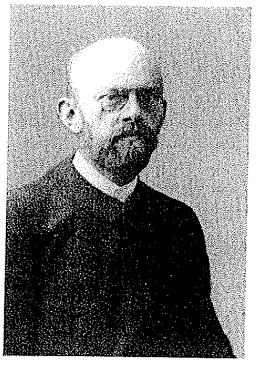

L'INFLUENZA DI DAVID HILBERT NELLA TEORIA DEI NUMERI

Roberto Dvornicich

IL PENSIERO DI DAVIDE HILBERT

A CENTO ANNI DAI "GRUNDLAGEN DER GEOMETRIE"
E DAL CONGRESSO INTERNAZIONALE DI PARIGI

Università degli Studi di Catania – Dipartimento di Matematica – Catania 23-25 settembre 1999

LE MATEMATICHE
Vol. LV (2000) – Supplemento n. 1, pp. 75–91

L'INFLUENZA DI DAVID HILBERT NELLA TEORIA DEI NUMERI

ROBERTO DVORNICICH

I contributi di Hilbert alla teoria dei numeri sono molteplici. Ci soffermeremo solo su due aspetti, che ci sembra abbiano influenzato in grande misura la teoria dei numeri nel ventesimo secolo: la teoria dei corpi di classe e il teorema di irriducibilità. Infine daremo brevi cenni sui problemi riguardanti la teoria dei numeri nella famosa lista dei 23 problemi di Hilbert.

1. La teoria dei corpi di classe.

La nozione di *corpo di classe* è generalmente attribuita ad Hilbert. In realtà questa nozione era già presente a Kronecker e il termine è stato coniato da Weber, poco prima che Hilbert scrivesse i suoi lavori sull'argomento.

La definizione più semplice di corpo di classe può essere data come segue:

Sia k un campo di numeri. Un'estensione algebrica K/k si dice un corpo di classe per k se tutti gli ideali primi principali di k si spezzano completamente in K.

Osserviamo che, usando il linguaggio moderno, con "ideali primi di k" intendiamo gli ideali primi dell'anello degli interi di k (Kronecker prima e Weber poi usavano la nozione di "divisori"). Weber stesso aveva subito generalizzato la precedente definizione in modo molto più utile per le applicazioni. Egli considerava "moduli interi" $\widetilde{\mathfrak{m}} = \mathfrak{m}\mathfrak{m}_\infty$ di k, dove $\mathfrak{m}$ è un prodotto formale finito di

primi di k con esponente positivo e $\mathfrak{m}_\infty$ è un prodotto di primi infiniti di k (corrispondenti alle valutazioni archimedee) reali e con esponente 1. Nel gruppo $J_\mathfrak{m}$ degli ideali frazionari relativamente primi con $\mathfrak{m}$ si può definire il sottogruppo unitario $J_\mathfrak{m}^1$ (unit ray ideal group) come segue:

$$J_\mathfrak{m}^1 = \{\frac{\mathfrak{a}}{\mathfrak{b}} | (\mathfrak{m}, \mathfrak{ab}) = 1, \frac{\mathfrak{a}}{\mathfrak{b}} \equiv 1 \bmod {}^\times \mathfrak{m}\}$$

dove il simbolo $\frac{\mathfrak{a}}{\mathfrak{b}} \equiv 1 \bmod {}^\times M$ significa che $\frac{\mathfrak{a}}{\mathfrak{b}} = \frac{(\alpha)}{(\beta)}$ è un ideale frazionario principale tale che $\frac{(\alpha)}{(\beta)} \equiv 1 \bmod \mathfrak{m}$ e α, β hanno lo stesso segno per tutte le valutazioni archimedee contenute in $\mathfrak{m}_\infty$. Si considerino poi gruppi quoziente $J_\mathfrak{m}/H_\mathfrak{m}$ dove $H_\mathfrak{m}$ è un sottogruppo di $J_\mathfrak{m}$ contenente $J_\mathfrak{m}^1$ e si considerino equivalenti due quozienti $J_{\mathfrak{m}_1}/H_{\mathfrak{m}_1}$ e $J_{\mathfrak{m}_2}/H_{\mathfrak{m}_2}$ se per il minimo comune multiplo dei moduli $\mathfrak{m} = [\mathfrak{m}_1, \mathfrak{m}_2]$ vale l'uguaglianza $H_{\mathfrak{m}_1} \cap J_\mathfrak{m} = H_{\mathfrak{m}_2} \cap J_\mathfrak{m}$, da cui $J_{\mathfrak{m}_1}/H_{\mathfrak{m}_1} \cong J_{\mathfrak{m}_2}/H_{\mathfrak{m}_2}$. Una classe di equivalenza di questi quozienti definisce un *gruppo di congruenza di classi* J/H nel senso di Weber. I singoli quozienti di una classe si dicono *interpretazioni* della classe e il più piccolo modulo $\mathfrak{f}$ delle interpretazioni (che è uguale al massimo comune divisore di tutti i moduli delle interpretazioni) si dice *conduttore* di J/H.

La definizione generale di Weber è allora la seguente:

Sia k un campo di numeri e sia J/H un gruppo di congruenza di classi di k. Un'estensione algebrica K/k si dice un corpo di classe per J/H se i primi che si spezzano completamente in K sono esattamente i primi della classe "principale" H.

Kronecker conosceva già degli esempi fondamentali di corpi di classe secondo questa definizione, ed aveva enunciato il suo famoso *teorema di completezza*:

Ogni estensione abeliana di $\mathbb{Q}$ è contenuta in un campo ciclotomico, e quindi è un corpo di classe.

Questo teorema fu dimostrato per la prima volta completamente da Weber e poi più semplicemente da Hilbert. Seguirono poi numerose altre dimostrazioni.

Prima di arrivare ai contributi di Hilbert, riassumiamo i risultati provati o congetturati da Weber negli anni 1897 e 1898. Innanzitutto, Weber enunciò il fondamentale *teorema di isomorfismo*:

Il gruppo di Galois $G(K/k)$ è isomorfo al gruppo delle classi J/H, e quindi è necessariamente abeliano.

Egli riuscì a dimostrare la prima disuguaglianza fondamentale

$$[J : H] = h \leq n = [K : k],$$

il *teorema di unicità*

$$H = H' \Leftrightarrow K = K',$$

il *teorema di ordinamento*

$$H \supseteq H' \Leftrightarrow K \subseteq K'$$

e un presupposto fondamentale del teorema di isomorfismo:

$$K/k \qquad \text{è normale.}$$

Inoltre egli congetturò in forma generale il *teorema di esistenza*:

Per ogni gruppo di congruenza di classi J/H di k esiste un corpo di classe K/k

e osservò che la dimostrazione di questo teorema avrebbe avuto come corollario una enorme generalizzazione del teorema di Dirichlet sui primi in progressione aritmetica.

I lavori di Hilbert sulla teoria dei corpi di classe concernono solamente il caso delle classi di ideali assolute (cioè quando H contiene tutti i primi principali), e inoltre le sue dimostrazioni riguardano solo il caso dei campi di numeri relativamente quadratici (cioè quando $n = 2$) con numero di classi $h = 2$. Tuttavia egli ebbe sempre presente il caso generale, e si dichiarò ottimista sul fatto che le sue dimostrazioni potessero essere generalizzate.

Egli concepì inoltre l'idea che la teoria dei corpi di classe potesse essere uno strumento non soltanto per dimostrare il teorema di completezza o generalizzazioni del teorema di Dirichlet, ma anche per sviluppare una *teoria delle estensioni relativamente abeliane* e per determinare delle *leggi di reciprocità di ordine superiore* (vedi Problema n. 9 della lista dei 23 problemi di Hilbert).

Uno dei risultati più importanti di Hilbert è proprio nella direzione delle leggi di reciprocità. Egli dimostrò la formula del prodotto

$$\prod_{\mathfrak{p}} \left(\frac{\mathfrak{a}, \mathfrak{b}}{\mathfrak{p}}\right)_n = 1,$$

dove $\mathfrak{p}$ varia tra tutti i primi (compresi quelli all'infinito) di un campo k contenente le radici n-esime dell'unità. (Il simbolo n-esimo di Hilbert $\left(\frac{\mathfrak{a}, \mathfrak{b}}{\mathfrak{p}}\right)_n$ ha per valore una radice n-esima dell'unità e la sua definizione precisa richiede la teoria di Kummer sulle estensioni cicliche. La cosa più importante comunque è che il simbolo n-esimo di Hilbert è legato al fatto che a sia o meno una norma locale da $k(\sqrt[n]{b})$ a k). Hilbert pose anche l'accento sull'analogia tra la formula

precedente e il teorema dei residui per le funzioni algebriche (se si fa eccezione per il fenomeno dell'inerzia, che compare nel caso aritmetico ma non nel caso dei campi di funzioni algebriche, i primi $\mathfrak{p}$ con simbolo $\neq 1$ corrispondono ai punti di ramificazione della superficie di Riemann).

Hilbert dimostrò anche (in casi speciali) il *teorema della norma*:

$(\frac{a,b}{\mathfrak{p}})_n = 1$ *per ogni* $\mathfrak{p} \Leftrightarrow a$ *è una norma relativa da* $k(\sqrt[n]{b})$ *a* k

e il *teorema del discriminante*:

K/k *ha discriminante relativo* $\mathfrak{d} = 1$.

Inoltre asserì il *teorema degli ideali principali*:

Tutti gli ideali di k diventano principali in K

e il seguente risultato sul numero delle classi

Il numero di classi di K non è divisibile per 2.

Se si fa eccezione per l'ultima proposizione, la cui generalizzazione è molto limitata, tutti gli altri risultati di Hilbert sono poi stati dimostrati veri nel caso generale.

Ecco un brevissimo riassunto di quanto è stato dimostrato successivamente.

La legge di reciprocità nel caso di esponenti primi ℓ:

$$(\frac{a}{b})_\ell = (\frac{b}{a})_\ell \quad \text{se } a \text{ e } b \text{ sono primari (e totalmente positivi per } \ell = 2)$$

è stata provata da Fürtwangler in vari articoli a cominciare dai primi anni del ventesimo secolo, anche nel caso della formula del prodotto del "norm residue symbol" di Hilbert. È da notare, fra l'altro, che la dimostrazione passa attraverso l'uso della *legge di decomposizione* in un'opportuna estensione del campo di base k.

Tagaki fece un passo decisivo nella teoria introducendo una variazione nella definizione di corpo di classe data da Weber. Egli fece corrispondere ad ogni estensione K/k e ad ogni modulo $\mathfrak{m}$ in k un gruppo di congruenza di classi *interpretato* modulo $\mathfrak{m}$, e cioè il più piccolo gruppo quoziente $J_\mathfrak{m}/H_\mathfrak{m}$ la cui classe principale $H_\mathfrak{m}$ contiene tutte le norme degli ideali A di K prime con $\mathfrak{m}$. In altri termini, $H_\mathfrak{m}$ consiste di tutti gli ideali $\mathfrak{a}$ di k primi con $\mathfrak{m}$ e tali che

$$\mathfrak{a} \sim N(A) \bmod \mathfrak{m}, \quad \text{i.e. } \frac{\mathfrak{a}}{N(A)} \cong a \equiv 1 \bmod \mathfrak{m} (a \in k).$$

Per $\mathfrak{m}$ sufficientemente grande (in realtà per $\mathfrak{m}$ multiplo di $\mathfrak{f}$, il conduttore di K/k) i gruppi $J_\mathfrak{m}/H_\mathfrak{m}$ coincidono e quindi costituiscono un gruppo di

congruenza di classi J/H nel senso di Weber. Avendo a disposizione la prima disuguaglianza fondamentale dimostrata da Weber, Tagaki diede la seguente definizione di corpo di classe

K/k si dice corpo di classe associato al gruppo di congruenza di classi J/H se e solo se vale l'uguaglianza $h = n$.

Sulla base di questa definizione, Tagaki provò che

La relazione di corpo di classe stabilisce una corrispondenza biunivoca tra tutte le estensioni abeliane K/k e i gruppi di congruenza di classi J/H in k.

Il teorema del discriminante potè essere generalizzato (con dimostrazione di Hasse) ad una *formula conduttore-discriminante.*

Artin (1927) diede un *isomorfismo esplicito* fra il gruppo di classi J/H e il gruppo di Galois $G(K/k)$. Questo isomorfismo è indotto dalla mappa che associa ad ogni primo $\mathfrak{p} \nmid \mathfrak{d}$ l'*automorfismo di Frobenius* $F_\mathfrak{p}$ di K/k rispetto a $\mathfrak{p}$, cioè l'automorfismo definito da

$$F_\mathfrak{p}(x) \equiv x^{N(\mathfrak{p})} \bmod \mathfrak{p} \text{ per tutti gli interi } x \in K,$$

dove $N(\mathfrak{p})$ è la norma assoluta di $\mathfrak{p}$. Nella notazione moderna,

$$F_\mathfrak{p} = \left(\frac{K/k}{\mathfrak{p}}\right),$$

e si estende la definizione per moltiplicatività agli ideali $\mathfrak{a}$ primi con $\mathfrak{d}$. L'isomorfismo esplicito sopra citato, detto anche *legge di reciprocità di Artin*, diventa allora

$$\left(\frac{K/k}{\mathfrak{a}}\right) = 1 \Leftrightarrow \mathfrak{a} \in H_\mathfrak{f}.$$

È da notare, comunque, che Artin riuscì a dimostrare la sua legge di reciprocità solo usando i risultati di Tchebotarev sulla densità dei primi il cui automorfismo di Frobenius appartiene ad una certa classe di coniugio.

Usando le proprietà dell'automorfismo di Frobenius, Artin ridedusse la legge di reciprocità nella forma generale (compresa la formula del prodotto), rendendola più comprensibile e la chiamò *legge generale di reciprocità.*

Infine, riferendosi ai lavori di Fütwangler, Artin dimostrò completamente anche il *teorema degli ideali principali*, enunciato precedentemente da Hilbert.

Per concludere citiamo brevemente alcuni risultati ottenuti dopo la dimostrazione dei teoremi di Artin.

Hasse, introducendo una variazione del simbolo di Hilbert, diede una classificazione degli elementi di k che sono la norma di elementi di K, in termini di un principio locale-globale, e aprì la strada alla *teoria dei corpi di classe locale*, essenzialmente sviluppata da Schmidt e Chevalley.

Chevalley inventò gli *ideali* di un campo k, che sono particolari elementi del prodotto cartesiano di tutti i completamenti di k, sistematizzando la definizione di gruppo di congruenza di classi con un trattamento simile a quello dei divisori e del gruppo di Picard in geometria algebrica.

Tate introdusse gli strumenti coomologici che hanno in gran parte semplificato la dimostrazione di molti risultati dell'intera teoria, e consentendo nuovi sviluppi, troppo tecnici per essere ricordati in questa sede, in particolare da parte di Shafarevich e di Weil.

BIBLIOGRAFIA

E. Artin - J. Tate, *Class Field Theory,* Benjamin, 1967.

J.W.S. Cassels - A. Fröhlich, *Algebraic Numbers Fields,* Academic Press, 1967.

D. Hilbert, *The Theory of Algebraic Number Fields,* (translated by I.T. Adamson), Springer, 1988.

W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers,* Springer- Verlag and PWN-Polish Scientific Publishers, Warszawa, 1990.

J. Neukirch, *Class Field Theory,* Springer, 1986.

A.N. Parshin - I.R. Shafarevic (Eds), *Number Theory II,* Enc. of Math. Sciences, Vol. 62, Springer, 1992.

2. Il Teorema di Irriducibilità.

Il Teorema di Irriducibilità di Hilbert, nella sua forma basilare, risale al 1892. Da allora ha subito evoluzioni di varia natura. Esso è strettamente connesso con le proprietà aritmetiche e *diofantee* di un campo. In particolare, esso ha applicazioni alla costruzione di estensioni di campi con assegnato gruppo di Galois.

Il *Teorema di Irriducibilità* di Hilbert (d'ora in avanti TIH) grosso-modo afferma che la specializzazione in $\mathbb{Q}$ spesso preserva l'irriducibilità di polinomi su $\mathbb{Q}$.

Più precisamente, si ha il seguente enunciato:

Siano $f_i(T_1, \ldots, T_r, X_1, \ldots, X_s) \in \mathbb{Q}[T_1, \ldots, T_r, X_1, \ldots, X_s]$, $1 \leq i \leq h$ *irriducibili e sia* $0 \neq g \in \mathbb{Q}[T_1, \ldots, T_r]$. *Allora esistono infinite r-ple* $(t_1, \ldots, t_r) \in \mathbb{Q}^r$ *tali che* $g(t_1, \ldots, t_r) \neq 0$ *e* $f_i(t_1, \ldots, t_r, X_1, \ldots, X_s) \in \mathbb{Q}[X_1, \ldots, X_s]$ *è irriducibile su* $\mathbb{Q}$ *per* $i = 1, \ldots, h$.

(Come esempio illustrativo, si consideri il seguente corollario: *Se* $F \in \mathbb{Q}(T_1, \ldots, T_r)$ *assume valori che siano quadrati perfetti per tutte le scelte di* $T_1, \ldots, T_r$ *in* $\mathbb{Q}$, *allora* F *è il quadrato di un polinomio su* $\mathbb{Q}$. Per dimostrarlo basta prendere $f(T_1, \ldots, T_r, X) = X^2 - F(T_1, \ldots, T_r)$ nell'enunciato del TIH).

In effetti Hilbert provò che $(t_1, \ldots, t_r)$ si può prendere in $\mathbb{Z}^r$ e che $\mathbb{Q}$ può essere rimpiazzato da qualunque campo di numeri [1]. Si è col tempo compreso che, benché alcune proprietà aritmetiche dei campi di numeri svolgano un ruolo fondamentale nelle (svariate) dimostrazioni del teorema, questo resta valido anche abbandonando altre specifiche proprietà. Ciò ha condotto a considerare a parte la classe dei campi k per i quali l'enunciato vale con k al posto di $\mathbb{Q}$. Si dice in tal caso che k è *hilbertiano*.

Prima di illustrare alcuni approcci al teorema, ricordiamo una delle principali motivazioni storiche e applicazioni del concetto: *la costruzione di campi di numeri* L *con gruppo di Galois* $Gal(L/\mathbb{Q})$ *isomorfo a un gruppo finito assegnato* G. Il problema se questo sia possibile per qualunque G è spesso detto *problema inverso della teoria di Galois* e si congettura abbia risposta affermativa.

Vediamo come ciò si lega con il TIH. Supponiamo di aver costruito un' estensione finita e normale L di $K := \mathbb{Q}(T_1, \ldots, T_r)$ con gruppo di Galois isomorfo a G. Sia α un elemento primitivo per L/K, intero su $\mathbb{Q}[T_1, \ldots, T_r]$ e sia $f \in \mathbb{Q}[T_1, \ldots, T_r, X]$ il suo polinomio minimo su K. Poiché L è normale su K, tutte le radici di f sono polinomi in α a coefficienti in K. Sia ora $P = (t_1, \ldots, t_r) \in \mathbb{Q}^r$ tale che tutti questi coefficienti siano definiti in P. Allora, specializzando $(T_1, \ldots, T_r)$ a P si vede che tutte le radici del polinomio $f(P, X) = f(t_1, \ldots, t_r, X)$ sono polinomi in una qualsiasi delle radici. Per semplicità supponiamo anche che tali radici siano distinte. (Questo avverrà a patto che P stia fuori dall'ipersuperficie definita dal discriminante di f rispetto a X). Scegliamo una tale radice e indichiamola con $\alpha(P)$. Da ciò che si è detto segue che l'estensione $\mathbb{Q}(\alpha(P))$ è normale su $\mathbb{Q}$ ed è facile vedere che il suo gruppo di Galois è isomorfo a un sottogruppo di G. (Geometricamente, si ha un rivestimento di Galois di A^r. Il gruppo di Galois G opera sulla fibra di ciascun

[1] La dimostrazione di Hilbert conteneva in effetti un errore (correggibile) in tal senso, come fu rilevato da A. Schinzel.

punto $P \in A^r(\mathbb{Q})$. Lo stabilizzatore di un punto Q della fibra, detto *gruppo di decomposizione* di Q, è il sottogruppo in questione [2]).

Supponiamo ora che $f(P, X)$ sia irriducibile su $\mathbb{Q}$. Allora è chiaro che $\alpha(P)$ genera su $\mathbb{Q}$ un'estensione normale di grado uguale al grado di α su K. Necessariamente il suo gruppo di Galois è isomorfo a G. Dunque, nella situazione ipotizzata, il TIH garantisce l'esistenza di famiglie di estensioni di $\mathbb{Q}$ con gruppo di Galois prefissato. (Anzi, se L/K è regolare su $\mathbb{Q}$, si ottengono estensioni del tipo voluto linearmente disgiunte su $\mathbb{Q}$ da campi prefissati).

Un esempio semplice è fornito dalle funzioni simmetriche. Siano $U_1, \ldots, U_r$ indeterminate e denotiamo con $T_1, \ldots, T_r$ le loro funzioni simmetriche elementari. Poniamo $L = \mathbb{Q}(U_1, \ldots, U_r)$ e $K = \mathbb{Q}(T_1, \ldots, T_r)$. Allora L è un'estensione di K con gruppo di Galois isomorfo a S_r. La costruzione precedente fornisce famiglie di estensioni di $\mathbb{Q}$ con il medesimo gruppo di Galois. Basta prendere un elemento primitivo α di L/K intero su K (ad es. $\alpha = \sum_{i=1}^{r} iU_i$) e considerare il suo polinomio minimo f su K (si trova $f = \prod_{\sigma \in S_r}(X - \sum_{i=1}^{m} \sigma(i)U_i)$). Il TIH dimostra che esistono infinite specializzazioni razionali dei T_i per cui esso rimane irriducibile, e la discussione di sopra si applica. (In particolare, immergendo un gruppo finito assegnato G in un gruppo simmetrico, si ottengono estensioni K/k di campi di numeri con gruppo di Galois isomorfo a G).

Per un certo periodo si credette che questo tipo di strategia avrebbe portato a una soluzione completa del sopracitato *problema inverso*. Vediamo come si pensava ad esempio di poter procedere. Sia G un gruppo finito assegnato. Immergiamo G in un opportuno gruppo simmetrico S_r e consideriamo l'estensione L/K or ora introdotta. Sia F il corpo fisso di G in L, cosicché L/F è un'estensione normale con gruppo G. Osserviamo che L è puramente trascendente su $\mathbb{Q}$ e F ne è un sottocampo (e dunque una varietà $\mathcal{W}$ con F come campo di funzioni è $\mathbb{Q}$-*unirazionale*). Ora, nel caso di dimensione 1, un ben noto teorema dovuto a Lüroth afferma che unirazionalità e razionalità sono proprietà equivalenti. Se ciò fosse vero per r qualunque, almeno per le varietà in oggetto (ossia se $\mathcal{W}$ dovesse necessariamente essere $\mathbb{Q}$-*razionale*), si potrebbe porre $F = \mathbb{Q}(V_1, \ldots, V_r)$ e le considerazioni precedenti (con F al posto di K) sarebbero applicabili. Questo era in sostanza il programma intravisto da Hilbert, E. Noether e altri. Senonché l'analogo in dimensione superiore del teorema di Lüroth si rivelò falso e nel 1969 R.G. Swan esibì controesempi alla strategia ora delineata, anche nel semplice caso in cui G fosse generato da un r-ciclo.

[2] Per "punto" della fibra, intendiamo $\mathbb{Q}$-punto, ossia punto irriducibile su $\mathbb{Q}$. Con l'ipotesi fatta sulle radici, ciò in pratica equivale a considerare un sistema completo di coniugati su $\mathbb{Q}$ di un punto nel senso "geometrico".

(Nemmeno nel caso in cui $G = A_r$ è noto se l'estensione quadratica di K in tal modo ottenuta sia puramente trascendente) [3].

Ciò nondimeno queste idee hanno portato (in tempi relativamente recenti) alla costruzione di molte specie di gruppi finiti come gruppi di Galois di estensioni di $\mathbb{Q}$ per mezzo di una tecnica (introdotta da M. Fried e altri) solo in parte diversa da quella esposta. Si inizia costruendo un'estensione di $\mathbb{C}(T)$ con gruppo di Galois isomorfo a G. Ciò è possibile interpretando G come gruppo di monodromia di un rivestimento ramificato di $\mathbb{P}^1$ e applicando il Teorema di Esistenza di Riemann. La geometria algebrica (o un'argomentazione di continuità) permette di ottenere tale estensione su $\overline{\mathbb{Q}}$ anziché su $\mathbb{C}$. Dunque si può supporre di aver costruito un'estensione di $k(T)$ con gruppo G, dove k è un campo di numeri. A questo punto la teoria della *discesa* di Weil permette talvolta di realizzare tale estensione prendendo $k = \mathbb{Q}$. Quando questo è possibile il TIH permette di scendere ulteriormente da $\mathbb{Q}(T)$ a $\mathbb{Q}$. Hilbert stesso produsse famiglie con gruppo S_r e A_r, per mezzo di analoghe costruzioni ad hoc.

Per tornare al TIH stesso, è abbastanza facile vedere che k è hilbertiano se e solo se la proprietà fondamentale vale per polinomi del tipo $f(T, X) \in k[T, X]$.

Vediamo ora un'ulteriore utile equivalenza, che illustra direttamente il legame del TIH con le equazioni diofantee.

Sia $f(T, X) \in k[T, X]$ irriducibile e sia Ω un campo di decomposizione di $f = 0$ su $k(T)$. Scriviamo una fattorizzazione $f = c(T)(X - \alpha_1) \cdots (X - \alpha_d)$ in Ω. Poiché gli α_i sono interi su $k[T, c(T)^{-1}]$, possiamo estendere l'omomorfismo di specializzazione $T \mapsto t \in k$ a $k[T, \alpha_1, \ldots, \alpha_d]$ per ogni $t \in k \setminus S$, dove S è un opportuno insieme finito. (Ciò corrisponde a scegliere un punto P sulla curva $f(T, X) = 0$, con $T(P) = t$). Per tali t avremo

$$f(t, X) = c(t) \prod_{i=1}^{d} (X - \alpha_i(t)).$$

Ora, se $f(t, X)$ è riducibile su k, un opportuno prodotto parziale (non banale) del lato destro avrà coefficienti in k. Sia J il sottoinsieme proprio di $\{1, \ldots, d\}$ corrispondente a tale prodotto e consideriamo $\Pi_{i \in J}(X - \alpha_i) \in \Omega[X]$. Poiché supponiamo f irriducibile tale prodotto avrà almeno un coefficiente, che indichiamo con ω_J, fuori da $k(T)$. Si ha però $\omega_J(t) \in k$. Ora, sia $g_J \in k(T)[X]$ il polinomio minimo di ω_J su $k(T)$. Naturalmente g_J è irriducibile su $k(T)$ e di grado > 1 in X. D'altra parte troviamo che $g_J(t, X)$ ha la radice $\omega_J(t)$ che sta in k.

[3] Cfr. anche [Oj] per controesempi all'analogo multi-dimensionale del Teorema di Lüroth.

Vediamo dunque che, se siamo in grado di garantire che nessun $g_J(t, X)$ abbia radici in k, allora $f(t, X)$ sarà irriducibile. In altre parole abbiamo dimostrato la seguente

Proposizione 1. *Sia k un campo con la seguente proprietà: "per ogni scelta dei polinomi $g_i(T, X) \in k[T, X]$, $i = 1, \ldots, h$, irriducibili su k e di grado > 1 in X, esistono infiniti $t \in k$ tali che nessun $g_i(t, X)$ abbia radici in k". Allora k è hilbertiano.*

Quando $g \in \mathbb{Q}[T, X]$, ricercare i $t \in \mathbb{Q}$ tali che $g(t, X)$ abbia una radice in $\mathbb{Q}$ è come risolvere *l'equazione diofantea* $g(T, X) = 0$, o ancora equivale a trovare i punti razionali su una data curva piana. Vediamo dunque come il TIH sia direttamente legato a classici problemi aritmetici. Mostreremo più avanti come in effetti la *geometria diofantea* implicitamente procuri dimostrazioni del TIH particolarmente efficaci.

Possiamo riformulare ulteriormente quanto ottenuto. Sia g come sopra e consideriamo i valori $t \in k$ "cattivi", ossia tali che $g(t, X) = 0$ ha soluzioni in k. Come sopra, possiamo considerare una curva piana $\mathcal{C}$ irriducibile su k, definita da $g(T, X) = 0$. I valori $t \in k$ "cattivi" danno luogo a $x \in k$ tale che $g(t, x) = 0$, ossia abbiamo ottenuto un punto razionale $P = (t, x) \in \mathcal{C}(k)$ e t è l'immagine di P tramite la funzione razionale $T \in k(\mathcal{C})$. Il fatto che k sia hilbertiano allora corrisponde al fatto che k non possa essere ricoperto da un numero finito di queste immagini. In altre parole, per un tale campo, gli insiemi immagine sono "piccoli". Possiamo in effetti partire da questi insiemi per definire un campo hilbertiano come segue (cfr. [5], [6]).

Definizione 1. Sia $\mathcal{V}/k$ una varietà irriducibile definita su k. Diciamo che un sottoinsieme $M \subset \mathcal{V}(k)$ di punti razionali su $\mathcal{V}$ è *magro* se è unione finita di insiemi che siano

(i) *contenuti in una sottovarietà propria di $\mathcal{V}/k$*, oppure
(ii) *contenuti in un'immagine $\phi(\mathcal{W}(k))$, dove $\mathcal{W}$ è una varietà irriducibile della stessa dimensione di $\mathcal{V}$ e $\phi : \mathcal{W} \to \mathcal{V}$ è una mappa razionale dominante di grado ≥ 2.*

Definizione 2. Diciamo che la varietà $\mathcal{V}/k$ ha la proprietà di Hilbert se $\mathcal{V}(k)$ non è magro.

Questa definizione è dovuta a J.-L. Colliot-Thélène e J.-J. Sansuc. È una proprietà k-birazionale di $\mathcal{V}$.

Quello che si è visto in precedenza equivale all'affermazione che *k è hilbertiano se e solo se $\mathbb{P}^1/k$ ha la proprietà di Hilbert.*

Non è difficile vedere che se $\mathcal{V}/k$ ha la proprietà di Hilbert, allora $\mathbb{P}^1/k$ ha la proprietà di Hilbert. (Se $\mathcal{C}_i$, $i = 1, \ldots, h$ sono curve definite su k con mappe razionali dominanti ϕ_i su $\mathbb{P}^1$, ciascuna di grado ≥ 2, allora si applichi l'ipotesi alle varietà $\mathcal{W}_i := \mathcal{C}_i \times_{\mathbb{P}^1} \mathcal{V}$, dove $f : \mathcal{V} \to \mathbb{P}^1$ è un'opportuna mappa razionale).

Pertanto abbiamo ottenuto la proposizione seguente, che può anche essere rimaneggiata come definizione alternativa di campo hilbertiano.

Proposizione 2. *Un campo k è hilbertiano se e solo se esiste una varietà $\mathcal{V}/k$ con la proprietà di Hilbert. In tal caso si può prendere $\mathcal{V} = \mathbb{P}^1$.*

Osservazione. Nel verificare se $\mathcal{V}(k)$ sia magro, possiamo limitare le considerazioni relative al punto (ii) nella Def. 1 alle varietà $\mathcal{W}$ geometricamente irriducibili. Infatti, se $\mathcal{W}$ non lo è, allora il suo campo di funzioni contiene un' estensione algebrica propria k' di k. Se $P \in \mathcal{W}$ è un punto normale, allora il suo anello locale contiene k', che è intero su k. Pertanto $P \notin \mathcal{W}(k)$ e pertanto $\mathcal{W}(k)$ è in effetti contenuto nella sottovarietà propria di $\mathcal{W}$ formata dai punti non-normali.

Esempi. È assai facile rendersi conto che campi come $\mathbb{C}, \mathbb{R}, \overline{\mathbb{Q}}$ o $\mathbb{Q}_p$ non sono hilbertiani [4]. Come abbiamo detto, Hilbert stesso dimostrò che i campi di numeri sono hilbertiani. In generale, non è troppo difficile dimostrare che se k è hilbertiano, allora lo è anche una sua qualunque estensione finita. In effetti si ha che *se k'/k è un'estensione finita e $\Omega_1 \subset \mathbb{P}^n(k')$ è magro relativamente a k', allora $\Omega := \Omega_1 \cap \mathbb{P}^n(k)$ è magro su k.* (Cfr. [5] o [6] per una dimostrazione che usa il *funtore restrizione degli scalari* $R_{k'/k}$; questo trasforma una k'-varietà in una k-varietà). Il risultato di Hilbert si riconduce in tal modo al caso $k = \mathbb{Q}$.

Dal fatto che $\mathbb{Q}$ sia hilbertiano si deduce con una semplice *diagonalizzazione* che esistono i cosiddetti *Insiemi di Hilbert Universali*, ossia sequenze $\{h_n : n \in \mathbb{N}\}$ di numeri razionali per cui, dato comunque un polinomio irriducibile $f(T, X) \in \mathbb{Q}[T, X]$, si ha che $f(h_n, X)$ è irriducibile per tutti gli n tranne un numero finito. V.G. Sprindzuk fu il primo a esibire esempi concreti di tali sequenze, espresse da valori di certe funzioni elementari.

Sia il Teorema di Bertini che altri metodi mostrano che i campi di funzioni di $\mathbb{Q}$-varietà di dimensione positiva sono hilbertiani. Se ne deduce che ogni campo finitamente generato su $\mathbb{Q}$ è hilbertiano. (Ciò vale anche per $k(t)$ al posto di $\mathbb{Q}$, per ogni campo k). Un bel risultato di R. Weissauer afferma che

[4] Si noti come in questi casi la denominazione "magro" possa apparire paradossale. Ad esempio $\mathbb{P}^1(\mathbb{Q})$ non è magro (su $\mathbb{Q}$) mentre $\mathbb{P}^1(\overline{\mathbb{Q}})$ lo è (su $\overline{\mathbb{Q}}$).

ogni campo con un insieme di valutazioni che soddisfi una formula di prodotto è hilbertiano (e si ritrovano i risultati citati come casi particolari). Weissauer dimostrò anche che certe estensioni algebriche di $\mathbb{Q}$ di grado infinito sono campi hilbertiani: ad esempio un suo teorema afferma che *se k è hilbertiano, M è una qualsiasi estensione di Galois di k e N è un'estensione finita propria di M, allora N è hilbertiano.* Più recentemente D. Haran ha dimostrato un teorema di notevole generalità sui casi in cui la proprietà di essere hilbertiano si conserva passando a un'estensione algebrica (di grado anche infinito).

Non ci soffermeremo però su questi risultati generali, ma invece approfondiremo il caso fondamentale $k = \mathbb{Q}$, descrivendo in breve alcuni approcci diversi al fatto che $\mathbb{Q}$ sia hilbertiano.

Il primo di questi risale sostanzialmente a Hilbert e Dörge. Esso produce in effetti un risultato più preciso. Sia $\Omega \in \mathbb{A}^1(\mathbb{Q}) = \mathbb{Q}$ un insieme magro. Sarà sufficiente trovare numeri razionali fuori da Ω. Sia $E(B)$ il numero di interi positivi $\leq B$ che stanno in Ω. Vale allora il seguente risultato [5].

Teorema 1. *Si ha $E(B) \ll B^{1-\epsilon}$, dove $\epsilon > 0$ dipende solo da Ω.*

(In effetti ϵ può essere sempre preso = 1/2).

Un altro approccio, che fornisce risultati molto più forti, fu proposto da Siegel e fa uso di un suo importante e profondo risultato sui punti interi su curve algebriche affini. Sia $\mathcal{C}/k \subset \mathbb{A}^n$ una curva algebrica affine assolutamente irriducibile, definita su un campo di numeri k, con anello di interi O_k. Diremo *punto intero* (su k) un punto in O_k^n. Sia $m = m(\mathcal{C})$ il numero di *punti all'infinito*, ossia necessari per completare una normalizzazione di $\mathcal{C}$. Si ha il

Teorema di Siegel. *Se $\mathcal{C}$ ha un numero infinito di punti interi su k, allora $\mathcal{C}$ ha genere 0 e inoltre $m \leq 2$.*

Sia ora Ω un insieme magro in $\mathbb{A}^1(k)$ e consideriamone l'intersezione con O_k. Analogamente a sopra, vogliamo contare il numero $E(B) = E_k(B)$ di punti ν in questo insieme tali che $\|\nu\| \leq B$. La norma $\|\nu\|$ ora considerata è semplicemente il massimo dei moduli dei coniugati di ν su $\mathbb{Q}$ [6].

Si vede facilmente che il numero di interi $\nu \in O_k$ con $\|\nu\| \leq B$ è, a meno di costanti, dell'ordine di grandezza di B^d, dove $d = [k : \mathbb{Q}]$. Abbiamo allora il seguente rafforzamento del Teorema 1.

Teorema 2. *Si ha $E(B) \ll B^{\frac{d}{2}}$.*

---

[5] Usiamo le classiche notazioni $f \ll g$ o $f = O(g)$ per indicare che $|f| \leq c|g|$, dove c, detto "costante implicita", è un numero che dipende solo da quantità basilari, normalmente chiarite dal contesto.

[6] Per $\nu \in O_k$, si ha $\log \|\nu\| \gg\ll h(\nu)$, dove h è l'altezza di Weil logaritmica.

Un ulteriore approccio consiste nel contare i punti razionali in un sottoinsieme magro di $\mathbb{P}^1$, misurandoli per mezzo dell'*altezza di Weil*. Si consulti [3] o [6] per definizioni e proprietà. Qui ricordiamo solo che l'altezza $H(\alpha)$ di un numero algebrico α di grado d su $\mathbb{Q}$ può essere definita come la radice d-ima del prodotto $|a_0| \prod_{i=1}^{d} \max(1, |\alpha_i|)$, dove a_0 è il coefficiente dominante del polinomio minimo di α su $\mathbb{Z}$ e dove gli α_i sono i coniugati di α. Il semplice, ma importante, *teorema di Northcott* afferma che gli α di grado e altezza limitati sono in numero finito. Un risultato di Schanuel afferma che il numero $N(B) = N_k(B)$ di elementi in un campo di numeri k con altezza $\leq B$ è asintotico a cB^{2d}, dove $d = [k : \mathbb{Q}]$ $c = c_k$ è una certa costante positiva.

Sia ora come sopra $\mathcal{C}/k$ una curva e $T : \mathcal{C} \to \mathbb{P}^1$ una mappa razionale dominante di grado ≥ 2. Sia $N_{\mathcal{C}}(B)$ il numero di punti $P \in \mathcal{C}(k)$ con $H(T(P)) \leq B$. Si ha la stima seguente:

Teorema 3. $N_{\mathcal{C}}(B) \ll B^d$.

Ancora un'altra possibilità parte dalla teoria delle equazioni su campi finiti, secondo un'idea che risale a M. Eichler e che è stata successivamente impiegata da altri autori.

Inoltre esistono altri approcci dimostrativi. Concludiamo ricordando, oltre ai lavori già citati, dimostrazioni dovute a Inaba, Fried, Roquette, Dèbes.

BIBLIOGRAFIA

[1] M. Fried - M. Jarden, *Field Arithmetic,* Springer-Verlag, 1986.

[2] D. Hilbert, *Über die Irreduzibilität ganzer rationaler Funktionen mit ganzähligen Koeffizienten,* J. reine angew. Math., 110 (1892), pp. 104–129.

[3] S. Lang, *Fundamentals of Diophantine Geometry,* Springer-Verlag, 1983.

[4] A. Schinzel, *Selected topics on polynomials,* The Univ. of Michigan Press, Ann Arbor, 1982.

[5] J.-P. Serre, *Topics in Galois Theory,* Jones and Bartlett publ., Boston, 1992.

[6] J.-P. Serre, *Lectures on the Mordell-Weil Theorem,* 2-nd Ed., Vieweg, 1990.

[7] H. Volklein, *Groups as Galois groups,* Cambridge Univ. Press, 1996.

3. Aggiornamenti sui problemi di teoria dei numeri proposti al congresso di Parigi.

Grosso modo, i problemi che riguardano la teoria dei numeri sono quelli che vanno dal numero 7 al numero 10.

Il problema n. 7, sull'irrazionalità e trascendenza di alcuni numeri, riguarda in generale il fatto che ci si aspetta che funzioni trascendenti assumano in generale valori trascendenti sui punti algebrici. In particolare, Hilbert si chiede se sia vero che, dati un numero α algebrico e diverso da 0,1 e un numero β algebrico e irrazionale, il numero α^β è trascendente (o almeno irrazionale). Il problema, giudicato come uno dei più difficili da Hilbert, è stato risolto, con risposta affermativa, da Gel'fond e Schneider indipendentemente nel 1934. La tecnica si applica più generalmente a valori di insiemi di funzioni che soddisfino equazioni differenziali o equazioni funzionali con coefficienti in un campo di numeri. In questo caso, le funzioni e^z, $e^{\beta z}$ hanno addirittura il vantaggio di possedere entrambe le proprietà. Risultati analoghi sono stati ottenuti per valori delle funzioni di Weierstrass $\wp(z)$ legate a curve ellittiche con parametri g_2, g_3 algebrici e all'invariante $j(\tau)$ delle curve ellittiche. I risultati di indipendenza algebrica, pure sottointesi da Hilbert, sono invece noti solo in pochi casi estremamente particolari. Il problema si può oggi forse sostituire con la seguente *congettura di Schanuel*:

Se $\alpha_1, \ldots, \alpha_n$ sono linearmente indipendenti sui razionali, allora il grado di trascendenza su $\mathbb{Q}$ del campo $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ è maggiore o uguale a n.

In particolare, la congettura implicherebbe che e e π sono algebricamente indipendenti (ponendo $\alpha_1 = 1$, $\alpha_2 = 2\pi i$).

L'ottavo problema riguarda l'ipotesi di Riemann e i classici problemi additivi della teoria dei numeri come il problema dei primi gemelli (e sue generalizzazioni) e la congettura di Golbach.

In questo campo i progressi sostanziali sono stati veramente pochi. Le tecniche per dimostrare l'ipotesi di Riemann sono state esplorate da molti autori senza successo. Nel frattempo l'ipotesi si è successivamente allargata a funzioni ζ di carattere più generale (per esempio funzioni L di Dedekind, di Artin, legate a curve ellittiche o altre varietà), ma il solo caso risolto positivamente riguarda le funzioni zeta legate alle curve sui campi finiti (congetture di Weil e dimostrazione finale di Deligne).

Sui primi gemelli, così come su altre configurazioni di primi, si hanno solo ipotesi euristiche, peraltro in ottimo accordo con i dati "sperimentali", ossia con le tabelle di primi fornite dai computers. Sulla congettura di Goldbach c'è un lavoro fondamentale di Chen, che dice che ogni numero pari è somma di due numeri p, q dove p è primo e q ha al più due fattori primi, e inoltre, con metodi

di crivello, si sa che la percentuale di numeri pari rappresentabili come somma di due primi è positiva (l'attuale "record" è di circa il 60 per cento dei numeri pari).

Sul nono problema, che riguarda le leggi di reciprocità generali, abbiamo parlato diffusamente nella prima parte di questa esposizione.

Il decimo problema riguarda la possibilità di trovare dei metodi effettivi per la risolubilità di equazioni diofantee. Il problema è stato risolto negativamente da Matijasevic nel 1970 (dopo lavori di Robinson e Church) con metodi che oggi riguardano più la logica che la teoria dei numeri.

Il dodicesimo problema, di carattere più generale, è definito da Hilbert a cavallo tra la teoria dei numeri, l'algebra e la teoria delle funzioni. Il problema riguarda la possibilità di generalizzare il teorema di Kronecker (e Weber) sui campi abeliani, domandandosi se non si possa trovare un teorema analogo quando si sostituisca al campo di base $\mathbb{Q}$ una sua estensione quadratica immaginaria o un campo di numeri qualsiasi o anche un campo di funzioni.

Con la teoria della moltiplicazione complessa il caso in cui K sia un campo quadratico immaginario si risolve in modo analogo al caso razionale, e le estensioni abeliane di K si trovano per mezzo dell'azione del gruppo di Galois assoluto $G(\overline{K}/K)$ sui punti di ordine finito di una certa curva con moltiplicazione complessa. In maniera meno conclusiva, si sono fatti dei progressi anche nel caso più generale di campi CM, ossia estensioni quadratiche totalmente immaginarie di campi totalmente reali e nel caso di campi quadratici reali (costruzione delle varietà di Shimura). Nel caso in cui K è un campo di funzioni *su un campo finito*, ossia un'estensione finita e separabile di $\mathbb{F}_q(T)$, c'è una descrizione completa delle estensioni abeliane di K per mezzo dei *moduli ellittici* di Drinfel'd. Il problema generale, tuttavia, è ancora aperto e fa parte dell'ambizioso programma di ricerca denominato *programma di Langland.*

Roberto Dvornicich,
Dipartimento di Matematica "Leonida Tonelli"
via Filippo Buonarroti, 2
56127 Pisa (Italy)
e-mail: dvornicich@dm.unipi.it