PROGETTO MIUR LAUREE SCIENTIFICHE

Facoltà di Scienze MFN-Università degli Studi di Torino

UNA INTRODUZIONE ALL'ALGEBRA MODERNA

Le idee e i metodi della Teoria di Galois

Giorgio Ferrarese - Margherita Roggero

UTTO QUELLO CHE AVRESTE VOLUTO SAPERE SULLE EQUAZIONI

e non avete mai osato chiedere...

Indice

Introduzione

Lo scopo di queste pagine è presentare una dimostrazione il più possibile semplice e completa della non risolubilità per radicali dell'equazione quintica, risultato come ben noto dovuto ai grandi matematici Ruffini (1765-1822) e Abel (1802-1829) e inserito poi da Galois (1811-1832) nella sua teoria generale delle equazioni.

Si tratta di uno dei risultati più significativi della matematica di tutti i tempi e certamente non mancano libri che presentano in modo rigoroso una sua dimostrazione o, d'altra parte, esposizioni a carattere divulgativo che ne illustrano a grandi linee le idee portanti. Spesso però i trattati deducono la dimostrazione come conseguenza di risultati molto più generali della Teoria dei gruppi e della Teoria delle estensioni di campi, la cui lettura integrale può risultare piuttosto pesante; all'opposto le esposizioni divulgative si limitano spesso ad una panoramica a volo d'uccello, senza entrare in alcun dettaglio tecnico e quindi senza chiarire il vero senso dei nuovi contenuti introdotti.

Noi abbiamo voluto, invece, presentare delle vere dimostrazioni, il più possibile complete ed esaurienti, ma anche comprensibili e concrete, cercando di evitare la caduta nei due tipi opposti di "generalità " ossia nell'eccesso di tecnica e astrazione o, all'opposto, nel tono discorsivo del tutto generico e superficiale.

La sollecitazione a questo lavoro ci è giunta da un gruppo di insegnanti di matematica delle scuole medie superiori, con i quali stiamo cercando il modo (se un modo ragionevole esiste) di raccontare qualcosa di questo affascinante momento della storia della conoscenza a studenti delle scuole superiori, almeno a quelli più interessati alla matematica. Queste note non sono destinate direttamente agli studenti, ma dovrebbero servire per il lavoro preparatorio agli interventi nelle classi.

La sfida è riuscire a trasmettere agli studenti almeno l'idea portante del procedimento logico che permette di dimostrare senza ombra di dubbio che non potranno mai essere trovate delle formule risolutive per le equazioni di

quinto grado. La dimostrazione che le equazioni di grado $n \leq 4$ sono risolubili per radicali è stata ottenuta nel modo più diretto possibile, ossia trovando esplicitamente le formule risolutive (e per questo ci sono voluti matematici molto in gamba e alcuni secoli di fatica). Però...

come si fa a provare che per $n \geq 5$ le formule risolutive non esistono?

L'idea è quella di individuare una qualche proprietà valida per le equazioni che ammettono formule risolutive e non valida per le altre. Ma non una proprietà qualsiasi. Deve essere controllabile in modo concreto e operativo; ci serve cioè una specie di "test diagnostico" che permette di stabilire se vale oppure no per una data equazione.

L'aspetto più affascinante della teoria di Galois non sta tanto nell'aver effettivamente individuato una proprietà siffatta, quanto nell'averla trovata in un campo della matematica che a prima vista sembra lontanissimo dalla teoria delle equazioni: quello dei GRUPPI DI SIMMETRIE o GRUPPI DI PERMUTAZIONI.

Ai gruppi di permutazioni è appunto dedicata la prima parte di questa esposizione. Nella seconda ci si propone il non facile compito di mostrare quale sia il collegamento tra simmetrie ed equazioni. Questa è senza dubbio la parte più difficile, ma speriamo che alla fine il collegamento appaia chiaro (e magari più naturale di quanto ci si sarebbe aspettati). Il punto di arrivo è la definizione del GRUPPO DI GALOIS di una equazione.

Nell'ultimo capitolo calcoliamo il gruppo di Galois di una equazione risolubile per radicali e poi quello di una particolare equazione quintica, mostrando come solo il primo possieda la proprietà di essere un GRUPPO RISOLUBILE (un nome un programma!). In questa esposizione abbiamo voluto adoperare la definizione originale di gruppo risolubile, quella che si può sostanzialmente far risalire a Galois stesso, che cosidera gruppi quoziente con un numero primo di elementi e non quella posteriore del tutto equivalente, presentata nella maggior parte dei trattati attuali, che utilizza la nozione di gruppo quoziente abeliano.

La nostra esposizione si conclude con la dimostrazione che:

se una equazione è risolubile per radicali, allora il suo gruppo di Galois è risolubile.

In realtà si può dimostrare anche il viceversa e quindi, poichè il gruppo di Galois di una equazione di grado n ha un numero finito di elementi ($\leq n!$), un numero finito di calcoli permette di stabilire se è risolubile o meno.

Per non interrompere e non appesantire la linea del ragionamento abbiamo evitato di inserire di volta in volta richiami alle nozioni di base più semplici

e probabilmente ben presenti al lettore. Per completezza le abbiamo però inserite in un'appendice. Non è indispensabile iniziare la lettura da lì, ma può essere utile, soprattutto per richiamare alla memoria le nozioni di base sui gruppi utilizzate nella trattazione.

Il gruppo simmetrico S_n

Permutazioni e loro composizione

Si dice permutazione di un qualsiasi insieme X una biezione di X in sé. L'insieme S_X di tutte le permutazioni di X è un gruppo rispetto alla composizione di funzioni. L'identità del gruppo è la funzione identica, quella che associa ad ogni elemento se stesso; l'inverso di una permutazione è la funzione inversa (biunivoca anch'essa). Se X ha più di 2 elementi, S_X non è un gruppo ABELIANO ossia vi sono permutazioni la cui composizione cambia a seconda dell'ordine con cui vengono composte.

In caso X sia l'insieme $I_n = \{1, 2, \ldots, n\}$, il gruppo delle permutazioni è detto GRUPPO SIMMETRICO DI ORDINE n e la sua notazione usuale è S_n.

L'ordine (ossia il numero degli elementi) di tale gruppo è $n!$.
Per rappresentare una permutazione σ di S_n spesso si usa una tabella che ha la forma di una matrice $2 \times n$: nella prima riga si scrivono tutti i numeri da 1 a n in un ordine qualsiasi (ad esempio in ordine crescente) mentre nella seconda si scrivono ordinatamente le immagini di ciascun numero della prima riga:

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$$

Si noti che i numeri in ciascuna riga sono scritti una e una sola volta, poiché la permutazione è una biezione. Osserviamo inoltre che σ è data dalle colonne di questa matrice, mentre l'ordine con cui si scrivono le colonne una dopo l'altra è un fatto non essenziale.

Esempio 1. *Una permutazione di S_6 è :*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 6 & 1 & 5 \end{pmatrix}$$

L'elemento neutro del gruppo S_n è la permutazione identica

$$e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$$

L'inverso di una permutazione σ è la permutazione che si ottiene scambiando tra loro le righe di σ (volendo si possono poi riordinare le colonne in modo che i numeri della prima riga siano in ordine crescente).

Ad esempio l'inverso della permutazione σ di prima è:

$$\sigma^{-1} = \begin{pmatrix} 2 & 4 & 3 & 6 & 1 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 3 & 2 & 6 & 4 \end{pmatrix}$$

Il prodotto tra due permutazioni, avviene da destra a sinistra secondo l'abitudine per la composizione di funzioni. Inoltre, come per la composizione di funzioni, in generale il risultato dipende dall'ordine dei fattori.

Esempio 2. *In S_3 consideriamo le due permutazioni:*

$$\rho = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad e \quad \theta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

I loro prodotti sono:

$$\rho\theta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad e \quad \theta\rho = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Nel prodotto $\rho\theta$ si applica prima θ e dopo la ρ: $(\rho\theta)(1) = \rho(\theta(1)) = \rho(2) = 1$, ecc.. Nel prodotto $\theta\rho$ si applica prima ρ e dopo la θ: $(\theta\rho)(1) = \theta(\rho(1)) = \theta(3) = 3$, ecc.

Decomposizione in cicli

Tra le permutazioni ve ne sono alcune particolarmente importanti, i CICLI. Dati $a_1, \dots, a_k \in I$, distinti, si indica con $(a_1\ a_2\ \dots\ a_k)$ la permutazione che manda a_i in a_{i+1} e a_k in a_1 e lascia invariati gli altri elementi. Tale permutazione è detta ciclo di lunghezza k o k-ciclo. Un ciclo di lunghezza 2 viene detto TRASPOSIZIONE o SCAMBIO.

Esempio 3. *La permutazione σ dell'Esempio 1 è un 5-ciclo in S_6:*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 6 & 1 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 & 6 & 5 \end{pmatrix} = \begin{pmatrix} 2 & 4 & 6 & 5 & 1 \end{pmatrix} = \dots$$

Due cicli sono DISGIUNTI se lo sono gli insiemi degli elementi da loro permutati.

Ogni permutazione può essere ottenuta come composizione di cicli; presentiamo due modi diversi, egualmente importanti, di decomposizione in cicli.

Teorema 4. *Sia σ una permutazione di S_n. Allora:*

1. *(**Decomposizione in cicli disgiunti**) $\sigma = \gamma_1 \cdots \gamma_s$ con γ_i cicli due a due disgiunti. Tale scrittura è unica a meno dell'ordine dei fattori.*

2. *(**Decomposizione in scambi**) $\sigma = \tau_1 \cdots \tau_s$ dove le τ_i sono trasposizioni. Tale scrittura non è unica, ma la parità di s dipende solo da σ. È inoltre possibile scegliere tutte le trasposizioni τ_i del tipo $(1\ h)$.*

Dimostrazione. Prima di tutto osserviamo che il prodotto di cicli disgiunti non dipende dall'ordine dei fattori e quindi l'ordine delle γ_i non conta; conta invece l'ordine degli scambi τ_i.

In entrambi i casi, proviamo l'esistenza delle decomposizioni in cicli, fornendo un metodo algoritmico effettivo per ottenerle.

1) Consideriamo il più piccolo i tale che $\sigma(i) \neq i$ e consideriamo il ciclo $(i\ \sigma(i)\ \sigma(\sigma(i))\ \cdots)$ che si chiude non appena si ritrova i stesso, dopo un numero di passaggi che è necessariamente minore o uguale di n. Se nel ciclo compaiono tutti gli elementi che in σ si spostano (cioè tali che $\sigma(j) \neq j$), ci fermiamo perché σ coincide col ciclo così ottenuto. In caso contrario, consideriamo il minimo j che viene spostato da σ e che non compare nel ciclo precedente e ripetiamo il procedimento, fino ad esaurire gli elementi di I_n spostati da σ. La permutazione σ è ovviamente il prodotto dei cicli costruiti (l'ordine non conta perché tali cicli sono disgiunti).

2) Una dimostrazione concreta e convincente dell'esistenza di una decomposizione in trasposizioni è quella di provare a riordinare n oggetti diversi (ad esempio carte di un mazzo di carte da gioco) posti gli uni accanto agli altri, eseguendo solo una sequenza opportuna di scambi di posto tra due carte alla volta. Usare la trasposizione $(1\ h)$ vuol dire scambiare tra loro la carta al primo posto e la carta all'h-esimo posto. È facile convincersi che è sempre possibile riordinare le carte in un modo predefinito a partire da una qualsiasi disposizione di esse e non è difficile neppure formalizzare in modo esplicito una procedura generale.
Quella che segue è una delle tante possibili e utilizza quanto provato al punto precedente.

Osserviamo che $(a_1\ a_2\ \dots\ a_k) = (a_1\ a_k)(a_1\ a_{k-1})...(a_1\ a_2)$ e quindi possiamo scrivere ogni ciclo come prodotto di trasposizioni. Grazie alla decomposizione in cicli disgiunti, possiamo allora scrivere ogni permutazione come prodotti di trasposizioni.

Notiamo che si potrebbero utilizzare anche soltanto trasposizioni del tipo $(1\ k)$, poiché $(h\ k) = (1\ k)(1\ h)(1\ k)$.

Un po' più difficile è verificare che la parità del numero di fattori in ogni decomposizione in scambi di σ è costante. Se una permutazione σ si può scrivere come prodotto di r scambi, possiamo ottenere un'altra scrittura di σ costituita da $r + 2r'$ scambi del tipo $(1\,k)$ mediante le sostituzioni del tipo precedente; poiché la parità di r e di $r + 2r'$ è la stessa, ci basterà provare che tutte le decomposizioni di σ in scambi del tipo $(1\,k)$ hanno la stessa parità.

Sia $P = P(n)$ il numero intero:

$$P = \prod_{1\le i<j\le n} (i - j) = (1 - 2)(1 - 3)\cdots(n - 1 - n)$$

Operando su $I_n = \{1, 2, \dots, n\}$ con una permutazione σ il corrispondente prodotto

$$\sigma(P) = \prod_{1\le i<j\le n} (\sigma(i) - \sigma(j))$$

coincide con P, tranne al più per il segno, in quanto $|P|$ e $|\sigma(P)|$ sono entrambi il prodotto dei fattori $|(i - j)|$ con $i, j \in I_n$, $i \neq j$..

Vediamo con quale segno compare ciascun fattore $(i - j)$ in $\tau(P)$ se τ è la trasposizione $(1\ k)$.

1. I fattori che non contengono né 1 né k non cambiano.
2. Il fattore $(1 - k)$ diventa $(k - 1)$: *c'è un cambio di segno.*
3. Se $1 < j < k$, i fattori $(1 - j)$ e $(j - k)$ diventano rispettivamente $(k - j)$ e $(j - 1)$ con 2 cambi di segno: il segno complessivamente non cambia.
4. Se $k < j$, i fattori $(1 - j)$ e $(k - j)$ diventano rispettivamente $(k - j)$ e $(1 - j)$: il segno complessivamente non cambia.

Quindi, la trasposizione τ muta il prodotto P in $\tau(P) = -P$. Così se $\sigma(P) = P$, σ può essere decomposta solo in un numero pari di trasposizioni, se invece $\sigma(P) = -P$, σ può essere decomposta solo in un numero dispari di trasposizioni. ∎

Il risultato seguente sarà uno dei punti chiave per provare la non risolubilità dell'equazione di quinto grado.

Proposizione 5. *Se H è un sottogruppo di S_5 che contiene un 5-ciclo e uno scambio, allora $H = S_5$.*

Dimostrazione. A meno di un cambio di nomi, si può supporre che lo scambio sia $\tau = (1\ 2)$. Componendo con se stesso il 5-ciclo un numero opportuno di volte (al massimo 4 volte) si trova un 5-ciclo σ in cui $\sigma(1) = 2$. Cambiando se necessario i nomi agli altri indici si può supporre che σ sia $(1\ 2\ 3\ 4\ 5)$. Proviamo che con questi si ottengono tutte le permutazioni.
Si ha:

$$\tau = (1\ 2)$$

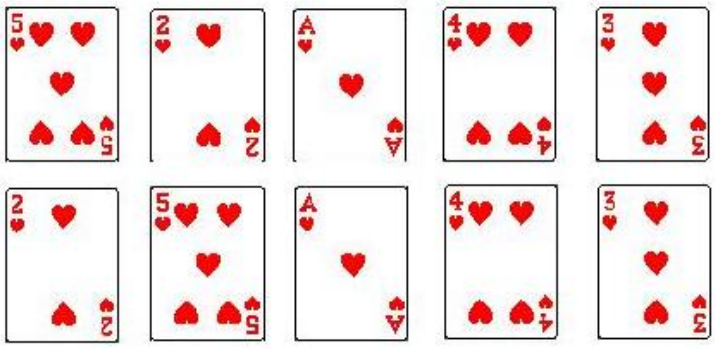
$$\tau\sigma\tau\sigma^{-1}\tau = (1\ 3)$$

$$\sigma^{-1}\tau\sigma^{-1}\tau\sigma\tau\sigma = (1\ 4)$$

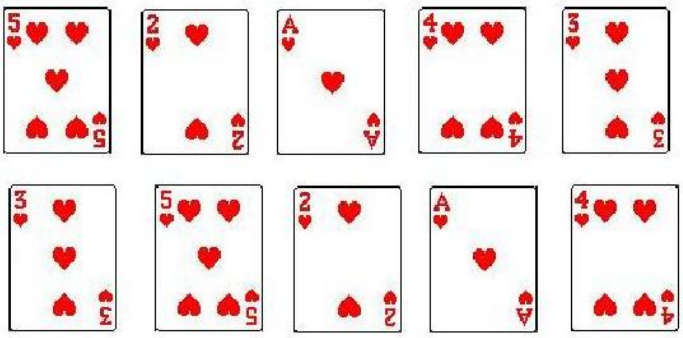
$$\sigma^{-1}\tau\sigma = (1\ 5)$$

Poiché si possono ottenere tutti gli scambi $(1\ k)$ il teorema 4 ci permette di concludere. ∎

Anche in questo caso ci si può convincere direttamente del risultato (e magari trovare una diversa dimostrazione) provando a riordinare in un modo prefissato 5 carte da gioco, mediante una sequenza di operazioni ciascuna delle quali può essere solo lo scambio delle prime due



oppure uno slittamento circolare in avanti (ogni carta si sposta nella posizione successiva, mentre l'ultima passa al primo posto).



IL GRUPPO ALTERNO A_n

Una permutazione è detta PARI oppure DISPARI a seconda che il numero di trasposizioni in cui si decompone sia pari oppure dispari. Le trasposizioni sono ovviamente dispari. Invece i 3-cicli sono pari:

$$(a_1\, a_2\, a_3) = (a_1\, a_3)(a_1\, a_2).$$

L'insieme delle permutazioni pari è un gruppo: il GRUPPO ALTERNO A_n.

Infatti, il prodotto di permutazioni pari è ancora, ovviamente, una permutazione pari, l'identità è pari e l'inversa di una permutazioni pari è pari.

Possiamo inoltre osservare che il prodotto di una permutazione dispari per una pari è dispari e quindi ci sono tante permutazioni pari quante dispari. Questa semplice osservazione prova che il gruppo alterno A_n ha $\frac{n!}{2}$ elementi e quindi che A_n *è normale in* S_n (cfr. Esempio 27 in Appendice).

Abbiamo detto che i 3-cicli sono permutazioni pari così come lo sono i "doppi scambi disgiunti" ossia quelli del tipo $(1\,2)(3\,4)$ oppure i 5-cicli e tanti altri. Proviamo una proprietà importante relativa ai 3-cicli e ai doppi scambi disgiunti che dice che non esistono sottogruppi propri di A_n che contengano tutti i 3-cicli e neppure sottogruppi propri che contengano tutti i doppi scambi disgiunti.

Proposizione 6. ***1)*** *Il gruppo alterno A_n è generato dai 3-cicli ossia ogni elemento di A_n è prodotto di 3-cicli.*

2) *Se $n \geq 5$, il gruppo alterno A_n è generato dai doppi scambi disgiunti ossia ogni elemento di A_n è prodotto di doppi scambi disgiunti.*

Dimostrazione. Preso un elemento $\sigma \in A_n$ lo possiamo scrivere come prodotto di un numero pari di trasposizioni. Raggruppiamo due a due tali trasposizioni. Proviamo che il prodotto di ogni coppia di trasposizioni può essere sostituito dal prodotto di 3-cicli e analogamente (quando $n \geq 5$) può essere sostituito dal prodotto di doppi scambi disgiunti.

- Se le due trasposizioni coincidono, si ottiene la permutazione identica e e le due trasposizioni si possono cancellare dalla scrittura di σ.
- Se le due trasposizioni sono disgiunte, ossia sono del tipo $(a\ b)(c\ d)$ con a, b, c, d tutti distinti, allora $(a\ b)(c\ d) = (a\ b\ c)(b\ c\ d)$.
- Se infine le due trasposizioni hanno un simbolo in comune, ossia sono del tipo $(a\ b)(b\ c)$, allora si ha $(a\ b)(b\ c) = (a\ b\ c)$ e si ha anche $(a\ b)(b\ c) = (a\ b)(d\ e)(b\ c)(d\ e)$: si noti che in quest'ultimo caso abbiamo usato 5 elementi distinti tra gli n e quindi è necessaria l'ipotesi $n \geq 5$.

■

Proviamo ora una caratteristica importante del gruppo alterno A_5, il fatto che non sia risolubile.

Un gruppo G si dice RISOLUBILE se è possibile trovare una catena finita di sottogruppi G_i

$$G = G_0 \supset G_1 \supset G_2 \supset ... \supset G_s = \{e\}$$

tale che ogni G_i è normale in G_{i-1} e ogni quoziente G_{i-1}/G_i ha ordine primo (ossia ha un numero primo di elementi).

Già la terminologia ci suggerisce che deve esserci uno stretto legame tra questa nozione e la risolubilità o meno di una equazione, legame che sarà oggetto dell'ultimo capitolo.

La definzione di gruppo risolubile che presentiamo è sostanzialmente quella adoperata da Galois nella sua dimostrazione originale. In seguito è stata sostituita da una formulazione un po' diversa che richiede che i quozienti G_{i-1}/G_i siano abeliani. Le due definizioni sono però equivalenti: se infatti G_{i-1}/G_i ha ordine primo, allora è sicuramente abeliano (cfr Corollario 25 in Appendice), mentre se G_{i-1}/G_i è abeliano, la catena può essere "raffinata" aggiungendo se necessario altri sottogruppi normali intermedi fino ad ottenerne una con quozienti di ordine primo.

Esempio 7. *I gruppi S_3 e S_4 sono risolubili. Infatti:*

$$S_3 \supset A_3 \supset \{e\}$$

$$S_4 \supset A_4 \supset V \supset W \supset \{e\}$$

dove $V = \{e, (1\ 2\ )(3\ 4\ ), (1\ 3\ )(2\ 4\ ), (1\ 4\ )(2\ 3\ )\}$ *e* $W = \{e, (1\ 2\ )(3\ 4\ )\}$. *La verifica che i sottogruppi sono normali e che i quozienti hanno ordine primo si ottiene immediatamente con semplici conteggi del numero di elementi (cfr. Proposizione 22 ed Esempio 27 in Appendice). L'unica verifica da fare direttamente è che* V *è normale in* A_4.

Invece:

Proposizione 8. *A_5 non è risolubile.*

Dimostrazione. Sia N un qualsiasi sottogruppo normale di A_5 (proprio ossia $N \neq A_5$); proviamo che A_5/N non può avere ordine primo.

Grazie alla Proposizione 6 sappiamo di poter trovare al di fuori di N sia un 3-ciclo σ sia un doppio scambio disgiunto τ. Dunque A_5/N possiede sia un elemento di periodo 3 (poiché né σ né σ^2 appartengono a N, mentre $\sigma^3 = e \in N$) sia un elemento di periodo 2 (poiché $\tau^2 = e \in N$). Allora grazie al Teorema di Lagrange (cfr. Teorema 21 in Appendice) possiamo dire che A_5/N ha un numero di elementi multiplo di 6 e quindi non primo. ∎

Corollario 9. *Il gruppo simmetrico S_5 non è risolubile.*

Dimostrazione. Sia H un sottogruppo normale di S_5 tale che S_5/H ha ordine primo p. Allora $H' = H \cap A_5$ è un sottogruppo normale di A_5 e A_5/H' è un sottogruppo di S_5/H: dunque l'ordine di A_5/H' divide p, cioè è p oppure 1. Grazie al risultato precedente sappiamo che A_5 non ha sottogruppi normali con quoziente di ordine primo e quindi H' deve coincidere con A_5 stesso. Di conseguenza H contiene tutto A_5 ed ha quindi un numero di elementi multipo di quello di A_5; poiché l'ordine di S_5 è doppio di quello di A_5, non rimane che $H = A_5$.

L'unico sottogruppo normale di S_5 con quoziente di ordine primo è dunque A_5 stesso e, per quanto prima dimostrato, la catena $S_5 \supset A_5$ non è ulteriormente prolungabile. ∎

Osservazione 10. A_5 è isomorfo al gruppo delle simmetrie rotazionali del dodecaedro e dell'icosaedro. Ciò indica la strada per collegamenti del tutto inaspettati tra la geometria dello spazio tridimensionale e l'algebra delle equazioni, come magistralmente esposto da F. Klein in [5].

Equazioni e campi

Radici di polinomi

In questo capitolo vedremo come le equazioni e le permutazioni siano collegate tra loro, ossia come ad una equazione di grado n si può associare un particolare sottogruppo di S_n, il gruppo di Galois.

Nel successivo e ultimo capitolo introdurremo l'esempio più importante, quello di una quintica non risolubile per radicali. Mostreremo infatti che il suo gruppo di Galois è tutto S_5 (che è un gruppo non risolubile) e concluderemo provando che la non risolubilità del gruppo di Galois di una equazione equivale proprio alla non risolubilità dell'equazione stessa.

Se $a_1,\ a_2, \ldots, a_n$ sono elementi di un campo F, una equazione nell'incognita x del tipo

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_{n-1} x + a_n = 0$$

si dice EQUAZIONE ALGEBRICA o POLINOMIALE a coefficienti in F di grado n. L'insieme $F[x]$ dei polinomi nella variabile x a coefficienti nel campo F con le operazioni usuali di somma e prodotto è un anello. Una proprietà importante dell'anello dei polinomi $F[x]$ a coefficienti in un campo è l'esistenza della DIVISIONE COL RESTO :

dati $p(x)$ e $b(x) \neq 0$ esistono e sono unici $q(x)$ e $r(x)$ tali che

$p(x) = b(x)q(x) + r(x)$ con $r(x)$ di grado inferiore a $b(x)$ oppure nullo.

Ad ogni polinomio $p(x)$ di $F[x]$ di grado $n = \partial p(x) > 0$, corrisponde l'equazione algebrica $p(x) = 0$, che possiamo sempre trasformare in una del tipo precedente moltiplicando $p(x)$ per l'inverso del suo coefficiente di grado massimo.

Diremo RADICE DEL POLINOMIO $p(x)$ ogni soluzione dell'equazione $p(x) = 0$ ossia ogni valore α per cui $p(\alpha) = 0$. Osserviamo che α può essere un elemento

di F oppure, più generalmente, di un campo K estensione di F. I campi di cui ci occuperemo (che chiameremo di volta in volta F, K, k, ecc.) saranno soltanto il campo $\mathbb{C}$ dei numeri complessi e suoi sottocampi: ricordiamo che ogni sottocampo di $\mathbb{C}$ contiene il campo dei numeri razionali $\mathbb{Q}$.

Uno dei più importanti risultati relativi alle radici dei polinomi è il seguente, che riportiamo senza dimostrazione.

Teorema 11 (Teorema fondamentale dell'algebra)**.** *Ogni polinomio con coefficienti complessi di grado n ($n > 0$) ha almeno una radice nel campo dei numeri complessi.*

Si dice che un polinomio $p(x) \in F[x]$ di grado $n > 0$ è RIDUCIBILE in $F[x]$ (oppure su F) se si può spezzare nel prodotto di due polinomi di $F[x]$ ciascuno con grado inferiore a n ma ≥ 1. Se ciò non è possibile, il polinomio si dice IRRIDUCIBILE in $F[x]$ (o su F). La terminologia precedente non si applica al polinomio nullo e, più in generale, ai polinomi costanti (ossia di grado 0).

Un polinomio può risultare irriducibile su un campo F e riducibile su un campo più grande K. Sono poi riducibili su un certo campo F tutti i polinomi di grado ≥ 2 che hanno una radice in F, come mostra il seguente risultato.

Teorema 12 (Ruffini)**.** *Siano $p(x) \in F[x]$ e $\alpha \in F$. Allora:*

$$\alpha \text{ è radice di } p(x) \iff (x-\alpha) \text{ divide } p(x).$$

Dimostrazione. Eseguiamo la divisione di $p(x)$ per $(x-\alpha)$:

$$p(x) = (x-a)q(x) + r(x) \quad \text{con } \partial r(x) < \partial(x-a) = 1 \text{ e quindi } r(x) = r \in F.$$

Valutiamo quest'espressione in α:

$$0 = p(\alpha) = (\alpha - \alpha)q(\alpha) + r \Rightarrow r = 0.$$

Allora $p(x) = (x-\alpha)q(x)$ è divisibile per $(x-\alpha)$. ∎

Grazie al teorema di Ruffini possiamo concludere che ogni polinomio $p(x)$ di $\mathbb{C}[x]$ di grado n ha esatteamete n radici complesse (eventualmente coincidenti) e si fattorizza in $\mathbb{C}[x]$ in fattori lineari. Infatti $p(x)$ ha una radice α e quindi si fattorizza in $(x-\alpha)q(x)$, con $\partial q(x) = n-1$. Se $n > 1$, allora anche $q(x)$ ha almeno una radice β che è anche radice di $p(x)$. Si ottiene quindi una nuova fattorizzazione $p(x) = (x-\alpha)(x-\beta)g(x)$ e così via.

Il teorema fondamentale dell'algebra è però un risultato puramente esistenziale, ossia non fornisce alcun metodo operativo che permetta di trovare le radici e quindi di fattorizzare esplicitamente un polinomio.

Anche nel caso di polinomi a coefficienti reali per trovare tutte le radici, ossia un numero di radici pari al grado, è necessario usare i numeri complessi non reali. L'unica informazione ulteriore riguarda il numero delle soluzioni reali e la forma di quelle non reali:

Teorema 13. *Se $p(x) \in \mathbb{R}[x]$, il numero di radici reali ha la stessa parità di $\partial p(x)$ e le radici non reali si presentano a coppie complesse coniugate.*

Il polinomio $p(x)$ si decompone allora in $\mathbb{R}[x]$ nel prodotto di fattori di grado 1, corrispondenti alle radici reali, e di fattori di grado 2 con discriminante negativo, corrispondenti alle coppie di radici complesse coniugate.

Dimostrazione. Presentiamo in modo esplicito la dimostrazione di questo risultato perché lo strumento essenziale su cui si basa giocherà nel seguito un ruolo centrale. Si tratta del CONIUGIO, ossia dell'isomorfismo di campi:

$$\chi\colon \mathbb{C} \to \mathbb{C} \text{ data da } z = a + ib \mapsto \overline{z} = a - ib$$

Gli elementi uniti secondo il coniugio, ossia quelli che sono i coniugati di se stessi, sono i numeri reali.

Possiamo estendere il coniugio all'anello dei polinomi:

$$\chi\colon \mathbb{C}[x] \to \mathbb{C}[x]$$

associando ad un polinomio $p(x)$ il polinomio che ha come coefficienti i coniugati dei coefficienti di $p(x)$. Anche in questo caso rimangono invariati i soli polinomi di $\mathbb{R}[x]$.

Se $p(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in \mathbb{R}[x]$ e α è una sua radice complessa non reale, allora $p(\alpha) = 0$ ossia $\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0$. Quindi si ha anche

$$\overline{\alpha^n + a_1\alpha^{n-1} + \cdots + a_{n-1}x + a_n} = \overline{\alpha}^n + a_1\overline{\alpha}^{n-1} + \cdots + a_{n-1}\overline{\alpha} + a_n = 0$$

ossia $p(\overline{\alpha}) = 0$ e $\overline{\alpha}$ è un'altra radice di $p(x)$.

Il polinomio $p(x)$ ha allora i due fattori $(x - \alpha)$ e $(x - \overline{\alpha})$ il cui prodotto è un polinomio di 2° grado a coefficienti reali e discriminante negativo $x^2 - 2ax + a^2 + b^2$, dove $\alpha = a + ib$. ∎

L POLINOMIO MINIMO

Se F è un sottocampo di $\mathbb{C}$ e $\alpha \in \mathbb{C}$, possiamo considerare il più piccolo sottocampo di $\mathbb{C}$ che contiene entrambi sia F sia α: lo indicheremo con $F(\alpha)$.

È facile convincersi che $F(\alpha)$ è costituito da tutte le espressioni del tipo $\frac{g(\alpha)}{h(\alpha)}$,

con $g(x), h(x) \in F[x]$ e $h(\alpha) \neq 0$. Infatti tutte queste espressioni devono appartenere ad un campo che contenga sia F sia α e, d'altra parte, esse costituiscono già da sole un campo.

Un numero complesso α si dice ALGEBRICO se è radice di un polinomio a coefficienti in $\mathbb{Q}$. Più in generale si dice algebrico su un campo F se è radice di un polinomio a coefficienti in F.

Se α è algebrico su F, vi sono molti polinomi a coefficienti in F di cui α è radice; tra essi ve ne è uno soltanto che è di grado minimo e monico (ossia con coefficiente direttivo 1). Se infatti vi fossero due diversi polinomi siffatti, allora anche il loro MCD avrebbe α come radice, ma grado inferiore. Tale polinomio si chiama il POLINOMIO MINIMO di α su F. Ogni altro polinomio di $F[x]$ che si annulla in α è un suo multiplo.

Il polinomio minimo di α su F è necessariamente un polinomio irriducibile su F: in caso contrario α sarebbe radice anche di uno dei suoi fattori, che ha, per definizione, grado inferiore. Inoltre, essendo irriducibile, tutte le sue radici sono semplici (cfr. Proposizione 30 in Appendice).

D'altra parte, ogni polinomio irriducibile $p(x)$ di $F[x]$ è il polinomio minimo su F di ogni sua radice complessa.

Il campo di spezzamento

Dato un polinomio $p(x) \in \mathbb{C}[x]$, può essere utile considerarlo come polinomio a coefficienti nel campo più piccolo possibile, ossia nel campo F che contiene $\mathbb{Q}$ e tutti i coefficienti di $p(x)$. La notazione algebrica per tale campo è $F = \mathbb{Q}(a_1, a_2, \ldots, a_n)$, poiché F si ottiene proprio considerando tutti gli elementi di $\mathbb{C}$ che si possono scrivere a partire dalle espressioni razionali fratte del tipo:

$$\frac{P(X_1, \ldots, X_n)}{Q(X_1, \ldots, X_n)}.$$

a coefficienti in $\mathbb{Q}$, sostituendo $a_1, \ldots, a_n$ alle variabili. Si devono però escludere tutti quei denominatori $Q(X_1, \ldots, X_n)$ tali che $Q(a_1, \ldots, a_n) = 0$.

Osserviamo che si ottiene lo stesso campo anche aggiungendo un coefficiente alla volta ossia come $F_1 = \mathbb{Q}(a_1)$, $F_2 = F_1(a_2)$, $\ldots$, $F = F_{n-1}(a_n)$.

In quest'ottica si inserisce anche la seguente definizione, che riguarda in sostanza il più piccolo campo su cui un dato polinomio si spezza nel prodotto di fattori lineari.

Definizione 14. Sia $p(x) \in F[x]$ e siano $\alpha_1, \alpha_2, \ldots, \alpha_n$ tutte le radici complesse di $p(x)$. Il minimo sottocampo K di $\mathbb{C}$ che contiene sia i coefficienti di $p(x)$, sia le sue radici si chiama CAMPO DI SPEZZAMENTO di $p(x)$. Se F è il minimo campo su cui $p(x)$ è definito, il suo campo di spezzamento è $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

OMOMORFISMI E PERMUTAZIONI

Possiamo a questo punto concretizzare una delle idee centrali del ragionamento: il collegamento tra omomorfismi di campi e permutazioni di radici (per le generalità sugli omomorfismi si veda l'Appendice).

Diremo che un omomorfismo di campi $\phi\colon H \to \mathbb{C}$ fissa il sottocampo F di H se $\phi(a) = a$ per ogni $a \in F$.

Teorema 15. *Siano $F \subset H \subset \mathbb{C}$ campi e sia $\alpha \in H$ un elemento algebrico su F con polinomio minimo $p(x) \in F[x]$.*

i) *Se $\phi\colon H \to \mathbb{C}$ è un omomorfismo che fissa F, anche $\gamma = \phi(\alpha)$ è radice di $p(x)$.*

ii) *Per ogni altra radice $\beta \in H$ di $p(x)$ vi è un unico omomorfismo di campi $\phi\colon F(\alpha) \to H$ che fissa F e tale che $\phi(\alpha) = \beta$.*

iii) *Se K è il campo di spezzamento di $p(x)$ su F e H un suo sottocampo, allora ogni omomorfismo $\phi : H \to K$ che fissa F si estende (non necessariamente in modo unico) ad un isomorfismo $\psi\colon K \to K$.*

Dimostrazione. i) Se $p(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ allora

$$\phi(\alpha^n + a_1\alpha^{n-1} + \cdots + a_{n-1}\alpha + a_n) = \phi(0) = 0$$

poiché ϕ è un omomorfismo di campi. Per lo stesso motivo il primo membro si può anche scrivere come

$$\phi(\alpha)^n + a_1\phi(\alpha) + \cdots + a_{n-1}\phi(\alpha) + a_n = 0.$$

Allora $\gamma^n + a_1\gamma^{n-1} + \cdots + a_{n-1}\gamma + a_n = 0$, ossia anche γ è radice di $p(x)$.

ii) Ricordiamo che ogni elemento di $F(\alpha)$ si ottiene a partire da una funzione razionale $\frac{g(x)}{h(x)}$ sostituendo α al posto di x, purché $h(\alpha) \neq 0$ ossia $h(x)$ non sia multiplo di $p(x)$.

L'omomorfismo ϕ si ottiene allora associando a ogni elemento siffatto quello che si ottiene sostituendo β alla x. Poiché α e β hanno lo stesso polinomio minimo, la condizione $h(\alpha) \neq 0$ equivale esattamente alla condizione $h(\beta) \neq 0$.

iii) Per definire ψ è sufficiente assegnare l'immagine ad ogni radice di $p(x)$ non contenuta in H. Sia α una di queste radici e sia $q(x)$ il suo polinomio minimo su H. Se $q(x) = \sum b_i x^i$, il polinomio $\overline{q(x)} = \sum \phi(b_i) x^i$ è un polinomio irriducibile a coefficienti nel campo $\phi(H)$ isomorfo ad H. Possiamo allora estendere ϕ a $H(\alpha)$ scegliendo come $\psi(\alpha)$ una qualsiasi delle radici di $\overline{q(x)}$ in K. Si noti che $q(x)$ è un fattore su H di $p(x)$ e quindi $\overline{q(x)}$ è un fattore su $\phi(H)$ di $\sum \phi(a_i) x^i = \sum a_i x^i = p(x)$; allora le radici di $\overline{q(x)}$ sono anche radici di $p(x)$ e appartengono sicuramente a K. ∎

In altre parole ogni omomorfismo $\phi\colon H \to \mathbb{C}$ che fissa F, essendo iniettivo perchè omomorfismo tra campi, non può far altro che permutare tra loro quegli elementi di H che sono radici di uno stesso polinomio irriducibile su F.

Non è detto, però, che in questo modo si realizzino tutte le possibili permutazioni tra le radici di un polinomio; in genere se ne possono ottenere solo alcune, che chiameremo PERMUTAZIONI AMMISSIBILI. Concretamente le permutazioni ammissibili sono quelle che rispettano tutte le possibili relazioni tra le radici che sono esprimibili mediante polinomi a coefficienti in F.

A parità di campo H, più è grande il campo fissato F, più relazioni polinomiali tra le radici si potranno costruire e quindi minore sarà il numero delle permutazioni ammissibili.

La corrispondenza così introdotta è particolarmente interessante quando il campo H è il campo di spezzamento K di un polinomio $p(x)$. Poichè tutte le radici di $p(x)$ appartengono a K, un omomorfismo $\phi\colon K \to \mathbb{C}$ che fissa F trasforma elementi di K in elementi che appartengono ancora a K ossia individua un isomorfismo del campo K in sé.

Ogni isomorfismo $\phi\colon K \to K$ che fissa F è individuato e individua una permutazione ammissibile tra le radici di $p(x)$; la composizione di due isomorfismi siffatti corrisponde alla composizione delle due permutazioni e l'isomorfismo inverso corrisponde alla permutazione inversa.

Dunque le permutazioni ammissibili formano un sottogruppo di S_n detto GRUPPO DI GALOIS di $p(x)$ su F.

A seconda dei casi e della convenienza, potremo pensare indifferentemente il gruppo di Galois sul campo F di una equazione $p(x)$ come costituito da

permutazioni tra le radici di $p(x)$, ammissibili su F, oppure come costituito da isomorfsmi del campo di spezzamento K di $p(x)$ che fissano F.

Questo seconda variante della definizione di gruppo di Galois ha il vantaggio di poter essere immediatamente estesa ad ogni campo E estensione del campo base F; si può infatti definire il gruppo di Galois $\Gamma_F(E)$ di E sopra F come il gruppo degli isomorfismi di E che fissano F.

In particolare sarà comodo considerare invece del campo di spezzamento K di una equazione (che può essere molto difficile da trovare) un campo più ampio E: vedremo che se $\Gamma_F(E)$ è risolubile, anche $\Gamma_F(K)$ lo è.

Il cerchio si chiude

n esempio per capire

L'esempio seguente dovrebbe permettere di capire molto concretamente il ruolo dei vari strumenti fino ad ora introdotti.

Esempio 16. *Consideriamo il polinomio* $p(x) = x^4 - 2 \in \mathbb{Q}[x]$ *irriducibile su* $\mathbb{Q}$ *(cfr. Criterio di Eisenstein ed Esempio 31 in Appendice). Per il Teorema fondamentale sappiamo che ha* 4 *radici complesse* α, β, γ, δ*; possiamo controllare col metodo della derivata che sono tutte distinte (cfr. Proposizione 30 in Appendice) . Allora:*

$$p(x) = x^4 - 2 = (x-\alpha)(x-\beta)(x-\gamma)(x-\delta).$$

Eseguendo i prodotti a secondo membro e eguagliando i coefficienti otteniamo le seguenti relazioni tra le radici:

$$\begin{cases} \alpha+\beta+\gamma+\delta = 0 \\ \alpha\beta + +\alpha\gamma + \alpha\delta + \beta\gamma + \beta\delta + \gamma\delta = 0 \\ \alpha\beta\gamma + \alpha\beta\delta + \alpha\gamma\delta + \beta\gamma\delta = 0 \\ \alpha\beta\gamma\delta = -2 \end{cases}$$

Ricavando α *dalla prima relazione e sostituendo nella terza otteniamo:*

$$-(\beta+\gamma)(\beta+\delta)(\gamma+\delta) = 0.$$

Per la legge di annullamento del prodotto due delle radici sono opposte: sia $\delta = -\gamma$*. Sostituendo nella prima otteniamo che anche le altre due sono opposte:* $\beta = -\alpha$*. A questo punto possiamo indicare le* 4 *radici come:*

$$\alpha \ , \ -\alpha \ , \ \gamma \ , \ -\gamma$$

Nel sistema rimangono soltanto due relazioni: $\begin{cases} \alpha^2+\gamma^2 = 0 \\ \alpha^2\gamma^2 = -2 \end{cases}$

Queste sono le uniche relazioni tra α e γ che possiamo scrivere usando soltanto coefficienti razionali. Possiamo osservare che rimangono del tutto invariate se sostituiamo in esse α con $-\alpha$ e/o γ con $-\gamma$ o anche α con γ o con $-\gamma$ in tutti i modi possibili. Ci sono quindi 8 permutazioni tra le radici che corrispondono a isomorfismi del campo di spezzamento $K = \mathbb{Q}(\alpha, \gamma)$ che fissano $\mathbb{Q}$:

$$\mathbf{e} = \begin{pmatrix} \alpha & -\alpha & \gamma & -\gamma \\ \alpha & -\alpha & \gamma & -\gamma \end{pmatrix} \qquad \sigma_{\mathbf{2}} = \begin{pmatrix} \alpha & -\alpha & \gamma & -\gamma \\ -\alpha & \alpha & \gamma & -\gamma \end{pmatrix}$$

$$\sigma_{\mathbf{3}} = \begin{pmatrix} \alpha & -\alpha & \gamma & -\gamma \\ -\alpha & \alpha & -\gamma & \gamma \end{pmatrix} \qquad \sigma_{\mathbf{4}} = \begin{pmatrix} \alpha & -\alpha & \gamma & -\gamma \\ \alpha & -\alpha & -\gamma & \gamma \end{pmatrix}$$

$$\sigma_{\mathbf{5}} = \begin{pmatrix} \alpha & -\alpha & \gamma & -\gamma \\ \gamma & -\gamma & \alpha & -\alpha \end{pmatrix} \qquad \sigma_{\mathbf{6}} = \begin{pmatrix} \alpha & -\alpha & \gamma & -\gamma \\ -\gamma & \gamma & \alpha & -\alpha \end{pmatrix}$$

$$\sigma_{\mathbf{7}} = \begin{pmatrix} \alpha & -\alpha & \gamma & -\gamma \\ \gamma & -\gamma & -\alpha & \alpha \end{pmatrix} \qquad \sigma_{\mathbf{8}} = \begin{pmatrix} \alpha & -\alpha & \gamma & -\gamma \\ -\gamma & \gamma & -\alpha & \alpha \end{pmatrix}$$

Si ricordi il Teorema 15 iii): ciascun isomorfismo è individuato dalla scelta delle immagini delle radici, immagini che sono necessariamente radici dello stesso polinomio; in breve ciascun isomorfismo è individuato da una opportuna permutazione delle radici. Tali permutazioni costituiscono il gruppo di Galois $\Gamma_{\mathbb{Q}}(K) = G_{\mathbb{Q}}$ su $\mathbb{Q}$ del polinomio.

Osserviamo ora che $\sqrt{2} \in K$ (poiché $\alpha^2 = \pm\sqrt{2}$); possiamo ora decidere di aggiungere $\sqrt{2}$ al campo base, ottenendo $F_1 = \mathbb{Q}(\sqrt{2})$.

Su F_1 il polinomio $p(x)$ si spezza in $(x^2 - \sqrt{2})(x^2 + \sqrt{2})$ e quindi α e γ non sono più interscambiabili poiché hanno polinomi minimi diversi, pur potendo ancora scambiare tra di loro α con $-\alpha$ e rispettivamente γ e $-\gamma$. Supponiamo che α e $-\alpha$ abbiano polinomio minimo $x^2 - \sqrt{2}$ e γ e $-\gamma$ abbiano $x^2 + \sqrt{2}$. Ci sono ora meno permutazioni ammissibili, ossia corrispondenti a isomorfismi di K in $\mathbb{C}$ che fissano F_1:

$$e \ , \ \sigma_2 \ , \ \sigma_3 \ , \ \sigma_4.$$

Abbiamo individuato dunque in $G_{\mathbb{Q}}$ un sottogruppo proprio G_{F_1}.

Ora, $\sqrt[4]{2} \in K$ (poiché soluzione di $x^4 = 2$): aggiungiamo allora $\sqrt[4]{2}$ al campo base ottenendo $F_2 = F_1(\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2})$. Il fattore $x^2 - \sqrt{2}$ si spezza ulteriormente in $(x - \sqrt[4]{2})(x + \sqrt[4]{2})$ e quindi $\alpha, -\alpha \in F_2$ non possono più

essere scambiate tra loro, ma γ e $-\gamma$ sì. Rimangono due sole permutazioni ammissibili associate ad isomorfismi che fissano F_2, ossia:

$$e \ , \ \sigma_4$$

(che sono rispettivamente l'identità e il coniugio).

Individuiamo quindi un ulteriore sottogruppo $G_{F_2} \subset G_{F_1} \subset G_{\mathbb{Q}}$.

Infine, anche l'unità immaginaria i appartiene al campo K (poiché $i\sqrt[4]{2} \in K$ come soluzione di $x^4 = 2$ e quindi $(i\sqrt[4]{2})/(\sqrt[4]{2}) = i \in K$). Se aggiungiamo i otteniamo il campo $F_3 = \mathbb{Q}(\sqrt[4]{2}, i)$ in cui $p(x)$ si spezza in fattori lineari. Allora $F_3 = K$ è il campo di spezzamento di $p(x)$, le 4 radici sono gli elementi di F_2:

$$\sqrt[4]{2} \ , \ -\sqrt[4]{2} \ , \ \sqrt[4]{2}i \ \ , \ -\sqrt[4]{2}i$$

e l'unica permutazione ammissibile, ossia che fissa F_3 è l'identità e. In tal caso il sottogruppo individuato non è altro che quello banale.

Analizziamo il significato di quanto abbiamo ottenuto in questo esempio. Le soluzioni dell'equazione esaminata sono esprimibili mediante radicali e quindi l'equazione è risolubile per radicali. Abbiamo calcolato il gruppo di Galois dell'equazione trovando il gruppo $G_{\mathbb{Q}} = \{e, \sigma_2, \ldots, \sigma_8\}$ con 8 elementi sul campo di definizione $\mathbb{Q}$. Aggiungendo poi al campo base uno alla volta i radicali necessari per esprimere le soluzioni, abbiamo ottenuto gruppi di permutazioni ammissibili, sottogruppi l'uno dell'altro:

$$G_{\mathbb{Q}} \supset G_{F_1} = \{e, \sigma_2, \sigma_3, \sigma_4\} \supset G_{F_2} = \{e, \sigma_4\} \supset G_{F_3} = \{e\}.$$

Ogni quoziente ha ordine 2 e quindi $G_{\mathbb{Q}}$ è un gruppo risolubile (cfr. Esempio 27 in Appendice).

L'esempio presentato mostra quindi una equazione risolubile per radicali il cui gruppo di Galois è un gruppo risolubile e soprattutto stabilisce in modo molto esplicito come le due proprietà sono collegate.

La quintica non risolubile

Nell'esempio precedente abbiamo calcolato il gruppo di Galois di una equazione senza utilizzare direttamente le radici del polinomio, anche se in realtà eravamo in grado fin da subito di calcolare esplicitamente le radici stesse. Almeno psicologicamente questo ci ha aiutato. Ora invece lavoreremo senza rete perché del prossimo polinomio non sappiamo calcolare a

prima vista le radici. Anzi, sarà proprio il polinomio di quinto grado per il quale dimostreremo che non esistono formule risolutive per radicali. Riusciremo comunque a calcolare il suo gruppo di Galois.

Esempio 17. *Consideriamo il polinomio* $p(x) = 2x^5 - 5x^4 + 5$ *definito e iriducibile sul campo* $F = \mathbb{Q}$ *(cfr. Criterio di Eisenstein ed Esempio 31 in Appendice). Indichiamo con* K *il suo campo di spezzamento.*

Un veloce studio di funzione di $y = p(x)$ *ci permette di sapere che questo polinomio ha esattamente* 3 *radici reali* α, β *e* γ *e quindi due radici complesse coniugate* δ *e* $\overline{\delta}$.

Vogliamo ora mostrare che il gruppo di Galois G *su* $\mathbb{Q}$ *della nostra equazione è tutto* S_5. *Per prima cosa osserviamo che* G *contiene lo scambio* $(\delta\,\overline{\delta})$ *ossia:*

$$\begin{pmatrix} \alpha & \beta & \gamma & \delta & \overline{\delta} \\ \alpha & \beta & \gamma & \overline{\delta} & \delta \end{pmatrix}$$

che corrisponde all'isomorfismo di K *in sé dato dal coniugio (che lascia fissi tutti i reali). Proveremo ora che contiene anche un* 5*-ciclo.*

Possiamo considerare il sottoinsieme G_α *di* G *delle permutazioni ammissibili che lasciano fisso* α*; si verifica facilmente che* G_α *è un sottogruppo non necessariamente normale (anche la composizione e l'inversa dei suoi elementi lasciano fisso* α*).*

Osserviamo che i laterali (sinistri) di G_α *corrispondono ciascuno ad una delle radici: infatti due permutazioni* σ *e* τ *sono in relazione se e soltanto se* $\tau^{-1}\sigma \in G_\alpha$ *ossia se* $\tau^{-1}\sigma(\alpha) = \alpha$ *cioè* $\sigma(\alpha) = \tau(\alpha)$.

Poiché il polinomio è irriducibile su $\mathbb{Q}$, *vi sono in* G *permutazioni che scambiano* α *con ciascuna delle altre radici. Infatti per il Teorema 15 possiamo costruire un omomorfismo* $\phi\colon F_1 = \mathbb{Q}(\alpha) \to \mathbb{C}$ *che fissa* $\mathbb{Q}$ *ed estenderlo ad un isomorfismo* $\psi\colon K = F_1(\beta, \gamma, \delta, \overline{\delta}) \to K$ *ossia ad una permutazione delle* 5 *radici.*

I laterali rispetto a G_α *sono dunque* 5 *e quindi per il Teorema di Lagrange (cfr Teorema 24 in Appendice) il gruppo* G *ha ordine* $5|G_\alpha|$, *multiplo di* 5. *Per il Teorema di Cauchy (cfr. Teorema 26 in Appendice)* G *possiede un elemento con periodo* 5*: in* S_5 *gli unici elementi con periodo* 5 *sono i* 5*-cicli.*

Grazie alla Proposizione 5 possiamo concludere che G, *contenendo una trasposizione e un* 5*-ciclo, coincide con tutto* S_5. *Ricordiamo che* S_5 *è un gruppo non risolubile!*

IRIAMO LE FILA
Il nostro discorso si potrà considerare concluso non appena avremo provato che una equazione non è risolubile per radicali quando non è risolubile il suo gruppo di Galois. Proveremo infatti che se una equazione è risolubile per radicali il suo gruppo di Galois è risolubile.

Quando esistono formule risolutive per radicali dell'equazione $p(x) = 0$, possiamo costruire un'estensione E di F aggiungendo al campo base F uno dopo l'altro i radicali che sono necessari per scrivere le soluzioni di $p(x) = 0$. In questo caso E contiene (ma non coincide necessariamente) con il campo di spezzamento K di $p(x)$. Si ottiene così una catena crescente di campi F_i che parte dal campo di definizione F e termina col campo E:

$$F_0 = F \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_r = E$$

in cui ogni passaggio intermedio è una estensione data dall'aggiunta di un RADICALE, ossia $F_i = F_{i-1}(c_i)$ dove $c_i \in \mathbb{C}$ e $c_i^s = a_i \in F_{i-1}$ per un qualche esponente intero s.

Gli isomorfismi di E che fissano ciascun campo F_i formano allora una catena decrescente di gruppi:

$$G_0 = \Gamma_F(E) \supseteq G_1 = \Gamma_{F_1}(E) \supseteq G_2 = \Gamma_{F_2}(E) \supseteq \cdots \supseteq G_r = \Gamma_E(E) = \{e\}$$

Anche per una equazione non risolubile si può costruire una catena di estensioni da F a K aggiungendo ogni volta un elemento opportuno (ad esempio una delle soluzioni dell'equazione) e alla catena di campi si può far corrispondere una catena decrescente di sottogruppi del gruppo di Galois. La proprietà peculiare delle equazioni risolubili per radicali sta proprio nel fatto che la catena si possa ottenere aggiungendo non elementi qualsiasi, ma dei radicali opportuni. Proveremo ora che a questa catena di campi così speciale corrisponde una catena di sottogruppi altrettanto speciale: una catena che rende il gruppo di Galois un gruppo risolubile. Ci troviamo dunque al punto conclusivo e cuore dell'intero ragionamento.

Osservazione 18. Il nostro ragionamento sarà notevolmente semplificato se, nel costruire l'estensione E, eseguiamo l'aggiunta successiva di radicali rispettando le seguenti due condizioni.

- **Aggiungiamo solo radicali p-esimi con p numero primo**. Se è necessario aggiungere una radice s-esima c di un numero a e $s = mp$, possiamo aggiungere per prima cosa $c' = c^m$ (che è un radicale p-esimo di a, rimandando a passi successivi l'aggiunta di c come radicale m-esimo di un elemento del nuovo campo così ottenuto, ripetendo per una fattorizzazione in primi di m il passo precedente). Quindi aggiungere un radicale s-esimo è equivalente ad aggiungere uno dopo l'altro un numero finito di radicali primi.

- **Per ogni primo p per cui servirà aggiungere i radicali p-esimi di un qualche numero, aggiungiamo innanzi tutto le radici p-esime dell'unità.** Osserviamo che, in questo modo, aggiungere un radicale p-esimo b di un numero a equivarrà ad aggiungerli tutti, poiché ogni radicale p-esimo di a si può ottenere come prodotto di b per un'opportuna radice p-esima dell'unità.

Teorema 19. *Sia $p(x)$ un polinomio risolubile per radicali definito sul campo F e sia E il campo costruito secondo le due condizioni precedenti. Allora il gruppo di Galois $\Gamma_F(E)$ è risolubile.*

Ricordando la definizione di gruppo risolubile, per completare la dimostrazione rimane soltanto da far vedere che ad ogni anello della catena di campi

$$F_{i-1} \subseteq F_i = F_{i-1}(c_i) \quad \text{con} \quad c_i^p \in F_{i-1}$$

(costruito rispettando i criteri indicati nell'Osservazione 18) corrisponde un anello della catena di sottogruppi

$$G_{i-1} \supseteq G_i \quad \text{con} \quad G_{i-1} = G_i \text{ oppure } G_i \text{ normale e } G_{i-1}/G_i \text{ di ordine } p.$$

Per evitare di portarci dietro gli indici riscriviamo la proprietà da dimostrare fissando l'attenzione su un singolo anello della catena.

Siano k un sottocampo di E e $c \in E$ un radicale p-esimo su k ossia un elemento tale che $c^p = a \in k$ per un qualche primo p. Siano poi:

$$G = \{\psi \colon E \to E \textit{ isomorfismi di campo che fissano } k\}$$

$$H = \{\phi \colon E \to E \textit{ isomorfismi di campo che fissano } k(c)\}.$$

Se $H = G$, non c'è nulla da provare. Supponiamo allora $H \neq G$: vogliamo provare che H è un sottogruppo normale di G e che il quoziente G/H ha ordine p.

Per provare la normalità utilizziamo il Criterio 28 dell'Appendice, ossia verifichiamo che:

$$\forall \psi \in G\,,\ \forall \phi \in H \text{ si ha } \psi^{-1}\phi\psi \in H.$$

Tutti gli isomorfismi coinvolti fissano k; dobbiamo allora controllare soltanto che $(\psi^{-1}\phi\psi)(c) = c$ ossia più semplicemente che $(\phi\psi)(c) = \psi(c)$.

La soluzione di una equazione a coefficienti in k potrà avere come immagine soltanto una soluzione della stessa equazione; nel caso in esame c e $\psi(c)$ sono entrambe soluzioni di $x^p = a$.

i) Proviamo per prima cosa la nostra tesi nel caso $a = 1$ ossia quando c è una radice p-esima η di 1: possiamo supporre che η sia la soluzione di $x^p = 1$ data in forma trigonometrica da $\eta = cos(\frac{2\pi}{p}) + isen(\frac{2\pi}{p})$ in modo che tutte le altre radici p-esime dell'unità siano potenze di η. Notiamo cha allora aggiungere η equivale ad aggiungere tutte le radici dell'unità. Inoltre, poiché anche $\psi(c)$ è una radice p-esima di 1 si avrà $\psi(\eta) = \eta^r$. Allora:

$$(\phi\psi)(\eta) = \phi(\eta^r) = (\phi(\eta))^r = \eta^r = \psi(\eta)$$

come richiesto dal Criterio 28 e quindi il sottogruppo H è normale.
(Ricordiamo sempre che gli omomorfismi rispettano le operazioni e in particolare che l'immagine di un prodotto è il prodotto delle immagini.)

ii) Proviamo ora la nostra tesi nel caso generale in cui a è un numero qualsiasi e c è una soluzione di $x^p = a$, supponendo però di aver già aggiunto in precedenza al campo le radici p-esime di 1. Notiamo che in tal caso aggiungere al campo la sola radice p-esima c di a equivale ad aggiungerle tutte poichè due soluzioni di $x^p = a$ si possono ottenere una dall'altra moltiplicando per una opportuna radice p-esima di 1. In particolare si avrà $\psi(c) = \eta^s c$ dove $\eta^s \in k$ poiché è una radice p-esima di 1.

Abbiamo allora:

$$(\phi\psi)(c) = \phi(\eta^s c) = \eta^s c = \psi(c)$$

come richiesto dal Criterio 28 e quindi anche in questo caso il sottogruppo H è normale.
Dunque il laterale modulo H di ogni isomorfismo ψ è perfettamente individuato se si assegna $\psi(c)$, poichè $\psi_1^{-1}\psi_2 \in H \iff (\psi_1^{-1}\psi_2)(c) = c \iff \psi_1(c) = \psi_2(c)$. Ora $\psi(c) = \eta^s c$ è una delle p radici p-esime di a, dunque il numero di classi, ossia l'ordine del gruppo G/H, è $\leq p$.

D'altra parte se $\psi(c) = \eta^s c \neq c$ gli isomorfismi ψ, ψ^2, ..., ψ^p sono tutti diversi, poichè assegnano immagini diverse a c in quanto, per ogni $s \neq 0$, η^s ha p potenze distinte; allora G/H ha almeno p elementi.

In conclusione G/H ha esattamente p elementi. ∎

Osservazione 20. La normalità di H in G equivale al fatto che due isomorfismi ψ_1 e ψ_2 di E che fissano k differiscono solo per un isomorfismo ϕ di E che fissa $k(c)$, ossia $\psi_1 = \phi\psi_2$, se e solo se $\psi_1(c) = \psi_2(c)$. Ciò permette di "contare" gli isomorfismi ψ a meno degli isomorfismi ϕ.

Generalizzando l'osservazione precedente si prova poi che il gruppo di Galois del campo di spezzamento di una equazione risolubile per radicali è un quoziente del gruppo di Galois di E, il campo costruito aggiungendo radicali. In formule possiamo scrivere

$$\Gamma_F(K) \simeq \Gamma_F(E)/\Gamma_K(E).$$

Infatti ad ogni isomorfismo di E che fissa F possiamo associare la sua restrizione a K, che risulta essere un isomorfismo di K poichè, come più volte sottolineato, le immagini delle soluzioni di una equazione devono necessariamente essere soluzioni della stessa equazione. Inoltre tale corrispondenza è chiaramente un omomorfismo di gruppi in cui due isomorfismi ψ_1 e ψ_2 di E si restringono ad uno stesso isomorfismo di K se e soltanto se $\psi_1^{-1}\psi_2$ si restringe all'identità, ossia fissa K. Notiamo che la normalità di $\Gamma_K(E)$ è immediata conseguenza del fatto di essere il nucleo dell'omomorfismo di restrizione.

Per poter concludere non ci resta che provare il seguente fatto del tutto generale:

Lemma 21. *Il quoziente di un gruppo risolubile è un gruppo risolubile.*

Dimostrazione. Consideriamo un gruppo risolubile G e un suo sottogruppo normale H. Ci basterà provare che se G ha un sottogruppo normale G_1 tale che G/G_1 ha un numero primo p di elementi, allora le classi in G/G_1 degli elementi di H coincidono con l'intero quoziente oppure costituiscono un suo sottogruppo normale tale che il quoziente ha p elementi.

Le classi degli elementi di G_1 costituiscono un sottogruppo di G/H: denotiamo tale sottogruppo con $\pi(G_1)$ e indichiamo mediante una soprallineatura la classe in G/H degli elemento di G. Per ogni $\phi \in G$ e ogni $\psi \in G_1$ avremo:

$$\overline{\phi}^{-1}\ \overline{\psi}\ \overline{\phi} = \overline{\phi^{-1}\psi\phi} = \overline{\psi'} \text{ dove, per la normalità di } G_1,\ \psi' \in G_1$$

ossia $\pi(G_1)$ è un sottogruppo normale di G/H.

Infine, ricordando che ci sono esattamente p laterali di G_1 in G, contiamo i laterali di $\pi(G_1)$ in G/H. Se α è un elemento di G che non appartiene ad H, il periodo di $\overline{\alpha}$ in G/H deve essere un divisore maggiore di 1 di p, ossia proprio p; in altri termini $\alpha^p \in G_1$ ed inoltre ogni elemento di G si può scrivere come $\alpha^r\psi$ per opportuni $\psi \in G_1$ e $r \in \mathbb{N}$, $0 \leq r \leq p-1$. Le stesse proprietà valgono allora per $\overline{\alpha} \in G/H$; quindi l'ordine di $\overline{\alpha}$ divide p e inoltre G/H è l'unione dei laterali $\overline{\alpha}^r\pi(G_1)$, che saranno tutti coincidenti se $\overline{\alpha}$ ha ordine 1 oppure sono p tutti distinti se $\overline{\alpha}$ ha ordine p. ∎

Pertanto abbiamo dimostrato che il gruppo di Galois di una equazione risolubile per radicali è risolubile come gruppo quoziente di un gruppo risolubile (per approfondimenti si vedano anche [1] e [10]).

Siamo finalmente arrivati alla conclusione della trattazione.

- Abbiamo trovato un esempio di quintica in $\mathbb{Q}[x]$ il cui gruppo di Galois è S_5;
- Abbiamo dimostrato che il gruppo S_5 non è risolubile.
- Abbiamo dimostrato che ogni equazione risolubile per radicali ha gruppo di Galois risolubile.

Allora le soluzioni della nostra equazione quintica non possono assolutamente essere scritte mediante radicali iterati di espressioni che coinvolgono solo i suoi coefficienti e numeri razionali.

Appendice

Richiami sui gruppi

Si dice GRUPPO un insieme G dotato di un'operazione, che indicheremo con $*$ (che, a seconda dei casi, può essere la somma, il prodotto, la composizione di permutazioni ecc.) per cui vale la proprietà associativa:

$$\forall\, a,\, b,\, c \in G \quad \text{si ha } a * (b * c) = (a * b) * c$$

rispetto alla quale c'è un elemento neutro:

$$\exists e \ \text{ tale che } \forall a \in G \quad \text{si ha } a * e = e * a = a$$

e ogni elemento è dotato di inverso:

$$\forall\ a \in\ G,\, \exists\, b \in G \ \text{ tale che } a * b = b * a = e$$

Non è richiesta in genere la validità della proprietà commutativa del prodotto; se vale, il gruppo si dice GRUPPO ABELIANO.

Da ora in poi tralasceremo il simbolo $*$ di operazione e adotteremo la simbologia tipica del prodotto; in particolare l'elemento neutro e sarà scritto anche 1_G, l'inverso di a sarà scritto a^{-1} e il prodotto iterato di un elemento a per se stesso n volte sarà scritto a^n.

In un gruppo valgono le seguenti proprietà:
- l'elemento neutro è unico
- l'inverso di ogni elemento è unico
- l'inverso del prodotto di due elementi è il prodotto degli inversi in ordine opposto, cioè

$$(ab)^{-1} = b^{-1}a^{-1}$$

Osserviamo che la moltiplicazione per un fissato elemento a di un gruppo G "permuta" gli elementi di G, ossia ogni elemento g di G si scrive in uno ed un solo modo come $g = ab$ per un opportuno $b \in G$ (ed esattamente $b = a^{-1}g$). Questa semplice osservazione permette di provare il seguente risultato.

Proposizione 22. *I gruppi con 2 oppure con 3 elementi sono tutti abeliani.*

Dimostrazione. Consideriamo dei gruppi $H = \{e, a\}$ e $G = \{e, a, b\}$ con 2 e 3 elementi rispettivamente; in entrambi i casi e è l'identità. La tabella della moltiplicazione è una tabella 2×2 e rispettivamente 3×3 del tipo:

$\cdot$	e	a
e		
a		

$\cdot$	e	a	b
e			
a			
b			

dove in ogni riga e in ogni colonna devono comparire tutti gli elementi una e una volta sola (e la moltiplicazione per e lascia invariati gli elementi). È facile convincersi, come in una variante del Sudoku, che c'è un solo modo di completare le tabelle e che il prodotto così ottenuto non dipende dall'ordine dei fattori: quindi H e G sono abeliani. ∎

Questi due esempi rientrano nel caso più generale di gruppi con un numero primo di elementi che, come vedremo tra breve, sono sempre abeliani. Molti dei gruppi più interessanti però non sono abeliani.

Un sottoinsieme non vuoto S di un gruppo G è un SOTTOGRUPPO se è un gruppo per la stessa operazione di G. Dalla definizione si deduce subito che devono appartenere ad un qualsiasi sottogruppo di G sia 1_G sia gli inversi in G degli elementi del sottogruppo. Vi è un comodo criterio per stabilire se un sottoinsieme S di G è un sottogruppo:

$$S \text{ è un sottogruppo di } G \iff S \neq \emptyset \text{ e } \forall\, a,\, b \in S \text{ si ha } ab^{-1} \in S.$$

Esempio 23. *Per ogni elemento a di G si può costruire un sottogruppo $\langle a \rangle$ costituito da tutte gli elementi del tipo a^n con $n \in \mathbb{Z}$. Come d'abitudine $a^0 = 1_G$ e $a^{-n} = (a^{-1})^n$. Anche se G non è abeliano, i suoi sottogruppi $\langle a \rangle$ lo sono sempre.*

Particolarmente importanti sono i gruppi con un numero finito di elementi: indichiamo con $|G|$ tale numero detto ORDINE del gruppo.

Ovviamente se G è finito, anche i suoi sottogruppi lo sono; in particolare l'ordine di un sottogruppo del tipo $\langle a \rangle$ si dice anche PERIODO dell'elemento a ed è il più piccolo intero $r > 0$ tale che $a^r = 1_G$.

Un sottogruppo S di G permette di costruire in G due relazioni di equivalenza. Una relazione $\sim_D$ definita da:

$$a \sim_D b \iff ba^{-1} \in S \quad \text{ovvero } \exists\, s \in S \text{ t.c. } b = sa$$

Si verifica facilmente che $\sim_D$ è una equivalenza e che suddivide quindi G in classi di equivalenza Sa dette LATERALI DESTRI di S:

$$Sa = \{\text{prodotti } sa \text{ al variare di } s \in S\}$$

Si può definire in modo analogo la relazione di equivalenza $\sim_S$:

$$a \sim_S b \iff a^{-1}b \in S \text{ ovvero } \exists s \in S \text{ t.c. } b = as$$

Le classi di equivalenza di $\sim_S$ dette LATERALI SINISTRI di S sono:

$$aS = \{\text{prodotti } as \text{ al variare di } s \in S\}$$

Nel caso di un gruppo finito G, una caratteristica importante dei laterali destri e sinistri è quella di avere ciascuno tanti elementi quanti S: infatti la moltiplicazione per un elemento a di G trasforma elementi distinti b, $c \in S$ in elementi distinti ba, ca di Sa (rispettivamente ab, ac di aS. Questa semplice osservazione prova il

Teorema 24 (Lagrange)**.** *L'ordine di ogni sottogruppo S di G divide l'ordine di G. Il periodo di ogni elemento $a \in G$ divide l'ordine di G.*

Infatti $|G|$ si può ottenere moltiplicando il numero di laterali destri (oppure sinistri) di S per il numero di elementi in ciascuno di essi, ossia per $|S|$; per la seconda parte basta applicare la prima ai sottogruppi $\langle a \rangle$.

Se l'ordine di un gruppo G è un numero primo p, preso un qualsiasi elemento a di G diverso da e, l'insieme H delle potenze di a costituisce un sottogruppo di G con almeno 2 elementi; per il teorema di Lagrange l'ordine di H è un divisore di p e quindi è p stesso ossia $G = H$. Una conseguenza interessante è:

Corollario 25. *Ogni gruppo N di ordine primo p è costituito dalle potenze di un suo qualsiasi elemento g diverso da e, ossia $N = \{e,\ g^2, \ldots, g^{p-1}\}$. Gruppi siffatti sono tutti abeliani.*

In generale, non è detto che per ogni numero m che divide $n = |G|$ esista sempre un sottogruppo di ordine m e, in particolare, un elemento con periodo m. Di questioni di questo genere si occupano i TEOREMI DI SYLOW. Per i nostri scopi sarà sufficiente conoscere il risultato seguente.

Teorema 26 (Cauchy)**.** *Se p è un numero primo che divide $n = |G|$, allora in G vi è almeno un elemento con periodo p.*

Dimostrazione. Scopo della dimostrazione è provare l'esistenza di elementi $a \in G$ diversi da e tali che $a^p = e$; se infatti $a^p = e$ allora il periodo di a è necessariamente un divisore di p e quindi è proprio p oppure 1 (ma l'unico elemento tale che $a^1 = e$ è ovviamente e stesso).

Consideriamo le n^{p-1} disposizioni con ripetizione (ossia sequenze ordinate) $(a_1, \ldots, a_{p-1})$ di $p-1$ elementi di G e aggiungiamo come p-esimo elemento l'inverso del loro prodotto $a_p = (a_1 \cdots a_{p-1})^{-1}$. Otteniamo così l'insieme Q di tutte le sequenze ordinate di p elementi del gruppo con prodotto e:

$$Q = \{(a_1, \ldots, a_{p-1}, a_p) \text{ tali che } a_i \in G \text{ e } \ a_1 a_2 \cdots a_{p-1} a_p = e\}\,.$$

Notiamo che ogni sequenza del tipo $(a_2, \ldots, a_{p-1}, a_p, a_1)$ che si può ottenere da una sequenza $(a_1, \ldots, a_{p-1}, a_p)$ di Q con uno "slittamento circolare " sta a sua volta in Q. Infatti da $a_1 \cdot a_2 \cdots a_p = e$, moltiplicando a destra per a_1 e a sinistra per il suo inverso si ottiene $a_2 \cdots a_p \cdot a_1 = a_1^{-1} \cdot e \cdot a_1 = e$.

Possiamo allora raggruppare tra loro quelle sequenze di Q che si possono ottenere una dall'altra con slittamenti circolari, ossia:

$$(a_1, \ldots, a_{p-1}, a_p)\,,\ (a_p\,, a_1, \ldots, a_{p-1})\,,\ (a_{p-1}, a_p\,, a_1, \ldots, a_{p-2})\,,\ \text{ ecc.}$$

I sottoinsiemi di Q così ottenuti sono formati al massimo da p sequenze diverse (perché p slittamenti circolari ci riportano nella posizione iniziale); se però nella sequenza ci sono degli elementi ripetuti, potremmo ottenere la sequenza iniziale anche dopo un numero minore di slittamenti.

Un caso limite è quello dalla sequenza $(e, e, \ldots, e)$ che coincide con tutti i suoi slittamenti; il sottoinsieme relativo è costituito da una sola sequenza. Allo stesso modo sono costituiti da una sola sequenza i sottoinsiemi relativi a sequenze del tipo $(a, a, \ldots, a)$ con $a^p = e$ (proprio gli elementi che cerchiamo!).

Negli altri casi invece i sottoinsiemi contengono esattamente p sequenze differenti; in caso contrario otterremo la sequenza iniziale per la prima volta dopo $s < p$ slittamenti; ma allora anche dopo t slittamenti, dove t è il resto della divisione di p per s: se infatti $p = cs + t$, t slittamenti in avanti sono come p slittamenti in avanti seguiti per c volte da s slittamenti indietro e quindi t slittamenti in avanti riportano alla posizione iniziale. Poichè p è un numero primo il resto t è > 0 e minore di s; otteniamo così una contraddizione con l'ipotesi che s fosse il minimo.

Allora gli elementi di Q si ripartiscono tra k sottoinsiemi con p elementi ciascuno e h ($h \geq 1$) sottoinsiemi con 1 solo elemento ciascuno e quindi vale l'uguaglianza $n^{p-1} = kp + h$. Poichè n è multiplo di p, anche n^{p-1} lo è e

di conseguenza deve esserlo pure h. Oltre ad e vi sono allora almeno altri $h \geq p-1$ elementi $a \in G$ tali che $a^p = e$, come volevamo. ∎

OTTOGRUPPI NORMALI E QUOZIENTI

In generale, se G non è abeliano, un laterale destro Na rispetto ad un sottogruppo N e il corrispondente laterale sinistro aN possono anche essere diversi (tuttavia nel caso dell'elemento neutro e vale sempre $eN = Ne = N$). Un sottogruppo N di G si dice NORMALE se ciascun suo laterale destro Na coincide come insieme col corrispondente laterale sinistro aN.

Osserviamo che la definizione precedente richiede che aN e Na siano uguali come insiemi e non che per ogni $b \in N$ si abbia $ab = ba$ (quest'ultima sarebbe una richiesta molto più forte!) In pratica:

$$\forall a \in G\ ,\ \forall n \in N \quad \text{deve esistere} \quad n' \in N \quad \text{t.c.} \quad an = n'a$$

e viceversa

$$\forall a \in G\ ,\ \forall m \in N \quad \text{deve esistere} \quad m' \in N \quad \text{t.c.} \quad ma = am'$$

Esempio 27. *Se un sottogruppo N di G ha la metà degli elementi di G ossia $|G| = 2|N|$, allora N è sicuramente normale in G. Infatti rispetto ad N ci sono due laterali sinistri e due destri; in entrambi i casi il laterale di e è N e quindi, in entrambi i casi, l'altro laterale non può essere altro che il complementare di N in G.*

Il motivo per cui sono importanti i sottogruppi normali è che ad essi sono associati i GRUPPI QUOZIENTE. Gli elementi del quoziente G/N sono i laterali di N.

Se N è un sottogruppo normale del gruppo G si può definire una operazione tra i laterali nel modo seguente:

$$aN \cdot bN = (ab)N.$$

Il problema che si potrebbe presentare con definizioni di questo genere è quello di ottenere risultati differenti a seconda di come si scrivono gli elementi da comporre. Infatti il laterale aN di un elemento a è anche il laterale $a'N$ di ogni altro elemento $a' \in aN$. La definizione ha senso soltanto se il risultato dell'operazione è unico, ossia solo se:

$$\forall\, a' \in aN\ ,\ \forall\, b' \in bN \quad \text{si ha} \quad (ab)N = (a'b')N.$$

Verifichiamo la validità di questa relazione usando proprio la normalità di N.

Per ipotesi esistono c, $d \in N$ tali che $a' = ac \in aN$, $b' = db \in Nb = bN$. Posto poi $d' = cd$ si ha $d'b \in Nb = bN$ e quindi esiste $d'' \in N$ tale che $d'b = bd''$; quindi $a'b' = acdb = ad'b = abd'' \in abN$. Allora i laterali di $a'b'$ e di ab coincidono e l'operazione di prodotto tra laterali è ben definita.

Un comodo criterio usato nella trattazione è il seguente:

Criterio 28.

$$N \text{ è normale in } G \iff \forall a \in G, \forall c \in N \text{ si ha } aca^{-1} \in N.$$

Infatti:

$$aN = Na \iff \forall c \in N\ \exists c' \in N :\ ac = c'a \iff \forall c \in N\ aca^{-1} \in N.$$

Esempio 29. *Il sottogruppo di S_3 generato da uno scambio non è normale. Consideriamo ad esempio il sottogruppo*

$$H = \left\{ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, e \right\}.$$

I laterali della permutazione $a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$*:*

$$aH = \left\{ a\,,\ a\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\} \qquad Ha = \left\{ a\,,\ \sigma a = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

sono chiaramente diversi tra loro.

In modo alternativo avremmo potuto verificare che H non è normale mediante il criterio precedente. La permutazione inversa di a è $a^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ *e quindi il prodotto* $a\sigma a^{-1}$ *è* $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ *che non appartiene ad H.*

RICHIAMI SUGLI OMOMORFISMI

Il termine omomorfismo ricorre spesso in matematica e significa concretamente funzione tra insiemi dotati di uno stesso tipo di struttura algebrica, compatibile con la struttura stessa.

Se G e G' sono gruppi, un OMOMORFISMO DI GRUPPI è una funzione $f : G \to G'$ tale che:

$$\forall x, y \in G \text{ si ha } f(xy) = f(x)f(y) \text{ in } G'.$$

Se K e K' sono campi, un OMOMORFISMO DI CAMPI è una funzione $f : K \to K'$ tale che:

$$\forall x, y \in K \text{ si ha } f(x+y) = f(x) + f(y) \text{ e } f(xy) = f(x)f(y) \text{ in } K'.$$

Un omomorfismo che sia anche iniettivo e suriettivo è detto ISOMORFISMO. Se tra due strutture algebriche vi è un isomorfismo, allora le proprietà dell'una corrispondono sempre a quelle dell'altra. Ad esempio se due gruppi sono isomorfi ed uno di essi è abeliano, anche l'altro lo è; i sottogruppi dell'uno corrispondono biunivocamente a quelli dell'altro ed in particolare i sottogruppi normali corrispondono ai sottogruppi normali, ecc.

Anche nel caso di semplici omomorfismi la necessità di rispettare le operazioni pone molte limitazioni alle possibili immagini degli elementi del dominio. L'immagine dell'elemento neutro rispetto ad una operazione del dominio, ad esempio, non può essere un qualsiasi elemento del codominio, ma deve necessariamente essere l'elemento neutro della corrispondente operazione nel codominio; così le immagini di elementi inversi devono essere a loro volta inverse l'una dell'altra, ecc.

Inoltre, spesso, le immagini di pochi elementi del dominio determinano l'intera funzione in quanto permettono di ottenere le immagini di tutti gli altri elementi. Gli omomorfismi sono quindi "pochi" rispetto a tutte le possibili funzioni.

Un omomorfismo di campi è necessariamente iniettivo: due elementi diversi di K non possono avere immagini uguali; in caso contrario la loro differenza avrebbe inverso nel campo K, mentre la differenza delle immagini sarebbe 0 che non ha inverso in K'.

RADICI MULTIPLE

Una radice α di $p(x) \in F[x]$, si dice RADICE MULTIPLA se $(x-\alpha)^2$ divide $p(x)$; la MOLTEPLICITÀ della radice α è il numero intero r tale che $(x-\alpha)^r$ divide $p(x)$, ma $(x-\alpha)^{r+1}$ non lo divide.

Talvolta può essere conveniente supporre che un certo polinomio sia privo di radici multiple. Per controllare che tale ipotesi sia soddisfatta (e in caso

contrario ottenere un polinomio $q(x)$ con le stesse radici di $p(x)$, ma tutte di molteplicità 1) possiamo ricorrere al semplice metodo seguente, che utilizza la derivata $p'(x)$ del polinomio $p(x)$. L'unica richiesta necessaria per applicare tale metodo è che $\mathbb{Q}$ sia contenuto nel campo F su cui $p(x)$ è definito.

Proposizione 30. *Se α è radice del polinomio $p(x) \in F[x]$ con molteplicità r, allora α è radice di $p'(x)$ con molteplicità $r-1$.*

Il polinomio $q(x) = \frac{p(x)}{MCD(p(x),p'(x))}$ ha quindi le stesse radici di $p(x)$, ma tutte con molteplicità 1.

La dimostrazione segue immediatamente dal calcolo della derivata di $p(x)$ scritto come $(x-\alpha)^r g(x)$. Ricordiamo che il MCD di due polinomi può essere calcolato mediante l'algoritmo euclideo con divisioni successive, procedura che non richiede la conoscenza della fattorizzazione di $p(x)$ in fattori irriducibili (vantaggio non piccolo dato che, in genere, la fattorizzazione di un polinomio non si sa calcolare).

Polinomi a coefficienti razionali

Contrariamente a quanto accade per i polinomi a coefficienti reali o complessi, i polinomi a coefficienti razionali ammettono sempre procedure algoritmiche per ottenere le loro radici razionali e, più in generale, la loro fattorizzazione razionale:

si badi bene, solo radici in $\mathbb{Q}$ e fattori irriducibili a coefficienti in $\mathbb{Q}$!

Sia $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ un polinomio a coefficienti razionali.
Possiamo intanto ricondurci al caso $a_i \in \mathbb{Z}$ moltiplicando se necessario per un denominatore comune.

Ogni numero razionale $q = \frac{c}{d}$ con c, $d \in \mathbb{Z}$ primi tra loro, per essere radice di $p(x)$ deve soddisfare le due condizioni: c divide a_0 e d divide a_n.

La verifica si ottiene sostituendo q in $p(x)$, eliminando i denominatori mediante moltiplicazione per d^n e raccogliendo opportunamente.

Le due condizioni non sono ovviamente sufficienti affinché q sia una radice di $p(x)$, ma ci forniscono una lista finita di numeri razionali (i rapporti tra ogni divisore di a_0 e ogni divisore di a_n) che contiene tutte le eventuali radici razionali del polinomio. Basterà allora eseguire la cernita sostituendo i candidati uno alla volta in $p(x)$ per vedere quali sono radici e quali non lo sono.

Metodi analoghi, lunghi ma efficaci, permettono di individuare la decomposizione di $p(x)$ in fattori irriducibili a coefficienti interi. Non li riportiamo; ci limitiamo a ricordare un risultato utilizzato in questa esposizione.

Criterio di Eisenstein. *Sia* $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ *un polinomio a coefficienti interi. Se esiste un intero* p *tale che:*

- p *divide i coefficienti* $a_{n-1}, \ldots, a_0$
- *ma* p *non divide* a_n *e* p^2 *non divide* a_0

allora $p(x)$ *non si decompone nel prodotto di polinomi a coefficienti interi.*

Esempio 31. *I polinomi* x^4-2 *e* $2x^5-5x^4+5$ *non si decompongono nel prodotto di due o più polinomi a coefficienti interi (o razionali) di grado positivo.*

Bibliografia

[1] E. Artin, *Galois Theory*, Notre Dame Press (1971).

[2] E.T. Bell, *I grandi matematici*, Sansoni (1990).

[3] C.B. Boyer, *Storia della matematica*, Mondadori (1976).

[4] J.B. Fraleigh, *A first course in Abstract Algebra*, Addison-Wesley (1967).

[5] F. Klein, *The icosahedron*, Dover (1956).

[6] M. Livio, *L'equazione impossibile*, Rizzoli Editore (2005).

[7] I. Niven, *Numeri razionali e irrazionali*, Zanichelli (1968).

[8] N. Pellicano, *Non risolubilità dell'equazione di* $5°$ *grado*, Tesi di Laurea triennale Università di Torino A.A. 2004-2005.

[9] G.M. Piacentini Cattaneo, *Algebra, un approccio algoritmico*, Decibel-Zanichelli (1996).

[10] I. Stewart, *Galois Theory*, Chapman and Hall (1973).

[11] L. Toti Rigatelli, *La mente algebrica: storia dello sviluppo della Teoria di Galois nel XIX secolo*, Bramante Editrice (1989).

[12] L. Toti Rigatelli, *Matematica sulle barricate: vita di Evariste Galois*, Sansoni Editore (1993).