda un polinomio $f(X,T)$ che confuti l'Hilbertianità; avrà grado maggiore di 1 in X. Dato che i valori $t \in k$ per cui $f(X,t)$ è irriducibile sono in numero finito, per ogni $t \in {}^*k \setminus k$ abbiamo che $f(X,t)$ è riducibile in $^*k$. Sia F il campo di spezzamento di $f(X,t)$ su $k(t)$. Si prenda P di grado 1 in $k(t)/k$ non ramificato in F (esiste per separabilità di f), si considerino gli automorfismi di $k(t)/k$ che lo lasciano fisso e li si estenda alla chiusura algebrica di $k(t)$. Chiamiamo il gruppo di automorfismi che ne risulta Φ.

Dato che l'estensione $F \cap {}^*k$ è propria e regolare (i.e. $F \cap \overline{k} = k$), ha almeno un punto di ramificazione che sarà distinto da P. Allora il composto $F^\Phi \cap {}^*k := \prod_{\phi\in\Phi} F^\phi \cap {}^*k$ ha infiniti punti di ramificazione, quindi ha grado infinito su $k(t)$. Dato che il campo residuo di P non cambia a meno di automorfismo su k e non c'è ramificazione, allora ha infinite estensioni a F^Φ e in particolare anche a Ω_t.

Se P non è ramificato o di grado 1 basta sostituire t con un'opportuna sua funzione razionale su k. $\square$

Definizione 10. Un elemento $t \in {}^*k$ si dice *polo-finito* se $t \notin k$ e il posto $t = \infty$ di $k(t)/k$ ha un numero finito di estensioni in Ω_t.

Corollario 11. *Il campo k è Hilbertiano se e solo se $^*k$ ha un almeno un elemento polo-finito.*

Formula del prodotto

Un campo k si dice con *formula del prodotto* se esiste una famiglia M di valori assoluti su k non banali a valori in $\mathbb{R}^+$ tali che:

1. l'insieme $\{v \in M \mid |x|_v \neq 1\}$ è finito per ogni $x \in k^\times$;
2. per ogni $x \in k$ si ha $\prod_{v\in M} |x|_v = 0$.

Esempio 12. Il campo $\mathbb{Q}$ ha una formula del prodotto data dai valori assoluti p-adici insieme al valore assoluto archimedeo, e questa formula si estende a tutti i campi di numeri. Il campo di funzioni di una curva ha pure una formula del prodotto: le valutazioni sono l'ordine di zero delle funzioni nei vari punti, e il prodotto banale è dovuto al fatto che la somma delle molteplicità degli zeri e la somma delle molteplicità dei poli coincidono.

Notazione: passeremo alla notazione additiva usando il logaritmo, scriveremo $v(x) := -\log(|x|_v)$ e chiameremo impropriamente le v 'valutazioni'. La formula del prodotto diventa quindi una formula 'della somma'.

Per formalizzare al prim'ordine la teoria, usiamo un linguaggio a tre sorte k, $\mathbb{R}$, M, il primo con struttura di campo, il secondo con struttura di gruppo ordinato e il terzo con un solo simbolo di funzione $\mathrm{eval} : k \times M \to \mathbb{R}$. Il punto 2 può essere assiomatizzato con lo schema di assiomi 'se le valutazioni non nulle sono al più n, la loro somma è nulla'.

Sia $(k, \mathbb{R}, M)$ un campo con formula del prodotto e sia $({}^*k, {}^*\mathbb{R}, {}^*M)$ una sua arbitraria estensione κ-satura, con $\kappa = |k| + |\mathbb{R}| + |M|$.

Definizione 13. Se quozientiamo ${}^*\mathbb{R}$ per l'inviluppo convesso di $v(k^\times)$, otteniamo un gruppo ordinato che chiameremo $\dot{\mathbb{R}}_v$. Sia $\dot{M}$ l'insieme delle valutazioni $\dot{v} : {}^*k \to \dot{\mathbb{R}}_v$. Notiamo che queste valutazioni devono necessariamente essere tutte non-archimedee, quindi l'insieme $\dot{\mathcal{O}} := \{x \in {}^*k \mid \forall \dot{v} \in \dot{M},\ \dot{v}(x) \geq 0\}$ è un anello.

Definizione 14. Sia Ω una sottoestensione di ${}^*k/k$ di grado di trascendenza 1 su k. Diremo che Ω è *M-aritmetico* se ogni posto di Ω/k è indotto da una valutazione $\dot{v} \in \dot{M}$.

Teorema 15. *Sia $t \in {}^*k \setminus k$ tale che Ω_t è M-aritmetico. Se l'insieme $\{\dot{v} \in \dot{S} \mid \dot{v}(x) < 0\}$ è finito, allora k è Hilbertiano.*

Dimostrazione. L'insieme dei posti sopra $t = \infty$ coincide con l'insieme di valutazioni dato sopra per definizione di M-aritmeticità, quindi è finito. Ma allora t è polo-finito, e k è Hilbertiano per il Teorema 11. □

Lemma 16. *Dato $x \in \dot{\mathcal{O}}$, allora l'insieme $\{v \in {}^*M \mid v(x) < 0\}$ è finito e contenuto in M.*

Dimostrazione. Innanzitutto, se $x \in k$ la conclusione è automatica per definizione di formula del prodotto, e poiché è un insieme finito definito in k, per $v \in {}^*M \backslash M$ deve valere $v(k^\times) = 0$. In particolare abbiamo $\dot{v} = v$ per $v \in {}^*M \backslash M$. Se quindi $x \in \dot{\mathcal{O}}$, allora $\{v \in {}^*M \mid v(x) < 0\}$ è contenuto in M, e deve essere finito poiché altrimenti per saturazione avrebbe un elemento anche fuori da M. □

Teorema 17 (Weissauer)**.** *Dato un $t \in {}^*k \setminus k$, se esiste un $w \in M$ tale che $\dot{w}$ non è banale su $k(t)$, allora Ω_t è M-aritmetico.*

Dimostrazione. L'anello $\dot{\mathcal{O}} \cap \Omega_t$ è un dominio di Dedekind. In particolare su di esso gli elementi per cui $\dot{w}(x) > 0$ formano un ideale massimale. Se ξ è un elemento non nullo di tale ideale, abbiamo che l'insieme $\{v \in {}^*M \mid v(\xi) < 0\}$ è finito e contenuto in M, e la seguente somma ha significato:

$$\sum_{v(\xi)<0} v(\xi).$$

D'altra parte, questa somma è contenuta in $\mathbb{R}$, poiché tutti i suoi addendi lo sono per via di $\xi \in \dot{\mathcal{O}}$. Tuttavia per formula del prodotto abbiamo che la seguente formula è sempre vera:

$$w(\xi) < -\sum_{v(\xi)<0} v(\xi).$$

Ma questo implica che anche $w(\xi)$ è in $\mathbb{R}$, e quindi $\dot{w}(\xi) = 0$. □

Teorema 18 (Weissauer)**.** *Se k ha una formula del prodotto, allora è Hilbertiano.*

Dimostrazione. Prendiamo un $x \in k$ ed un $v \in M$ tali che che $v(x) \neq 0$. Quindi l'insieme $p(y)$ delle formule che dicono che y ha valutazioni non banali esattamente dove le ha x, e che $v(y) < c$ per ogni $c \in \mathbb{R}$, è finitamente soddisfatto da qualche potenza x^n. Allora per saturazione esiste un elemento $t \in {}^*k \setminus k$ tale che $v(t)$ è maggiore di qualsiasi multiplo intero di $v(x)$, e in particolare $\dot{v}$ non è banale su t, mentre t ha un numero finito di $\dot{v} \in \dot{S}$ tali che $\dot{v}(x) \neq 0$. Quindi Ω_t è S-aritmetico e k è Hilbertiano per il Teorema 15. □

Riferimenti bibliografici

[Hil92] David Hilbert, *Uber die Irreduzibilitat ganzer rationaler Funktionen mit ganzzahligen Koeffizienten*, Journal für die reine und angewandte Mathematik (1892).

[Roq75] Peter Roquette, *Nonstandard aspects of Hilbert's irreducibility theorem*, Model Theory and Algebra (A memorial tribute to Abraham Robinson), Lecture Notes in Math, vol. 498, Springer, Berlin, 1975, pp. 209–266.

[Wei82] Rainer Weissauer, *Der Hilbertsche Irreduzibilitatssatz*, Journal für die reine und angewandte Mathematik **334** (1982).