UNIVERSITÀ DEGLI STUDI DI ROMA TRE
FACOLTÀ DI SCIENZE M.F.N.

Teoria Computazionale di Galois

Sintesi della Tesi di Laurea in Matematica
di
Silvia Ghigi

Relatore: Francesco Pappalardi

La Teoria di Galois è la teoria matematica che associa ad ogni polinomio in una variabile a coefficienti in un campo un gruppo, il gruppo di automorfismi del suo campo di spezzamento.

Tale gruppo descrive alcune proprietà fondamentali del polinomio e del suo campo di spezzamento. Ad esempio il gruppo di Galois permette di determinare se un'equazione polinomiale è risolubile per radicali, cioè se il campo di spezzamento del polinomio che definisce tale equazione è contenuto in un ampliamento radicale del suo campo di definizione, e quindi le radici del polinomio in questione sono esprimibili come funzioni radicali e razionali dei coefficienti.

Questo problema è forse la genesi della Teoria di Galois, matematico francese morto prematuramente in duello, che nel 1830 dimostrò:

Teorema di Galois (1830). *Sia $f(X) \in \mathbb{Q}[X]$, F campo. Allora $f(X)$ è risolubile per radicali se e soltanto se il suo gruppo di Galois su $\mathbb{Q}$ è un gruppo risolubile.*

Dunque la Teoria di Galois permette di spostare il problema della risolubilità per radicali allo studio dei gruppi risolubili: risulta fondamentale saper calcolare esplicitamente il gruppo di Galois del polinomio che definisce l'equazione da studiare.

In questa tesi vengono studiati dei metodi generali che portano alla formulazione di algoritmi specifici per il calcolo dei gruppi di Galois dei polinomi monici irriducibili di grado ≤ 7 a cofficienti razionali. I campi considerati sono dunque tutti sottocampi di $\mathbb{C}$.

Nel primo capitolo vengono ricordati i risultati più importanti della Teoria di Galois; in particolare, dopo aver definito il gruppo di Galois di un ampliamento normale di campi, è enunciato e dimostrato il Teorema fondamentale, che stabilisce la corrispondenza biunivoca tra i sottogruppi del gruppo di Galois di un polinomio ed i sottocampi del suo campo di spezzamento.

Sia L un ampliamento normale e finito di K e sia $G = Gal(L/K)$. La seguente corrispondenza è biunivoca:

$$\left\{\text{campi } F,\ K \subseteq F \subseteq L\right\} \longleftrightarrow \left\{\text{gruppi } H,\ H \subseteq G\right\}$$
$$L^H \longmapsto H$$
$$F \longmapsto Gal(L/F).$$

Inoltre viene analizzata l'azione del gruppo di Galois sulle radici del polinomio, che ha luogo in quanto tale gruppo si interpreta come un gruppo di permutazioni sulle radici stesse, e quindi come sottogruppo di S_n, dove n è il grado del polinomio. Più precisamente si ha l'omomorfismo iniettivo:

$$G = Gal_K p(X) \xrightarrow{\iota} S_n$$
$$\sigma \longmapsto \iota(\sigma)$$

dove $\iota(\sigma)(i) = j$ se $\sigma(r_i) = r_j$ ($r_1, \ldots, r_n$ sono le n radici di $p(X)$).

Nel secondo capitolo è descritto e spiegato il metodo fondamentale per il calcolo dei gruppi di Galois, basato sullo studio del polinomio risolvente tratto dall'articolo di Stauduhar [Sta].

Un polinomio risolvente di $f(X) \in \mathbb{Q}[X]$ è caratterizzato dal fatto che il suo campo di spezzamento è un sottocampo del campo di spezzamento di f.

Nel Paragrafo 2.3 vengono dimostrati il Teorema fondamentale per determinare il gruppo di Galois di un polinomio irriducibile a coefficienti interi $f(X)$ tramite la risolvente (Teorema 2.5) e l'estensione di tale teorema (Corollario 2.1), sintetizzabili nel seguente:

Teorema. *Sia $f(X) \in \mathbb{Z}[X]$ e sia $n = deg(f)$. Siano $\Gamma = Gal_{\mathbb{Q}} f(X)$ e G sottogruppi di H, con $H \leq S_n$ transitivo. Sia $F(X_1, \ldots, X_n) \in \mathbb{Z}[X_1, \ldots, X_n]$ invariante in H sotto l'azione di tutte e sole le permutazioni di G e sia*

$$Q(H, G) = \prod_{i=1}^{k} (y - \pi_i F(r_1, \ldots, r_n))$$

una risolvente di f, dove $\{\pi_1, \ldots, \pi_k\}$ è un insieme di rappresentanti per le classi laterali destre di H/G e $r_1, \ldots, r_n$ sono le radici di f. Supponiamo inoltre che la risolvente $Q(H, G)$ non abbia radici multiple. Allora

$$\Gamma \subseteq G \iff F(r_1, \ldots, r_n) \in \mathbb{Z}$$

e

$$\Gamma \subseteq \pi_i G \pi_i^{-1} \iff \pi_i F(r_1, \ldots, r_n) \in \mathbb{Z}.$$

Questo risultato permette di decidere se il gruppo di Galois è contenuto o meno in un fissato sottogruppo di S_n.

Poiché i polinomi in considerazione sono irriducibili ed i gruppi di Galois portano radici di un fattore irriducibile in radici dello stesso fattore irriducibile, tali gruppi saranno sottogruppi transitivi di S_n, con $n = deg(f)$.

L'assunzione dell'assenza di radici multiple della risolvente è un fatto fondamentale; qualora ciò non si verifichi è necessario ovviare con la sostituzione del polinomio del quale vogliamo calcolare il gruppo di Galois con un altro polinomio ottenuto attraverso una trasformazione di Tschirnhausen (l'algoritmo è descritto nel Capitolo 6).

Dato un polinomio monico irriducibile a coefficienti interi che definisce un campo numerico $\mathbb{Q}(\vartheta)$ (dove ϑ è una radice del polinomio), una trasformazione di Tschirnhausen permette di trovare un altro polinomio monico irriducibile che definisce lo stesso campo numerico, e dunque possiede lo stesso gruppo di Galois.

Sulla base del Teorema fondamentale della risolvente il procedimento da seguire è quello di calcolare $Q(S_n, G)$ per i sottogruppi transitivi G di S_n,

$G \neq A_n$, a partire da quelli massimali, e verificare se tale risolvente ha radici intere per determinare se Γ è contenuto in qualche coniugato di G.

Va osservato che se $\Gamma \subseteq \pi_i G \pi_i^{-1}$ basta riordinare le radici del polinomio f ponendo $r'_j = r_{\pi_i(j)}$ e si ha $\Gamma \subseteq G$.

L'algoritmo procede finché nessuna delle risolventi ha una radice intera oppure si giunge ad un sottogruppo G minimale. Nel primo caso rimangono solo due possibilità per il gruppo di Galois, A_n e S_n, e per concludere si verifica se il discriminante del polinomio è o meno un quadrato perfetto, sulla base del seguente:

Teorema 2.6. *Sia $p(X) \in \mathbb{Q}[X]$ un polinomio monico irriducibile di grado n. Si ha che $Gal_{\mathbb{Q}} p(X) \subseteq A_n$ se e solo se $\Delta(p(X))$ è un quadrato perfetto.*

Risulta evidente che per poter applicare il metodo della risolvente appena descritto è necessario conoscere le tavole di classificazione dei sottogruppi transitivi di S_n. Proprio per la grande importanza che in questa trattazione riveste il problema della classificazione dei gruppi transitivi, abbiamo deciso di dedicare il Capitolo 5 a questa parte della teoria; in particolare il Paragrafo 5.3 contiene le tavole di classificazione. D'altronde il metodo della risolvente non può essere applicato nel caso in cui tale classificazione non sia nota, ovvero per polinomi di grado superiore a 15.

Nel terzo capitolo è analizzata l'azione del gruppo di Galois sulle radici della risolvente; infatti $\Gamma = Gal_{\mathbb{Q}} p(X)$ agisce sugli zeri della generica risolvente $Q(M_1, M_2)$ permutando gli r_i, zeri di $p(X)$:

$$\Gamma \times \{\pi_1 F(r_1 \dots r_n), \dots, \pi_k F(r_1 \dots r_n)\} \to \{\pi_1 F(r_1 \dots r_n), \dots, \pi_k F(r_1 \dots r_n)\}$$

$$(\sigma, \pi_j F(r_1 \dots r_n)) \mapsto (\sigma \pi_j) F(r_1 \dots r_n)$$

Tramite lo studio delle proprietà di tale azione fatto nell'articolo di Soicher [Soi] si giunge, nel Corollario 3.1, ad una analoga formulazione del Teorema 2.5, ma sotto un diverso punto di vista:

Teorema 3.1. *Sia $p(X) \in \mathbb{Z}[X]$ un polinomio monico irriducibile di grado n. Sia $\Gamma = Gal_{\mathbb{Q}} p(X)$.*

Le orbite dell'azione di Γ *sugli zeri di* $Q(M_1, M_2)$ *sono precisamente l'insieme degli zeri dei distinti fattori irriducibili (su* $\mathbb{Z}$*) di* $Q(M_1, M_2)$*.*
In particolare:

$$\left\{\begin{array}{c}\textit{gradi dei fattori irriducibili}\\ \textit{di } Q(M_1,M_2) \textit{ su } \mathbb{Z}\end{array}\right\} \equiv \left\{\begin{array}{c}\textit{lunghezza delle orbite dell'azione di } \Gamma\\ \textit{sugli } [M_1 : M_2] \textit{ zeri di } Q(M_1,M_2)\end{array}\right\}$$

Corollario 3.1. *$Q(M_1, M_2)$ ha una radice in $\mathbb{Z}$ se e solo se Γ è coniugato ad un sottogruppo di M_2 tramite un elemento di M_1.*

Il quarto capitolo contiene la parte più operativa, ovvero quella degli algoritmi specifici per calcolare il gruppo di Galois di un polinomio monico irriducibile a coefficienti interi di grado $3, 4, 5, 6, 7$, descritti nel libro di Cohen [Co].

Prendere in considerazione solo polinomi monici irriducibili a coefficienti interi non costituisce un fatto restrittivo, in virtù dei seguenti lemmi:

Lemma 1.1. *Se $f(X) = p_1(X)p_2(X) \in \mathbb{Q}[X]$ e p_1, p_2 sono i suoi fattori irriducibili, si ha*

$$Gal_{\mathbb{Q}} f \lesssim Gal_{\mathbb{Q}} p_1 \times Gal_{\mathbb{Q}} p_2$$

tramite l'omomorfismo iniettivo

$$Gal_{\mathbb{Q}} f \longrightarrow Gal_{\mathbb{Q}} p_1 \times Gal_{\mathbb{Q}} p_2$$

$$\sigma \mapsto (\sigma_{|_{K_1}}, \sigma_{|_{K_2}})$$

dove K_i è il campo di spezzamento di p_i su $\mathbb{Q}$. Inoltre

$$Gal_{\mathbb{Q}} f \cong \{(\sigma_1, \sigma_2) \in Gal_{\mathbb{Q}} p_1 \times Gal_{\mathbb{Q}} p_2 |\ \sigma_{1|_{K_1 \cap K_2}} = \sigma_{2|_{K_1 \cap K_2}}\}.$$

Lemma 1.2. *Se $f(X) \in \mathbb{Q}[X]$ allora esiste $h(X) \in \mathbb{Z}[X]$ monico tale che*

$$Gal_{\mathbb{Q}} f = Gal_{\mathbb{Q}} h.$$

Il **grado 3** è molto semplice, in quanto esistono solo due sottogruppi transitivi di S_3, ovvero S_3 stesso e A_3, quindi per concludere basta verificare se il discriminante del polinomio è un quadrato perfetto.

I sottogruppi transitivi di **grado 4** sono cinque $(S_4, A_4, D_4, V_4, C_4)$ e l'algoritmo per tale grado è una applicazione del metodo della risolvente precedentemente descritto. Per calcolare il gruppo di Galois di un qualsiasi polinomio di grado 4 irriducibile a coefficienti interi è necessario al più l'uso di due risolventi, una di terzo grado $(Q(S_4, D_4))$ e una di secondo grado $(Q(D_4, C_4))$.

I sottogruppi transitivi di **grado 5** sono cinque $(S_5, A_5, D_5, M_{20}, C_5)$ e l'algoritmo per tale grado è ancora una fedele applicazione del metodo della risolvente. Per calcolare il gruppo di Galois di un qualsiasi polinomio di grado 5 irriducibile a coefficienti interi è necessario al più l'uso di due risolventi, una di sesto grado $(Q(S_5, M_{20}))$ e una di secondo grado $(Q(D_5, C_5))$.

Il procedimento per il **grado 6** è molto più complesso, infatti i sottogruppi transitivi propri di S_6 sono 15. In questo caso l'algoritmo si basa su una variazione del metodo generale della risolvente descritto nel Paragrafo 2.5, in quanto utilizza la teoria delle trasformazioni razionali, trattata nell'articolo di Girstmair [Gir].

Definizione 4.1. *Siano* $m, n \in \mathbb{N}$. *Sia* $M \subseteq M(m) = \{f \in K[Z]$ *polinomi monici separabili di grado* $m\}$, $H \leq S_n$.

Una <u>*trasformazione razionale*</u> *di* M *in* $M(H) = \{f \in M(n) \mid Gal_K f \cong H\}$ *è un insieme finito* $\mathcal{R}$ *di polinomi in* $K[X_1, X_2, \ldots, X_m, Z]$ *tale che per ogni* $f \in M$ *esiste* $R \in \mathcal{R}$ *con le seguenti proprietà:*

1. $K(R \star f) \subseteq K(f)$
2. $R \star f \in M(H)$

dove, se $f = Z^m + a_1 Z^{m-1} + \cdots + a_m \in K[Z]$, *allora* $R \star f = R(a_1, \ldots, a_m, Z) \in K[Z]$.

Inoltre l'algoritmo per calcolare il gruppo di Galois di un polinomio irriducibile di grado 6 si basa sui seguenti fatti:

1. Ad ogni gruppo $G \leq S_m$ si può associare la partizione di G $l = (l_1, \ldots, l_r)$, $l_1 \geq l_2 \geq \ldots l_r \geq 1$, $l_1 + \cdots + l_r = m$, dove gli l_j sono le lunghezze delle orbite dell'azione di G su $\{1, \ldots, m\}$.

2. Se $f \in M(G)$ allora si fattorizza in $K[Z]$ secondo la partizione l di G, ovvero gli interi $l_1, \ldots, l_r$ sono esattamente i gradi dei fattori irriducibili di f su $K[Z]$.

3. Ogni omomorfismo $\phi : S_m \longrightarrow S_n$ suddivide i sottogruppi di S_m in classi: due gruppi $G, H \leq S_m$ appartengono alla stessa classe se e solo se le partizioni di $\phi(G)$ e $\phi(H)$ coincidono.

L'algoritmo prende in input un polinomio $f \in M(6)$ e determina $G \leq S_6$ tale che $f \in M(G)$.

A priori è fissato un automorfismo non interno ϕ di S_6 (ad esempio quello definito nel libro di Rotman [Rot]). Esso fornisce informazioni supplementari in quanto $Aut(S_6)/Int(S_6) \cong \mathbb{Z}_2$ e ϕ è un automorfismo non interno di S_6 mentre, se $m \neq 6$, $Aut(S_m) = Int(S_m) \cong S_m$. Viene studiata la suddivisione in classi dei sottogruppi transitivi G di S_6 determinata da tale automorfismo in base alla partizione di $\phi(G)$. In questo modo vengono individuate 7 classi.

In base ai teoremi sulle trasformazioni razionali (cfr. Paragrafo 4.4.1) per stabilire in quale classe si trovi il gruppo di Galois di f è sufficiente analizzare la fattorizzazione di una particolare risolvente di f (Proposizione 4.3), che in questo caso ha grado 6. Tale risolvente è $R \star f$, dove $R \in \mathbb{Z}[X_1, \ldots, X_6, Z]$ è un polinomio tratto dall'articolo di Girstmair [Girs].

L'algoritmo passa in rassegna tutte le possibili fattorizzazioni (ognuna individua univocamente una classe di sottogruppi transitivi di S_6) e, per determinare nell'ambito di una stessa classe quale sia il gruppo di Galois, utilizza il calcolo di alcuni discriminanti.

Unica eccezione è rappresentata dalla classe associata ad una risolvente irriducibile; in tal caso è necessario procedere col metodo generale e calcolare una ulteriore risolvente ($Q(S_6, G_{72})$), di grado dieci.

I sottogruppi transitivi propri di S_7 sono sei ($A_7, PSL(2,7), M_{42}, M_{21}, D_7, C_7$) e l'algoritmo per il grado 7 risulta relativamente semplice, in quanto utilizza un'unica risolvente, di grado 35; in questo senso il **grado 7** rappresenta un caso "speciale". Infatti ogni sottogruppo transitivo proprio H di S_7 è

univocamente determinato dalla lunghezza delle orbite della seguente azione:

$$H \times \binom{[7]}{3} \longrightarrow \binom{[7]}{3}$$

$$(\sigma, \{i,j,k\}) \longrightarrow \{\sigma(i), \sigma(j), \sigma(k)\}$$

dove

$$\binom{[7]}{3} = \left\{ \{i,j,k\} \mid i,j,k \in [7] \right\}.$$

La risolvente $g(X)$ utilizzata nell'algoritmo per il grado 7 è la seguente:

$$g(X) = \prod_{\{i,j,k\} \in \binom{[7]}{3}} \left(X - (\vartheta_i + \vartheta_j + \vartheta_k) \right)$$

dove $\vartheta_1, \ldots, \vartheta_7$ sono le radici di $p(X)$, polinomio irriducibile di grado 7 del quale vogliamo calcolare il gruppo di Galois, che denotiamo con Γ. Una tale risolvente ha la proprietà che l'azione di Γ sulle sue radici equivale all'azione di Γ su $\binom{[7]}{3}$, quindi le cardinalità delle orbite di tale azione coincidono con i gradi dei fattori irriducibili di $g(X)$.

L'algoritmo analizza le varie possibilità per i gradi dei fattori irriducibili di $g(X)$, in quanto ad ognuna di queste possibilità corrisponde univocamente un preciso sottogruppo transitivo di S_7 (al più, se la risolvente risulta irriducibile, occorre calcolare anche il discriminante di $p(X)$ per determinare se il gruppo di Galois è S_7 oppure A_7).

Nel quinto capitolo vengono analizzati i sottogruppi transitivi di S_n.

Tale capitolo è fondamentale in quanto, come sottolineato in precedenza, i possibili gruppi di Galois di un polinomio irriducibile sono solo quelli transitivi. Inoltre il metodo della risolvente per trovare il gruppo di Galois richiede la conoscenza delle tavole di classificazione di tali gruppi, contenute nel Paragrafo 5.3.

Definizione 5.1. *Un sottogruppo H di S_n si dice transitivo sull'insieme $[n] = \{1, \ldots, n\}$ se per ogni $i, j \in [n]$ esiste $\sigma \in H$ tale che $\sigma(i) = j$.*

I gruppi transitivi sono suddivisi in due famiglie:

- gruppi primitivi;
- gruppi imprimitivi.

Definizione 5.2. *Un sottogruppo H di S_n si dice imprimitivo se è transitivo e stabilizza una partizione di $[n]$ dove ognuno degli m insiemi della partizione ha la stessa cardinalità k. In altre parole per ogni $\sigma \in H$ e per ogni $i = 1, \ldots, m$ esiste $j \in \{1, \ldots, m\}$ tale che $\sigma P_i = P_j$, dove $P_1, \ldots, P_m$ è una partizione di $[n]$ e $|P_i| = k$. k è chiamato grado di imprimitività di H.*

Se $H \leq S_n$ è transitivo ma non imprimitivo, allora si dice primitivo.

Nel Paragrafo 5.1 sono descritte le tappe fondamentali nella storia della classificazione dei gruppi transitivi di grado basso, che è contenuta nell'articolo di Miller [Mil].

Infine nel settimo capitolo è trattata la teoria degli interi algebrici.

Definizione 7.1. *Un numero complesso è un intero algebrico se è radice di qualche polinomio monico a coefficienti in $\mathbb{Z}$.*

L'insieme degli interi algebrici risulta essere un anello, che indichiamo con $\bar{\mathbb{Z}}$, ovvero

$$\bar{\mathbb{Z}} = \{\alpha \in \mathbb{C} | \, \exists \, p(X) \in \mathbb{Z}[X] \text{ monico tale che } p(\alpha) = 0\}.$$

Dunque le radici dei polinomi presi in considerazione negli algoritmi (in quanto polinomi monici irriducibili a coefficienti interi) sono interi algebrici e ciò è un presupposto fondamentale affinché i polinomi risolventi utilizzati abbiano coefficienti interi (cfr. Teorema 2.4).

Riferimenti bibliografici

[BuMc] G.Butler & J.McKay, *"The transitive groups of degree up to 11"*, Comm.Algebra **11**, (1983), pag. 863-911. 1,5.

[Cay] A.Cayley, *"On the substitution groups for two, three,..., eight letters"*, Quart.J.Pure Appl.Math., v.**25**, (1891), pag. 71-88 e 137-155.

[CHM] J.H.Conway, A.Hulpe & J.McKay, *"On Transitive Permutation Groups"*, LMS J.Comput.Math. **1**, (1998), pag. 1-8.

[Co] H.Cohen, *"A Course in Computational Algebraic Number Theory"*, GTM **138**, Springer-Verlag, Berlin, (1993).

[Gir] K.Girstmair, *"On the Computation of Resolvents and Galois Group"*, Manuscripta Math. **43**, (1983), pag. 289-307.

[Girs] K.Girstmair, *"On Invariant Polynomials and Their Application in Field Theory"*, Math.Comp.**48**, (1987), pag. 781-797.

[Lef] P.Lefton, *"Galois Resolvent of Permutation Groups"*, Amer.Math. Monthly **84**, (1977).

[Mc] J.McKay, *"Some remarks on computing Galois Groups"*, SIAM J.Comput., v.**8**, (1979), pag. 344-347.

[Mil] G.A.Miller, *"Historical note on the determination of all the permutation groups of low degrees"*, The Collected Works of George Abram Miller **1**(ed.George A.Miller), University of Illinois Press, (1935), pag. 1-9. 1

[Rot] J.J.Rotman, *"An introduction to the Theory of Groups"*, GTM **148**, Springer-Verlag, New York, (1995), pag. 156-167.

[Soi] L.Soicher, *"The Computation of the Galois Group"*, Thesis in department of Computer Science, Concordia University, Montreal, Quebec, Canada, (1981).

[SoMc] L.SOICHER & J.MCKAY, *"Computing Galois Groups over the rationals"*, Journal of Number Theory **20**, (1985), pag. 273-281.

[Sta] R.P.STAUDUHAR, *"The determination of Galois groups"*, Math. Comp.**27**, (1973), pag. 981-996.

[Wie] H.WIELANDT, *"Finite Permutation Groups"*, Academic Press, New York, (1968).

Testi sulla Teoria di Galois

[Ar] E.ARTIN, *"Galois theory"*, edited and with a supplemental chapter by A.N.Milgram., reprint of the 1944 second edition, Dover Publications, Inc., Mineola, NY, 1998.

[Art] M.ARTIN,*"Algebra"*, Bollati-Boringhieri, (1998).

[Fe] M.H.FENRICK, *"Introduction to Galois Correspondence"*, Birkäuser, (1992).

[Gab] S.GABELLI, *"Dispense per il corso di AL4"*, Corso di Laurea in Matematica, Università Roma Tre, a.a.2000-2001.

[Hu] T.W.HUNGERFORD, *"Algebra"*, reprint of the 1974 original, GTM **73**, Springer-Verlag, New York-Berlin, 1980.

[Mar] D.A.MARCUS, *"Number Fields"*, Universitext, Springer-Verlag, New York-Heidelberg, (1977).

[Pro] C.PROCESI, *"Elementi di Teoria di Galois"*, Decibel, Zanichelli, seconda ristampa, (1991).

[Ro] J.ROTMAN, *"Galois Theory"*, Universitext, Springer-Verlag, (1990).

[Ste] I.STEWART, *"Galois Theory"*, Chapman and Hall, (1989).

La bibliografia si riferisce all'intera tesi.