

# LA TEORIA DI GALOIS DOPO GALOIS

Tamás Szamuely

L'editor della *Lettera Matematica Pristem* mi ha gentilmente chiesto di scrivere una rassegna informale di alcuni aspetti moderni della teoria di Galois, comprendenti la teoria di Galois infinita e l'approccio di Grothendieck. Ecco il mio tentativo di soddisfare la richiesta. Naturalmente, giacché tratterò degli argomenti avanzati, devo supporre che il lettore sia a conoscenza di alcuni concetti di matematica superiore, compreso la teoria di Galois di base, così come è presentata nei consueti testi di algebra. Le ultime parti richiederanno anche qualche conoscenza di aspetti fondamentali di topologia insiemistica e di analisi complessa.

Ma partiamo dall'inizio.

## 1. CHE COS'È UN'ESTENSIONE DI GALOIS?

Nella seconda metà del XIX secolo, alcuni eminenti matematici, come Liouville, Jordan, Dedekind e Weber, dedicarono notevoli sforzi per capire e sviluppare il lavoro rivoluzionario di Galois. Durante questo lavoro di chiarificazione, l'importanza della teoria di Galois si spostò gradualmente dalle equazioni alle estensioni dei campi, fino ad arrivare alla forma attuale. Nel corso di questo processo, il concetto di estensione di Galois di un campo venne ridefinito più volte. Elenchiamo quattro diverse formulazioni, in ordine crescente di astrazione.

La definizione più vicina all'approccio originale di Galois è la seguente:

(1) *Un'estensione di Galois è un'estensione  $L|K$  di campi nella quale  $L$  si ottiene aggiungendo a  $K$  tutte le radici di un polinomio irriducibile e separabile a coefficienti in  $K$ .*

Si ricordi che un polinomio irriducibile è separabile se non ha radici multiple. Di conseguenza, un'estensione di campi viene detta separabile se sono separabili i polinomi minimi di tutti i suoi elementi.

Il passo ulteriore fu quello di osservare che la precedente definizione poteva essere resa indipendente dalla scelta del polinomio.

(2) *Un'estensione di Galois è un'estensione finita e separabile  $L|K$  che soddisfa la seguente proprietà: se un polinomio irriducibile a coefficienti in  $K$  ha una radice in  $L$ , tutte le sue radici sono in  $L$ .*

Qui l'accento è già sui campi, ma i polinomi rimangono ancora in agguato. Un ulteriore passo verso l'astrazione divenne possibile quando Dedekind definì il grup-

po di Galois come il gruppo degli automorfismi di un'estensione di Galois. Negli approcci precedenti era sempre definito come un gruppo che permuta le radici di un polinomio defintorio.

(3) *Un'estensione di Galois è un'estensione finita e separabile  $L|K$  per la quale ogni elemento di  $L$  che non appartiene a  $K$  viene trasformato da un automorfismo di  $L$  che tiene fisso  $K$ .*

Il legame con la precedente definizione è il seguente: un automorfismo di  $L$  che tiene fisso  $K$  deve trasformare un elemento  $\alpha \in L$  in un'altra radice del suo polinomio minimo su  $K$ . Se  $\alpha$  non è in  $K$ , esiste almeno un'altra radice del genere.

L'ultimo passo venne fatto da Emil Artin negli anni '40. È la definizione più elegante di estensione finita di Galois.

(4) *Un'estensione di Galois è un'estensione  $L|K$  in cui  $K$  è il campo fisso di un gruppo finito  $G$  di automorfismi che agiscono su  $L$ .*

Per mettere in relazione questa definizione con la precedente, occorre dimostrare che una estensione di campi come quella data qui sopra è automaticamente separabile. La proprietà della definizione segue di conseguenza. Il gruppo  $G$  è detto gruppo di Galois dell'estensione  $L|K$ .

Sempre Artin formulò la corrispondenza di Galois come la conosciamo oggi. Ricordiamo l'enunciato:

*Sia  $L|K$  un'estensione finita di Galois con gruppo di Galois  $G$ . Esiste una corrispondenza biunivoca fra le estensioni  $M|K$  contenute in  $L$  ed i sottogruppi  $H \subset G$ . Le estensioni di Galois corrispondono ai sottogruppi normali. In questo caso, il gruppo di Galois di  $M$  su  $K$  è isomorfo a  $G/H$ .*

La corrispondenza è data associando ad  $M$  il sottogruppo di  $G$  i cui elementi fissano  $M$  elemento per elemento e, viceversa, associando ad un sottogruppo  $H \subset G$  il sottocampo di  $L$  fissato da  $H$ .

Questo enunciato è perfettamente nello spirito della grande scuola algebrica tedesca dell'inizio del XX secolo. Ancora oggi lo insegnamo e lo applichiamo. Rimaneva tuttavia un ulteriore passo da intraprendere: quello di indebolire la condizione di finitezza.

## 2. IL GRUPPO DI GALOIS ASSOLUTO

Esistono molte motivazioni per studiare le estensioni algebriche infinite. Una di queste proviene dalla ricerca di classi speciali di estensioni nella teoria algebrica dei numeri. Ad esempio, i campi ciclotomici, che sono ottenuti aggiungendo al

campo  $\mathbf{Q}$  dei numeri razionali una radice  $\omega$  dell'unità, hanno sempre svolto un ruolo rilevante a partire dalla scoperta della loro importanza per l'ultimo teorema di Fermat. Ogni radice  $n$ -ma di  $\omega$  è ancora una radice dell'unità, pertanto i campi ciclotomici danno luogo in maniera naturale alla comparsa di torri di estensioni di campi. Ad esempio, si può fissare un numero primo  $p$  e considerare la torre  $\mathbf{Q}(\mu_p) \subset \mathbf{Q}(\mu_{p^2}) \subset \mathbf{Q}(\mu_{p^3}) \subset \dots$  dei campi che si ottengono aggiungendo le radici dell'unità  $p$ -esima,  $p^2$ -esima,  $p^3$ -esima e così via. La loro unione è una estensione algebrica infinita molto interessante, il cui studio ha portato alla nascita di uno dei rami più importanti dell'aritmetica di oggi, la *teoria di Iwasawa*.

Un'altra motivazione sorge da un problema puramente algebrico: come trovare dei campi sui quali ogni equazione polinomiale ha una soluzione? Che non si tratti di un problema puramente accademico è un fatto che risale ad un famoso teorema di Gauss, oggi noto come *teorema fondamentale dell'algebra*:

*Sul campo  $\mathbf{C}$  dei numeri complessi, ogni equazione polinomiale  $f = 0$  ha una radice  $\alpha \in \mathbf{C}$ .*

Inoltre, ogni radice dell'equazione deve essere in  $\mathbf{C}$ , come si vede dividendo  $f$  per fattori della forma  $(x - \alpha)$ .

Ma come trovare altri esempi? C'è un'idea naturale: partire da un campo  $K$  e cercare un metodo per aggiungere a  $K$  tutte le soluzioni delle equazioni polinomiali a coefficienti in  $K$ . Il campo risultante  $\overline{K}$  avrà la proprietà richiesta. Infatti, per costruzione di  $\overline{K}$ , dato un polinomio  $f$  a coefficienti in  $\overline{K}$ , i suoi coefficienti, che sono in numero finito, appartengono a qualche estensione finita  $L$  di  $K$ . Ma allora una radice  $\alpha$  di  $f$  giace in un'estensione finita di  $L$  che è ancora un'estensione finita di  $K$ . In quanto tale, è generata dalle radici di un polinomio a coefficienti in  $K$  e dunque  $\alpha$  deve giacere in  $\overline{K}$ .

Per  $K = \mathbf{Q}$  la costruzione di  $\overline{K}$  è facile. Basta considerare  $\mathbf{Q}$  come sottocampo di  $\mathbf{C}$  e prendere tutti i numeri complessi che sono radici di qualche polinomio a coefficienti in  $\mathbf{Q}$ . Si dimostra che questi numeri formano un campo, il *campo dei numeri algebrici*. Giacché dal teorema fondamentale dell'algebra sappiamo che le radici di ogni polinomio a coefficienti in  $\mathbf{Q}$  giacciono in  $\mathbf{C}$ , abbiamo risolto il problema.

Per quei campi che non possono essere immersi in  $\mathbf{C}$  (ad esempio quelli di caratteristica positiva o le estensioni trascendenti di  $\mathbf{C}$ ) il metodo precedente non funziona. La soluzione generale fu trovata in un articolo fondamentale di Steinitz [6] che utilizzava le tecniche, abbastanza nuove per il tempo, della teoria degli insiemi, in particolare l'assioma di scelta. Egli dimostrò:

*Ogni campo  $K$  ha una chiusura algebrica  $\overline{K}$  che è un'estensione algebrica di  $K$*

tale che ogni equazione polinomiale a coefficienti in  $\overline{K}$  ha una radice in  $\overline{K}$ . Inoltre  $\overline{K}$  è unico, a meno di un, non unico, isomorfismo.

È questa non unicità che risulta cruciale per sviluppare la teoria di Galois infinita. Il fatto che  $\overline{K}$  sia algebrico su  $K$  significa che è generato dalle radici di polinomi a coefficienti in  $K$ . Si ha pertanto che  $\overline{K}$  si ottiene veramente aggiungendo in maniera sistematica tutte le radici di questi polinomi.

Una volta che si dispone di una chiusura algebrica  $\overline{K}$  è possibile definire una chiusura separabile  $K_s$  di  $K$  come quella degli elementi di  $\overline{K}$  il cui polinomio minimo su  $K$  è separabile. Si verifica che questi elementi formano un campo sul quale ogni polinomio separabile ha una radice. Si consideri ora il gruppo degli automorfismi di  $K_s$  che fissano  $K$ . Questo è il *gruppo di Galois assoluto* di  $K$ : lo denotiamo con  $\Gamma$ . Dipende dalla scelta di  $K_s$ , ma la sua classe di isomorfismi non ne dipende.

Il gruppo assoluto di Galois  $\Gamma$  ha molti aspetti importanti. In primo luogo ha la proprietà della precedente definizione (3): ogni elemento  $\alpha \in K_s$ , non in  $K$ , viene trasformato da qualche elemento di  $\Gamma$ . La dimostrazione di questo fatto usa un altro teorema non banale di Steinitz: trasformando  $\alpha$  in un'altra radice  $\alpha'$  del suo polinomio minimo, l'isomorfismo che ne risulta  $K(\alpha) \xrightarrow{\sim} K(\alpha')$  si può estendere ad un automorfismo di  $K_s$ . Un altro punto importante è che  $K_s$  è l'unione di tutte le estensioni finite di Galois di  $K$  che sono contenute in  $\overline{K}$ ; questo avviene perché è possibile immergere ogni estensione separabile finita in una estensione finita di Galois. Inoltre, la considerazione di  $\Gamma$  fornisce un metodo per dare un'ulteriore definizione di estensione finita di Galois:

(5) *Un'estensione separabile finita  $L|K$  contenuta in  $K_s$  è di Galois se  $\sigma(L) \subset (L)$  per ogni  $\sigma \in \Gamma$ .*

Il fatto che  $L$  sia contenuto in  $K_s$  non è una restrizione severa, in quanto ogni  $L$  separabile su  $K$  può essere immerso in  $K_s$ . Otteniamo così un'altra comprensione degli aspetti fondamentali della teoria di Galois: si può decidere se un'estensione è di Galois utilizzando il gruppo assoluto di Galois che “è sempre lì”. Il prossimo passo consiste nell'usarlo per descrivere *tutti* i sottocampi di  $K_s$ .

### 3. TEORIA DI GALOIS INFINITA

La discussione dei paragrafi precedenti motiva alcune maniere equivalenti per definire un'estensione di Galois possibilmente infinita. Ne citiamo due. La prima è una variante della definizione (3): un'estensione di Galois è un'estensione algebrica separabile  $L|K$  tale che ogni elemento di  $L$  che non giace in  $K$  sia trasformato da

un automorfismo di  $L$  che fissa  $K$ . La seconda è motivata dalla definizione (5): un'estensione  $L|K$  contenuta in  $K_s$  è di Galois se  $\sigma(L) \subset L$  per ogni  $\sigma$  del gruppo assoluto di Galois  $\Gamma$ . L'estensione di Galois infinita più interessante è naturalmente la chiusura separabile  $K_s$ .

Qualche che sia la definizione adottata, c'è un unico modo per definire il gruppo di Galois  $Gal(L|K)$ : è il gruppo degli automorfismi di  $L$  che fissano  $K$ . Tuttavia, è la seconda definizione che ci fornisce la chiave di una fondamentale proprietà del gruppo di Galois. Precisamente, data un'estensione di Galois  $M|K$  contenuta in  $L$ , si ha un omomorfismo naturale di gruppi  $Gal(L|K) \rightarrow Gal(M|K)$  per restrizione degli automorfismi da  $L$  a  $M$ . Inoltre, questo omomorfismo è suriettivo grazie al teorema di Steinitz menzionato nel paragrafo precedente: è possibile estendere ogni automorfismo di  $M$  su  $K$  ad un automorfismo di  $K_s$ , il quale deve preservare  $L$  per definizione. Quindi  $Gal(M|K)$  si presenta come quoziente di  $Gal(L|K)$ ; in particolare questo fatto si applica a tutte le estensioni di Galois finite contenute in  $L$ .

Il fatto fondamentale ora è che  $Gal(L|K)$  è completamente determinato dai suoi quozienti finiti. Ciò non è poi tanto sorprendente se si ricorda dal paragrafo precedente che  $L$  è l'unione di tutte le estensioni di Galois finite che contiene. Tuttavia, una formulazione precisa di questo fatto richiede uno strumento algebrico sofisticato che si chiama *limite inverso*: si dice che  $Gal(L|K)$  è il limite inverso dei suoi quozienti finiti. Un gruppo che sia il limite inverso di gruppi finiti viene detto *gruppo profinito*. Non diamo qui i dettagli delle definizioni di limite inverso e di gruppo profinito. Ciò che importa tenere a mente è che i gruppi profiniti sono determinati dai loro quozienti finiti.

I gruppi profiniti hanno un'importante proprietà aggiuntiva: sono *gruppi topologici*. È possibile introdurre la topologia per mezzo di un metodo generale che parte mettendo la topologia discreta su ogni quoziente finito. Tuttavia, nel caso dei gruppi di Galois, esiste un approccio più diretto, introdotto da Krull nell'innovatore articolo [4] sulla teoria di Galois infinita. Per tutte le estensioni di Galois finite  $M|K$  contenute in  $L$ , si considerino i nuclei degli omomorfismi  $Gal(L|K) \rightarrow Gal(M|K)$  visti in precedenza e si dichiara che questo è un sistema di intorni aperti dell'identità di  $Gal(L|K)$ . Per un elemento generico  $\sigma \in Gal(L|K)$ , un sistema di intorni aperti è dato dai laterali  $\sigma U$ , dove  $U$  è un intorno aperto dell'identità. Si verifica che questi insiemi aperti formano la base di una topologia su  $Gal(L|K)$ : in onore del suo scopritore è detta *topologia di Krull*. Si dimostra che  $Gal(L|K)$  con la topologia di Krull è un gruppo topologico compatto di Hausdorff.

Ogni sottogruppo aperto di  $Gal(L|K)$  è anche chiuso poiché il suo comple-

mento è unione di laterali che devono essere anch'essi aperti. Quindi, ogni intersezione, anche infinita, di sottogruppi aperti è un sottogruppo chiuso. D'altra parte, non è difficile mostrare che ogni sottogruppo chiuso è intersezione degli aperti che lo contengono. Questo suggerisce come sviluppare la corrispondenza di Galois per le estensioni infinite: poiché i sottogruppi normali aperti corrispondono alle estensioni finite di Galois, i sottogruppi chiusi devono corrispondere alle estensioni arbitrarie di Galois, ancora per il fatto che queste ultime sono unioni di estensioni finite di Galois. In effetti, Krull ha dimostrato la seguente corrispondenza generalizzata di Galois:

*Sia  $L|K$  un'estensione di Galois con gruppo di Galois  $G$ . Esiste una corrispondenza biunivoca fra le estensioni  $M|K$  contenute in  $L$  e i sottogruppi chiusi  $H \subset G$ . Le estensioni finite corrispondono ai sottogruppi aperti e le estensioni di Galois ai sottogruppi normali chiusi. In quest'ultimo caso, il gruppo di Galois di  $M$  sopra  $K$  è isomorfo a  $G/H$ .*

A questo punto sorge in maniera naturale la questione se esistano sottogruppi non chiusi nel gruppo di Galois  $G$  o, in altre parole, se esistano sottogruppi che non si presentano come sottogruppi di elementi di  $G$  che fissano qualche estensione. Di fatto, questa questione è stata risolta da Dedekind [2], ben prima che Krull formulasse la sua teoria. Il suo argomento era il seguente: se  $L_1 \subset L_2 \subset L_3 \subset \dots$  è una catena strettamente crescente di estensioni di Galois finite di  $K$ , allora ogni automorfismo di  $Gal(L_i|K)$  si può estendere almeno in due modi a  $L_{i+1}$  per la classica teoria di Galois. Dunque, una catena infinita dà luogo ad un gruppo di Galois non numerabile che ha una quantità non numerabile di sottogruppi. Ma se il campo di base  $K$  è numerabile, ad esempio  $K = \mathbf{Q}$ , esiste soltanto una quantità numerabile di estensioni finite di  $K$  perché esiste soltanto una quantità numerabile di polinomi a coefficienti in  $K$ . Occorre osservare al proposito che questo lavoro di Dedekind fornì la maggiore ispirazione alla teoria di Krull. Di fatto, già Dedekind aveva intuito che i gruppi di Galois infiniti devono godere di qualche proprietà di continuità.

Nelle situazioni concrete è facile mostrare dei sottogruppi non chiusi. Ad esempio, se  $\mathbf{F}_q$  denota il campo finito di ordine  $q$ , l'automorfismo di Frobenius  $F : x \mapsto x^q$  di  $\overline{\mathbf{F}}_q$  non genera un sottogruppo chiuso. Di fatto è facile descrivere la teoria di Galois dell'estensione infinita  $\overline{\mathbf{F}}_q|\mathbf{F}_q$  senza menzionare i gruppi profiniti. Come sappiamo dalla teoria dei campi finiti, per ogni intero  $r > 0$  esiste un'unica sottoestensione  $\mathbf{F}_{q^r}|\mathbf{F}_q$  di  $\overline{\mathbf{F}}_q|\mathbf{F}_q$  di grado  $r$  su  $\mathbf{F}_q$  ed inoltre è un'estensione di Galois di  $\mathbf{F}_q$  con gruppo  $\mathbf{Z}/r\mathbf{Z}$ . Ne segue che i sottogruppi aperti di  $\Gamma = Gal(\overline{\mathbf{F}}_q|\mathbf{F}_q)$  sono totalmente ordinati rispetto all'inclusione e quindi ogni

sistema di sottogruppi aperti ha intersezione banale oppure ha un elemento minimo. Quindi ogni sottogruppo non banale chiuso  $H \subset \Gamma$  è di fatto aperto; inoltre è normale e  $\Gamma/H$  è ciclico. Il sottogruppo ciclico infinito di  $\Gamma$  generato da  $F$  non è aperto: il suo campo fisso è  $\mathbf{F}_q$  ma non uguaglia  $\Gamma$ .

#### 4. LA RIFORMULAZIONE DI GROTHENDIECK

Alexander Grothendieck, la cui influenza sulla matematica nella seconda metà del XX secolo è paragonabile a quella di Galois nel XIX, ha trovato una riformulazione molto utile del teorema fondamentale della teoria di Galois che può essere generalizzata ad altri, numerosi, casi. Nel suo seminario [3], ha dato una generale formulazione categoriale che comprende molte situazioni. Qui ci riferiamo al caso già considerato delle estensioni di campi. Secondo il punto di vista di Grothendieck, lo scopo della teoria di Galois è quello di classificare le estensioni separabili finite di un dato campo per mezzo di rappresentazioni di permutazioni.

Per chiarire questa idea, sia  $K$  un campo di base e  $L|K$  un'estensione separabile finita. Si fissi una chiusura separabile  $K_s$  di  $K$ . Come sappiamo dal lavoro dello stesso Galois,  $L$  è generato su  $K$  da un solo elemento  $\alpha$ . Sia  $f$  il polinomio minimo di  $\alpha$  su  $K$  e  $\alpha_1, \alpha_2, \dots, \alpha_n$  siano le radici di  $f$  in  $K_s$ . Il gruppo assoluto di Galois  $\Gamma := \text{Gal}(K_s|K)$  agisce con permutazioni sull'insieme finito  $\alpha_1, \alpha_2, \dots, \alpha_n$ : per ogni  $\sigma \in \Gamma$ , la  $n$ -pla  $\sigma(\alpha_1), \sigma(\alpha_2), \dots, \sigma(\alpha_n)$  è ancora il sistema degli  $\alpha_i$  disposto eventualmente in maniera diversa. Ci sono due importanti proprietà di questa azione. Dapprima, è *transitiva*, vale a dire, dati comunque  $\alpha_i$  e  $\alpha_j$  si può trovare un  $\sigma \in \Gamma$  tale che  $\sigma(\alpha_i) = \alpha_j$ . Inoltre è *continua* rispetto alla topologia di  $\Gamma$ . Ciò significa che, per ogni  $\alpha_i$ , l'insieme dei  $\sigma$  tali che  $\sigma(\alpha_i) = \alpha_i$  è un sottogruppo aperto di  $\Gamma$ .

La riformulazione di Grothendieck può ora essere espressa come segue:

*Esiste una corrispondenza biunivoca fra le classi di isomorfismo delle estensioni separabili finite di  $K$  e gli insiemi finiti  $S$  con un'azione transitiva continua di  $\Gamma$ .*

Abbiamo già visto come associare un  $\Gamma$ -insieme finito e continuo ad un'estensione di campi. Per ottenere il passaggio in senso inverso, si prende un elemento  $\alpha_i \in S$  e si considera il suo stabilizzatore in  $\Gamma$ , vale a dire l'insieme dei  $\sigma \in \Gamma$  tali che  $\sigma(\alpha_i) = \alpha_i$ . È un sottogruppo aperto di  $\Gamma$ , quindi, per la teoria di Galois infinita, fissa un'estensione separabile finita  $L|K$ . Se si sceglie lo stabilizzatore di un altro elemento, si arriva al campo fisso di un sottogruppo aperto coniugato, il quale fissa un'estensione isomorfa ad  $L$ .

In qualche senso, rispetto alla corrispondenza di Galois di Artin, la precedente

formulazione della teoria di Galois è più vicina all'approccio originale di Galois, in quanto anche Galois considerava la rappresentazione delle permutazioni del gruppo di Galois sulle radici dell'equazione: questo fatto rimane abbastanza in ombra se si considera soltanto la corrispondenza sottogruppi - sottocampi.

La condizione di transitività della  $\Gamma$ -azione può essere indebolita pur di considerare non solo le estensioni separabili finite di  $K$  ma anche i loro prodotti diretti finiti. Seguendo Grothendieck, questi sono usualmente detti *k-algebre étale finite*.

## 5. RAPPRESENTAZIONI DI MONODROMIA

Un'altra situazione, già abbondantemente studiata nel XIX secolo, nella quale le equazioni possono essere classificate per mezzo di rappresentazioni di gruppi è la teoria della monodromia delle equazioni differenziali. Si consideri un'equazione differenziale lineare:

$$(1) \quad y^{(n)} + a_1 y^{(n-1)} + \dots + a_{(n-1)} y' + a_n y = 0$$

nel piano complesso  $\mathbf{C}$ , dove i coefficienti  $a_i$  sono funzioni complesse, olomorfe con l'eccezione di un numero finito di punti  $x_1, x_2, \dots, x_r$ , dove si possono estendere meromorficamente. Per un fondamentale teorema di esistenza di Cauchy, ogni punto  $x \neq x_i$  ha un intorno aperto  $U$ , che non contiene nessuno degli  $x_i$ , nel quale l'equazione ha  $n$  soluzioni locali olomorfe  $y_1, y_2, \dots, y_n$ , linearmente indipendenti su  $\mathbf{C}$ . Inoltre, ogni soluzione locale su  $U$  è una loro combinazione lineare. In altri termini, localmente intorno ad  $x$ , le soluzioni dell'equazione formano uno spazio vettoriale di dimensione  $n$  su  $\mathbf{C}$ .

Il problema è che, muovendo il punto  $x$ , lo spazio delle soluzioni può non rimanere lo stesso. Per rendersene conto, si consideri il più semplice esempio, quando  $r = 1$  e l'equazione ha la forma

$$y' = fy$$

con una funzione meromorfa  $f$ , olomorfa al di fuori di  $x_1$ . È noto che tutte le soluzioni locali dell'equazione sono multipli per una costante della funzione  $\exp \circ F$ , dove  $F$  è una primitiva di  $f$ . Tuttavia, l'analisi complessa di base insegna che una primitiva di  $f$  non esiste su tutto  $X \setminus \{x_1\}$  ma soltanto su  $X \setminus D$  dove  $D$  è una semiretta che parte da  $x_1$ . Ad esempio, se  $x_1 = 0$ , esiste una ben definita primitiva  $F_-$  di  $f$  su  $U_- = \mathbf{C} \setminus [0, -i\infty)$  ed un'altra primitiva  $F_+$  sopra  $U_+ = \mathbf{C} \setminus [0, i\infty)$ . L'intersezione  $U_- \cap U_+$  si spezza in due componenti connesse  $C_- = \{z : \operatorname{Re}(z) < 0\}$

e  $C_+ = \{z : \operatorname{Re}(z) > 0\}$ . Poiché  $F_+$  ed  $F_-$  possono differire soltanto per una costante su ciascuna componente, è possibile prenderle in modo che sia  $F_- = F_+$  su  $C_-$ , ma allora differiranno per una costante  $c$  su  $C_+$ ! Dunque, scegliendo un ciclo chiuso intorno a 0, ad esempio la circonferenza di raggio 1, in un intorno di 1 possiamo prendere la soluzione locale  $\exp \circ F_+$ . Muovendosi da 1 lungo la circonferenza, possiamo ancora usare per qualche tempo la stessa soluzione locale intorno a ciascun punto della circonferenza, ma in qualche punto di  $C_-$  dobbiamo cambiare  $F_+$  in  $F_-$ , perché  $F_+$  non è definito su tutta la circonferenza. Di conseguenza, tornati ad 1, si ottiene  $\exp \circ F_-$  come ‘continuazione’ della soluzione locale, che è  $e^c(\exp \circ F_+)$ . La costante  $e^c$  è la *monodromia* dell’equazione attorno a 0.

Il procedimento qui sopra può essere generalizzato all’equazione generale (1). Si scelgano dei cicli chiusi  $\gamma_i$  passanti per  $x$  e tali che ciascuno di essi abbia al proprio interno soltanto il punto  $x_i$ , ma non  $x_j$ . Per un  $i$  fissato si può ripetere quanto fatto nel caso particolare discusso in precedenza: partiamo da una soluzione locale  $y_x$  di (1) attorno ad  $x$  e consideriamo la sua continuazione ad una soluzione locale lungo  $\gamma_i$ . Tornati ad  $x$ , abbiamo un’altra soluzione locale  $z_x$  attorno ad  $x$ . In generale non sarà un multiplo rispetto a una costante, perché l’equazione può essere più complicata, tuttavia giacerà nello stesso spazio vettoriale delle soluzioni locali attorno ad  $x$ .

Possiamo procedere in questo modo per ogni  $i$ . Un ostacolo apparente è che il risultato dipenda *a priori* dalla scelta dei cicli  $\gamma_i$ , tuttavia il classico *teorema di monodromia* dell’analisi complessa dice che ciò non è vero: cambiando  $\gamma_i$  con un altro ciclo  $\gamma'_i$  con le stesse proprietà, la soluzione locale risultante  $z_x$  sarà la stessa. Dal punto di vista moderno, ciò avviene perché  $\gamma_i$  e  $\gamma'_i$  sono *omotopi*: possono essere deformati con continuità l’uno nell’altro senza incontrare nessun  $x_i$  nel cammino. Questa osservazione è il germe della nozione di *gruppo fondamentale*: si possono considerare, a meno di deformazioni continue, *tutti* i cicli chiusi passanti per  $x$  che non toccano i punti  $x_i$ . Su questo insieme è possibile introdurre un’operazione di gruppo, prendendo come prodotto di due cicli  $\gamma$  e  $\delta$  il ciclo ottenuto percorrendo  $\delta$  e poi  $\gamma$  (passa due volte per  $x$ , ma lo si può deformare in modo che ciò non avvenga: ad esempio, il prodotto  $\gamma_i \cdot \gamma_j$  può essere rappresentato da un ciclo attorno ad  $x$  che non si autointerseca e contiene al proprio interno  $\gamma_i$  e  $\gamma_j$ ). Il gruppo  $\Pi$  che ne risulta è generato dalle classi dei cicli  $\gamma_i$ . Si osservi che l’operazione di continuazione delle soluzioni locali di (1) lungo cicli che rappresentano elementi di  $\Pi$  è  $\mathbf{C}$ -lineare. In altri termini, si ha un’azione di  $\Pi$  sullo spazio vettoriale su  $\mathbf{C}$  delle soluzioni di (1) attorno ad  $x$ . Fissata una base  $y_1, y_2, \dots, y_n$  di questo spazio,

si ottiene un omomorfismo  $\rho : \Pi \rightarrow GL(n, \mathbf{C})$  che viene detto *rappresentazione di monodromia* di (1) attorno ad  $x$ .

Il problema che ora sorge è il seguente: è possibile classificare le equazioni differenziali per mezzo delle loro rappresentazioni di monodromia, allo stesso modo con cui le rappresentazioni delle permutazioni del gruppo di Galois classificano le estensioni finite di campo? Il lettore dotato di intuito avrà subito osservato che il problema non è formulato correttamente. Dare un'estensione di campi non è la stessa cosa che dare un'equazione polinomiale, anche se è noto che ogni estensione finita proviene di fatto da un polinomio. Per le equazioni differenziali, il problema deve analogamente essere spezzato in due parti.

La prima parte è usualmente detta *corrispondenza di Riemann-Hilbert*. In forma elementare dice:

*Esiste una corrispondenza biunivoca fra le classi di isomorfismo delle rappresentazioni di monodromia  $\rho : \Pi \rightarrow GL(n, \mathbf{C})$  ed i sistemi locali, cioè i sistemi di funzioni olomorfe sui sottoinsiemi aperti di  $\mathbf{C}$ , non contenenti gli  $x_i$ , che localmente, attorno a ciascun punto, formano uno spazio vettoriale  $n$ -dimensionale su  $\mathbf{C}$ .*

La seconda parte è il *problema di Riemann-Hilbert*, il quale chiede:

*È vero che ogni sistema locale (e quindi ogni rappresentazione di monodromia) proviene da un'equazione differenziale lineare (1)?*

La risposta non è priva di ambiguità, soprattutto se si richiedono proprietà addizionali all'equazione. Citiamo il più famoso risultato classico, quello di Pljmelj [5]:

*Ogni sistema locale come sopra proviene da un'equazione differenziale lineare (1) i cui coefficienti sono funzioni meromorfe in  $\mathbf{C}$ . Inoltre, si può scegliere l'equazione in modo che sia Fuchsiana, vale a dire che in ogni punto singolare il coefficiente  $a_i$  abbia un polo al più di ordine  $i$ .*

È importante osservare che, sebbene nel precedente enunciato i coefficienti dell'equazione hanno al massimo dei poli in  $x_i$ , possono anche avere dei poli in un numero finito di altri punti. Si può considerare una rappresentazione di monodromia che tenga conto anche di questi poli ulteriori, pur di considerare la condizione addizionale che l'azione degli elementi del gruppo che provengono da cicli attorno a questi punti extra sia banale. In altre parole, che la continuazione di una soluzione locale attorno a questi punti non cambi. Questi punti sono chiamati classicamente *singolarità apparenti*. Se non si ammettono le singolarità apparenti, l'enunciato non vale. Per una splendida introduzione al problema di Riemann-Hilbert ed alle

sue generalizzazioni, si veda il rendiconto di Beauville [1].

Siamo così arrivati ad enunciati che somigliano alla formulazione moderna della teoria di Galois. Grazie largamente all'intuito di Grothendieck è ora possibile sviluppare molte teorie generali che le comprendono entrambe; si veda ad esempio il mio libro [7], dove i concetti esaminati in questo articolo sono spiegati in maggior dettaglio. Ma i legami fra questi campi della matematica sono ancora più forti. Negli ultimi decenni, le equazioni differenziali e, in misura ancora maggiore, le considerazioni topologiche che sorgono dalla loro teoria, sono state applicate con successo alla costruzioni di interessanti estensioni di Galois di campi come  $\mathbf{C}(t)$  ed anche di  $\mathbf{Q}$ . D'altro lato, metodi presi nella teoria di Galois si sono dimostrati di fondamentale importanza per analizzare le equazioni differenziali. Possiamo felicemente osservare che, due secoli dopo Galois, le sue idee non sono soltanto più vive che mai, ma hanno invaso gran parte della ricerca matematica moderna.

#### BIBLIOGRAFIA

A. Beauville, Monodromie des systèmes différentielles linéaires à pôles simples sur la sphère de Riemann [d'après A. Bolibruch], Séminaire Bourbaki, exposé 765, *Astérisque* 216 (1993), 103–119.

R. Dedekind, *Über die Permutationen des Körpers aller algebraischen Zahlen*, Abhandlungen der Gesellschaft der Wissenschaften zu Göttingen, 1901.

A. Grothendieck, *Revêtements étales et groupe fondamental* (SGA 1), Lecture Notes in Mathematics, vol. 224, Springer-Verlag, Berlin-New York, 1971. New annotated edition: Société Mathématique de France, Paris, 2003.

W. Krull, Galoissche Theorie der unendlichen algebraischen Erweiterungen, *Math. Ann.* **100** (1928), 687–698.

J. Pljemeľ, Riemannsche Funktionenscharen mit gegebener Monodromiegruppe, *Monatshefte Math. Phys.* 19 (1908), 211–246.

E. Steinitz, Algebraische Theorie der Körper, *J. reine angew. Math.* 137 (1908), 167–309.

T. Szamuely, *Galois Groups and Fundamental Groups*, Cambridge Studies in Advanced Mathematics, vol. 117, Cambridge University Press, 2009.