Il teorema di Liouville ovvero perché "non esiste" la primitiva di e^{x^2}

Camillo De Lellis

Il seguente contributo del professor Camillo De Lellis è l'elaborazione della conferenza che ha tenuto il 29 settembre 2012 presso il Liceo cantonale di Bellinzona, nell'ambito del convegno *L'eredità di Evariste Galois, matematico e rivoluzionario. Convegno sulla Teoria di Galois e le sue applicazioni*, organizzato dalla *Commissione di Matematica della Svizzera Italiana*.

1. Introduzione

Il titolo di questa noticina è volutamente provocatorio: la funzione di variabile reale $x \mapsto e^{x^2}$ è continua e quindi la primitiva – anzi **tante** primitive, vista la nota arbitrarietà di una costante additiva – esiste, eccome se esiste! Ce lo garantisce un classico teorema del calcolo e quindi, se riuscissimo a dimostrare il contrario, la matematica sarebbe contraddittoria e potremmo tornarcene tutti a casa a rinnovare il curriculum (noi matematici professionisti, s'intende...). Tuttavia è noto ai più che, per quanto tempo ci si spenda e a prescindere da quanto talento si abbia nell'arte di "primitivare", la ricerca di una forma chiusa per la primitiva di e^{x^2} è immancabilmente elusiva, perché la primitiva di e^{x^2} *non si può esprimere in termini di funzioni elementari*. "È noto" nel senso che molti sanno che è stato dimostrato da qualcuno. D'altra parte, a tutt'oggi non ho ancora incontrato un collega che mi abbia assicurato di aver letto tale dimostrazione. Lo si sa e basta.

Questa nota è allora dedicata al Prof. Paolo Spinelli, esimio preside della Facoltà di Scienze dell'Università di Bari, che come tutti i fisici non sempre resiste alla tentazione di sfottere il collega matematico della porta accanto. Un annetto fa, al termine di un'esaltante riunione della Commissione di Garanzia PRIN, Paolo mi fece notare la scarsa professionalità della mia categoria. Ci si attende che il matematico che spiattella con sicumera una certa affermazione sappia anche esaurientemente motivarla: la nostra mania di dimostrare tutto dovrebbe essere proprio ciò che ci distingue dai colleghi di fisica, con il loro spregiudicato approccio alle verità matematiche. Pertanto Paolo avrebbe voluto che, dopo avergli incautamente dichiarato la mia fede nell'impossibilità di trovare una forma chiusa per la primitiva di e^{x^2}, alla fine della riunione gli dessi uno straccio di spiegazione. Avrei potuto sostenere che ero troppo stanco per un compito sicuramente

impegnativo. Ho invece confessato la mia ignoranza e ammesso che la mia sicurezza era basata solo sul sentito dire; ma ho anche promesso che un giorno avrei soddisfatto la sua curiosità. Ci proverò con questa nota.

Prima però di immergerci nell'analisi del problema vorrei ripercorrere brevemente la sua storia. Come suggerisce il titolo, il primo a dimostrare l'impossibilità di esprimere una primitiva di e^{x^2} in termini di funzioni elementari è stato Liouville, in [7]. La dimostrazione che riportiamo qui non è però la sua, ma piuttosto una rielaborazione dovuta a Rosenlicht in [15] e basata su precedenti lavori di Ostrowski. Tale dimostrazione è essenzialmente di natura algebrica e usa svariati concetti che hanno la loro origine nella Teoria di Galois, anche se, contrariamente a quanto alcuni erroneamente affermano, il Teorema di Liouville non può essere considerato un *risultato di Teoria di Galois*, perché i gruppi di Galois non entrano mai in gioco.

In ogni caso, vista l'indubbia vicinanza, ho pensato che fosse una buona idea per una conferenza in un convegno di aggiornamento organizzato dal Canton Ticino per gli insegnanti della scuola superiore, un convegno che verteva appunto sulla Teoria di Galois. Come a volte, purtroppo, mi accade, forse ho puntato su un argomento troppo ambizioso e ostico. È inoltre opinabile che il materiale della conferenza e di questa nota si presti ad essere usato nella scuola superiore, se non per scaldare qualche aula fredda ... Mi scuso pertanto con i docenti che si sono pazientemente sorbiti l'ora e mezzo di miei deliri alla lavagna e spero che almeno la bellezza del risultato di Liouville non si sia del tutto persa.

Per quanto le dimostrazioni e le discussioni riportate di seguito si basino su alcuni strumenti matematici alquanto avanzati, ho cercato di fornire una spiegazione intuitiva per tutto e credo che, anche senza possedere conoscenze profonde, il lettore che abbia

- un'infarinatura di calcolo infinitesimale – ovvero sappia derivare e integrare,
- un minimo di familiarità con i numeri complessi,
- una vaga conoscenza degli assiomi dei campi (commutativi),
- e dimestichezza con il calcolo dei polinomi,

può assorbire da queste pagine le idee più importanti. Il lettore che conosce bene il calcolo infinitesimale e ha una discreta familiarità con l'algebra astratta apprezzerà anche le svariate sottigliezze degli argomenti più intricati. Infine, se conosce anche l'analisi complessa, potrà comprendere quei dettagli, secondo me marginali, che però rendono le considerazioni del tutto rigorose.

Come spesso accade nella matematica moderna, a partire dal risultato di Liouville, nella seconda metà del secolo scorso si è sviluppata un'intera branca della quale gli argomenti trattati qui sono solo i prodromi. Per chi fosse interessato,

la bibliografia di questa nota contiene qualche riferimento. Purtroppo (o per fortuna?) come matematico mi occupo di tutt'altro e questa è per me una breve escursione in terra incognita – tanto per avvertirvi che, benché sia convinto che questa nota esponga decentemente le idee principali della dimostrazione e non contenga errori importanti, qualcosa potrebbe essermi sfuggito e qualche lemma potrebbe non essere del tutto inappuntabile, in quanto a rigore matematico.

2. Formulazione del problema

In matematica le regole del gioco sono (quasi) sempre chiare. Il "quasi" non è una colpa della matematica, ma piuttosto dell'umanità di chi, finora, l'ha praticata – o l'ha inventata, non c'è accordo su questo punto. Cosa si intende allora con la frase *non si può esprimere in termini di funzioni elementari*? Tanto per cominciare, battezziamo la primitiva di e^{x^2}. In questo paragrafo la chiamiamo F e ci togliamo di torno la fastidiosa costante additiva imponendo $F(0) = 0$.

Una funzione reale di variabile reale è esprimibile in termini di funzioni elementari se è ottenuta componendo tra loro un numero finito di funzioni dei 4 tipi seguenti:

(a) funzioni razionali (ovvero rapporti di polinomi) a coefficienti reali;

(b) funzioni algebriche (ovvero le funzioni lisce che, localmente, esprimono soluzioni reali di polinomi a coefficienti reali);

(c) logaritmi ed esponenziali;

(d) funzioni trigonometriche e loro inverse.

Ciò che ci prefiggiamo – l'uso del plurale nei lavori di matematica dà sempre questa erronea impressione che l'autore sia aiutato da schiere di amici, o venga letto da migliaia di persone – ciò che ci prefiggiamo, dicevo, è allora di dimostrare che non c'è alcun intervallo dell'asse reale su cui la F sia il fortunato risultato di una tale composizione. Ovviamente, se non lo possiamo fare in "piccolo", ovvero su un intervallo, tantomeno potremo farlo su tutto l'asse reale: ci prefiggiamo quindi un compito potenzialmente più difficile. Ammoniamo il lettore – io e tutti gli amici che mi stanno aiutando – che la maggiore difficoltà è solo apparenza, come si può concludere da un semplice argomento di continuazione analitica.

Per renderci la vita un po' più semplice, d'ora in poi considereremo in realtà funzioni f di variabile reale a valori complessi. Chiaramente una f di questo tipo può essere decomposta come

$$f = \operatorname{Re} f + i \operatorname{Im} f$$

dove le funzioni $x \mapsto \operatorname{Re} f(x)$ e $x \mapsto \operatorname{Im} f(x)$ danno semplicemente la parte reale e quella immaginaria del numero complesso $f(x)$. Per noi derivare e integrare tali

funzioni significherà semplicemente derivare e integrare le rispettive parti reale e immaginaria e "ricomporle" nel modo ovvio. Per intenderci, se $h = f + ig$ e f e g sono funzioni reali, allora $h' = f' + ig'$. Per la primitiva procediamo analogamente. Penseremo quindi e^{x^2} come la funzione $x \mapsto e^{x^2} + i \cdot 0$ e vedremo di negare l'esistenza di una primitiva "complessa" elementare (di nuovo, ammoniamo il lettore che questo è solo apparentemente più complicato). Il motivo per tuffarci nel mondo complesso è semplice: in tale mondo le funzioni trigonometriche sono riconducibili a quelle esponenziali, così come le loro inverse si riducono a logaritmi. In particolare la nota formula di Eulero ci mostra come il seno sia una somma di esponenziali:

$$\sin x = \frac{e^{ix} - e^{-ix}}{2i}.$$

Essenzialmente manipolando quest'unica formula si riesce ad esprimere tutte le funzioni trigonometriche e le loro inverse a partire da logaritmi ed esponenziali. Questo ci libera dalla necessità di considerare la classe (d) nella lista di sopra. D'altra parte ci vorrà un po' di cura nella definizione dei logaritmi, vista la multivocità di tale operazione nel campo complesso. Di questo ci occuperemo tra un attimo.

3. Campi differenziali, estensioni e funzioni elementari

Per procedere dobbiamo introdurre il protagonista principale delle nostre discussioni.

Definizione 3.1. Un campo differenziale K è un campo nell'usuale senso del termine nell'algebra astratta (quindi un insieme con due operazioni, somma e prodotto, che soddisfano i soliti assiomi di campo, si veda ad esempio [6]) e che possiede una mappa $' : K \to K$, detta *derivata*, che soddisfa le seguenti proprietà:

(D1) $(ab)' = a'b + ab'$ per ogni $a, b \in K$;

(D2) $(a + b)' = a' + b'$ per ogni $a, b \in K$.

L'insieme degli elementi del campo la cui derivata è 0 (che è un sottocampo!) è detto *campo delle costanti*.

Il campo differenziale più semplice che considereremo in questa nota è il campo delle funzioni razionali, a coefficienti complessi, di una variabile reale.

Definizione 3.2. Indicheremo con $\mathbb{C}[x]$ l'anello dei polinomi a coefficienti complessi, ovvero delle funzioni $\mathbb{R} \ni x \mapsto f(x) \in \mathbb{C}$ della forma

$$f(x) = \sum_{j=0}^{n} c_j x^j, \qquad \text{dove } c_0, \ldots, c_n \in \mathbb{C}.$$

Indicheremo con $\mathbb{C}(x)$ il campo delle funzioni razionali, ovvero delle "funzioni" della forma

$$f(x) = \frac{P(x)}{Q(x)} \qquad \text{tali che } P, Q \in \mathbb{C}[x] \text{ sono polinomi primi tra loro.}$$

Con "primi tra loro" intendiamo, come al solito, che P e Q non hanno fattori comuni non banali, ovvero che non hanno radici (complesse!) in comune. D'altra parte abbiamo virgolettato il termine "funzioni" nel paragrafo precedente perché è ovvio che il valore di una generica $f \in \mathbb{C}(x)$ potrebbe non essere definito in alcuni punti (comunque un numero finito!). La derivata su $\mathbb{C}(x)$ è ovviamente la solita derivata e il sottocampo delle costanti non è altro che il solito sottocampo delle *funzioni costanti*: $\mathbb{C}(x)$ è a tutti gli effetti un campo differenziale e (D1) e (D2) non sono altro che la regola di Leibniz e l'additività della derivata. Il lettore attento avrà notato che manca la formula per la derivata del quoziente nella Definizione 3.1. In realtà non c'è bisogno di aggiungerla: il lettore molto attento avrà notato che essa è una conseguenza diretta di (D1) e (D2).

Osservazione 3.3. Nel seguito, ogni volta che tratteremo un campo differenziale K, esso sarà un "campo differenziale di funzioni complesse di variabile reale" dove si suppone che le funzioni in gioco siano definite su un intervallo $I \subset \mathbb{R}$ (comune a **tutti** gli elementi di K) tranne al più un insieme di punti isolati (che però potranno dipendere dalla funzione stessa). Queste funzioni f soddisferanno in realtà tutte una proprietà molto più forte:

(M) f è la restrizione all'intervallo I di una funzione meromorfa definita su un intorno complesso di I.

Il lettore che non è familiare con l'analisi complessa può tranquillamente trascurare i discorsi che faremo in seguito sulle funzioni meromorfe e la condizione (M). Il nucleo più importante delle idee esposte in questa nota non ha a che vedere con l'analisi complessa: la condizione (M) è solo un modo veloce per garantire la coerenza di alcuni dettagli, che altrimenti richiederebbero tediose giustificazioni. Raccogliamo qui di seguito quelle conseguenze che, se date per buone, eviterebbero alcune discussioni. Infatti, se f e g soddisfano (M), allora:

(M1) possiamo trascurare di discuterne la differenziabilità: f e g sono addirittura analitiche sul loro dominio di definizione;

(M2) l'insieme $\{f = g\}$ consiste sempre di punti isolati, se f e g sono distinte;

(M3) se la derivata di f si annulla in un sottointervallo, allora f è costante **su tutto il suo dominio di definizione**.

Per tutte queste proprietà rimandiamo a un qualsiasi testo classico di analisi complessa, come ad esempio [16]. Notiamo che (M3) non può essere conclusa come al solito dal teorema fondamentale del calcolo perché il dominio di definizione di f *non è connesso*.

Osservazione 3.4. Stiamo escludendo dalle nostre considerazioni anche comuni funzioni "definite a tratti", come

$$\varphi(x) = \begin{cases} \frac{1}{x} & \text{se } x > 0 \\ -\frac{1}{x} & \text{se } x < 0. \end{cases}$$

Infatti φ non soddisfa la condizione (M) su $I = \mathbb{R}$. Questo non inficia il nostro discorso perché mostreremo che non c'è **alcun intervallo** $I \subset \mathbb{R}$ su cui una primitiva di e^{x^2} è esprimibile in termini di funzioni elementari (in particolare si veda la formulazione del Corollario 4.4).

Definizione 3.5. Sia I un dato intervallo di $\mathbb{R}$. Supponiamo che K sia un campo di funzioni f, ciascuna definita su I tranne al più un insieme di punti isolati (che può dipendere da f stessa) e che soddisfi (M). Allora diciamo che K è un *campo di funzioni*. Se inoltre per ogni elemento f di K la derivata appartiene a K, allora diciamo che K è un *campo differenziale di funzioni*.

In pratica, visto che nel seguito considereremo sempre campi di funzioni K e come derivata prenderemo *sempre* la solita derivata, decidere o meno se K è differenziale equivarrà a capire se la solita operazione di differenziazione ci dà sempre elementi di K quando operiamo su K. D'altra parte è lecito chiedersi se, in uno qualsiasi di questi campi, non sia possibile definire un'altra operazione che soddisfi gli assiomi (D1) e (D2) ma non coincida con la "derivata dell'analisi". È sicuramente il caso per la mappa banale che assegna ad ogni elemento la funzione identicamente nulla. C'è in realtà una certa rigidità: se K è un campo di funzioni elementari (si rimanda ai paragrafi successivi per la definizione) ogni derivata su K, nel senso della Definizione 3.1, che coincida con la "derivata dell'analisi" sulle funzioni costanti e sulla funzione $x \mapsto x$, è necessariamente la solita operazione di differenziazione. Non useremo nel resto delle nostre discussioni questo fatto, che però si può verificare senza troppo sforzo ed è essenzialmente equivalente ad altre considerazioni che faremo.

Per rendere molti discorsi successivi più semplici, converrà introdurre polinomi e funzioni razionali a coefficienti in un campo arbitrario K, che verranno indicati con $K[X]$ e $K(X)$. Non stiamo in questo caso parlando di "funzioni" nel vero senso del termine, ma piuttosto di scritture "formali" del tipo

$$\sum_{j=0}^{n} k_j X^j \qquad \text{(per i polinomi)} \tag{3.1}$$

$$\frac{\sum_{j=0}^{n} k_j X^j}{\sum_{l=0}^{m} \kappa_l X^l} \qquad \text{(per le funzioni razionali)}\,, \tag{3.2}$$

dove i coefficienti k_j e κ_l sono elementi del campo K e, in (3.2), si suppone che denominatore e numeratore non abbiano fattori comuni non banali, ovvero siano polinomi primi fra loro relativamente al solito procedimento di "divisione con resto" per polinomi su un campo arbitrario, che d'ora in poi chiameremo *algoritmo*

di divisione euclideo – in pratica l'algoritmo euclideo non è altro che l'algoritmo comunemente chiamato *di Ruffini* nei licei. Primi fra loro vuol quindi dire che non c'è un polinomio di grado positivo che divida entrambi senza resto. Se poi un polinomio P non è diviso (senza resto) da *alcun* polinomio di grado minore e positivo, allora diremo, coerentemente con la letteratura, che P è irriducibile.

Una tipica situazione, che potrebbe generare confusione nel lettore – ma speriamo di no! – e che incontreremo spesso, è la seguente. K è già di per sé un campo di funzioni su un intervallo I, ad esempio il campo $\mathbb{C}(x)$. Un elemento in $K[X]$ è allora dato da una scrittura del tipo

$$R := \sum_{l=0}^{n} g_l X^l$$

dove ciascuna g_l è una "funzione" su I (ovvero un elemento di K: usiamo le virgolette solo perché al dominio di g_l potrebbe mancare una manciata di punti). Data un'ulteriore funzione di variabile reale f (ad esempio $x \mapsto f(x) = e^x$) – che non è necessariamente un elemento di K – potremo allora considerare la funzione $h := R(f)$, data da

$$x \mapsto h(x) := \sum_{i=0}^{n} g_l(x) \left(f(x)\right)^l . \tag{3.3}$$

h è allora definita ovunque su I eccetto che per un insieme di punti isolati e non è difficile vedere che, qualora f soddisfi (M) (come abbiamo già postulato per le g_l), allora anche h la soddisfa. Nell'esempio specifico $x \mapsto f(x) = e^x$ e $g_l \in \mathbb{C}(x)$ avremmo

$$x \mapsto \sum_{l=0}^{n} g_l(x) e^{lx} ,$$

che è una funzione meromorfa su tutto $\mathbb{C}$.

Osservazione 3.6. Grazie a (M), $h = R(f)$ è meromorfa in un intorno complesso di I e quindi (si veda (M2)) vale una delle seguenti alternative:

- o $\{h = 0\}$ è un insieme di punti isolati;
- o h è identicamente nulla.

Esaminiremo ora in dettaglio cosa succede nei due casi dell'Osservazione 3.6 e in particolare come possiamo estendere il campo K in modo da includere g.

Definizione 3.7. Sia K un campo di funzioni su un intervallo I e $f : I \to \mathbb{C}$ una funzione che soddisfa (M) ma non appartiene a K. Distinguiamo due casi:

(A) C'è un polinomio $P \in K[X]$ tale che $h := P(f)$ è identicamente nulla (in altre parole f è uno zero del polinomio P). In tal caso diciamo che f è *algebrica* su K. Da argomenti classici sappiamo che esiste un polinomio irriducibile di

grado $m > 1$ di cui f è uno zero (si veda ad esempio [6]). Definiamo allora il campo $K(f)$ come

$$K(f) = \{Q(f) : Q \in K[X] \quad \text{ha grado} \leq m-1\} .$$

(T) Non c'è alcun polinomio come in (A). In tal caso diciamo che f è *trascendente* su K e definiamo il campo

$$K(f) = \left\{ \frac{P(f)}{Q(f)} : P, Q \in K[X] \quad \text{sono polinomi primi tra loro} \right\} .$$

Nel seguito si darà spesso il caso che il "dominio" di definizione del campo K non coincida con quello di f: ci troveremo sempre però in situazioni in cui i due domini si intersecano e quindi, a patto di restringere sia f sia gli elementi di K a un intervallo comune, potremo procedere come sopra.

Che $K(f)$ sia un campo, nel secondo caso è ovvio. Nel primo caso viene dal "solito trucco" che si incontra agli inizi della Teoria di Galois. Supponiamo infatti che P sia un polinomio irriducibile di cui f è uno zero e sia m il suo grado. È chiaro che $K(f)$ è chiuso per quanto riguarda la somma. Per quanto riguarda il prodotto, basta osservare che se $a = bc$ e $b, c \in K(f)$ allora $a = Q(f)$ per qualche polinomio $Q \in K[X]$. Se il grado di Q è maggiore di $m-1$ possiamo usare l'algoritmo euclideo di divisione tra polinomi a coefficienti in un campo (si veda [6]) per scrivere $Q = Q_1 P + R$, dove $R \in K[X]$ è un polinomio di grado minore di m. Visto che $P(f) = 0$ otteniamo allora $Q(f) = R(f)$ e quindi concludiamo che $a \in K(f)$. Dobbiamo ora far vedere che per ogni elemento di $K(f)$ che non sia identicamente nullo, $K(f)$ contiene il suo reciproco. L'argomento usa un'identità potente che sarà nominata spesso in seguito. Consideriamo un elemento non nullo $a \in K(f)$. Allora $a = Q(f)$ per qualche polinomio $Q \in K[X]$ di grado al più $m-1$ che non è il polinomio identicamente nullo. P non può dividere Q perché il grado di Q è minore. Essendo P irriducibile ne segue che P e Q sono primi tra loro. Possiamo allora invocare l'identità di Bézout e affermare l'esistenza di polinomi $R, S \in K[X]$ tali che

$$PR + QS = 1$$

(si veda ad esempio la Sezione 3.9 di [6]). Visto che $P(f) = 0$, ne concludiamo che $aS(f) = Q(f)S(f) = 1$. Ma $S(f)$ è un elemento di $K(f)$ e pertanto il reciproco di a appartiene a $K(f)$.

In generale i campi costruiti nella Definizione 3.7 non sono necessariamente campi differenziali, anche nel caso che lo sia K. O meglio, come vedremo sotto, se K è un campo differenziale, le sue estensioni algebriche sono sempre dei campi differenziali, ma quelle trascendenti in generale no. Lo sono però due particolari classi di estensioni trascendenti, che poi sono le uniche di cui ci occuperemo nel resto di questa nota.

Definizione 3.8. Sia K un campo differenziale di funzioni su un intervallo I. Una funzione f definita su un intervallo $J \subset I$ e che soddisfa (M) è

- un *logaritmo* su K se esiste un elemento g di K che è definito ovunque su J, non si annulla mai (su J) e tale che $f' = g'/g$;
- un *esponenziale* su K se esiste un elemento g di K che è definito ovunque su J e tale che $f' = g'f$.

Ovviamente, segue dalla definizione che, a meno delle solite costanti e della multivocità del logaritmo complesso, nei due casi di sopra g è effettivamente il logaritmo – più propriamente **un** logaritmo, visto che abbiamo a che fare con valori complessi – o l'esponenziale di f. In particolare

- se g è definito ovunque su J, allora $J \ni x \mapsto e^{g(x)}$ soddisfa (M) ed è un esponenziale su K;
- e se g in aggiunta non si annulla su J, a patto di scegliere una determinazione log del logaritmo complesso, $J \ni x \mapsto \log(g(x))$ soddisfa (M) ed è un logaritmo su K.

Il seguente lemma ci garantisce che le tre speciali estensioni di campo di cui d'ora in poi ci occuperemo, ovvero ottenute attraverso l'aggiunta di elementi algebrici, logaritmi o esponenziali, sono sempre estensioni differenziali.

Lemma 3.9. *Sia K un campo differenziale di funzioni e f un elemento non appartenente a K che è o algebrico o un logaritmo o un esponenziale su K. Allora $K(f)$ è un campo differenziale di funzioni.*

DIMOSTRAZIONE. Viste le regole (D1) e (D2) è ovvio che dobbiamo solo controllare che f' appartenga a $K(f)$. Per esponenziali e logaritmi questo è ovvio. Dobbiamo quindi solo controllare il caso algebrico. Consideriamo un polinomio $P \in K[X]$ di grado minimo di cui f è uno zero. Scriviamo allora

$$P = \sum_{j=0}^{m} a_j X^j \qquad \text{con } a_0, \dots a_m \in K\,.$$

Notiamo che $P(f) = 0$. Differenziando questa identità troviamo

$$f' \sum_{j=1}^{m} j a_j f^{j-1} = -\sum_{j=0}^{m} a_j' f^j \tag{3.4}$$

Se definiamo il polinomio $Q = \sum_{j=1}^{m} j a_j X^{j-1}$, osserviamo che questo polinomio non può essere nullo: il grado di P è almeno 2, altrimenti f apparterrebbe al campo K. Quindi il grado di Q è $m - 1 \geq 1$: pertanto $Q(f)$ è un elemento di $K(f)$ non banale (invertibile). Ma anche il membro sinistro di (3.4) è un elemento di $K(f)$. Dividendo entrambi i membri di (3.4) per $Q(f)$ otteniamo allora una formula per f' che mostra come f' sia effettivamente un elemento di $K(f)$.

Siamo ora pronti per definire le funzioni "elementari".

Definizione 3.10. Un campo differenziale di funzioni L è detto un'*estensione elementare* di un campo differenziale di funzioni K se esiste una successione finita di funzioni $f_1, \dots, f_N$ e di campi $K_0, K_1, \dots, K_N$ tali che

- $K_0 = K$ e $K_N = L$;
- per ogni $i \leq N-1$, $K_{i+1} = K_i(f_{i+1})$ e f_{i+1} è algebrica o un logaritmo o un esponenziale su K_i.

Il campo L verrà allora indicato con il simbolo $K(f_1, \dots, f_N)$. Una funzione f è *elementare* se appartiene a un'estensione elementare del campo delle funzioni razionali $\mathbb{C}(x)$.

Ovvero, una funzione è elementare se ottenuta aggiungendo un numero finito di funzioni algebriche o logaritmi o esponenziali alle funzioni razionali e chiudendo il nuovo insieme di funzioni rispetto alle operazioni di somma e prodotto. Ad esempio e^{e^x} è elementare (due estensioni esponenziali di $\mathbb{C}(x)$!), così come $\sqrt{\log x}$ (un'estensione logaritmica seguita da una algebrica).

Osservazione 3.11. Stiamo volutamente ignorando i domini di definizione per non appesantire il discorso. Ad esempio per la seconda funzione potremmo dare, come è naturale, un qualsiasi intervallo $J \subset]1, \infty[$. Ma potremmo anche usare un intervallo di $]0, 1[$: dovremmo estrarre la radice di un numero negativo e potremmo decidere di definirla come $i\sqrt{|\cdot|}$, con la convezione che $\sqrt{}$ ci dà un numero positivo. Entrambe le scelte sono legittime se ci accordiamo sul chiamare *estrazione di radice* una qualsiasi funzione $x \mapsto f(x)$ definita su un intervallo I, che rispetti la condizione (M) e tale che, per ogni $x \in I$, $f(x)$ sia uno zero del polinomio $P(X) = X^2 - x$ (che è un elemento irriducibile di $K[X]$ se scegliamo $K = \mathbb{C}(x)$). L'importante è che l'intervallo I di definizione non contenga lo 0: se lo includiamo non c'è modo di trovare una funzione che rispetti tutti questi requisiti ((M) è decisivo!).

Attenzione: abbiamo battezzato come elementari tante funzioni che proprio "elementari" non sono. Prendiamo ad esempio un polinomio P di quinto grado a coefficienti in $K = \mathbb{C}(x)$ non costanti. Questo avrà la forma

$$P(X) = \sum_{j=0}^{5} f_j X^j \,.$$

Scegliamo un qualsiasi intervallo J su cui tutte le funzioni f_i siano definite. Per ogni $t \in J$ otteniamo un polinomio a coefficienti complessi $P_t := \sum_{j=0}^{5} f_j(t) X^j$. L'insieme dei punti $t \in J$ per cui questo polinomio non ha 5 radici distinte è discreto (è di nuovo una conseguenza dell'analisi complessa, si veda il Lemma 5.1 più avanti). Sia quindi t un qualsiasi punto in J per cui P_t ha 5 radici distinte. Allora (per il teorema della funzione implicita: rimandiamo di nuovo al Lemma

5.1 per la dimostrazione) in un intorno J' di t troviamo 5 distinte funzioni analitiche $g_1, \ldots, g_5$ della variabile t che risolvono $P_t(g_j(t)) = 0$ per ogni t. Ciascuna di queste funzioni è algebrica su $\mathbb{C}(x)$. Quindi ciascuna di esse è una funzione elementare secondo la Definizione 3.10. Ma come ben sappiamo dalla classica Teoria di Galois, le soluzioni di un generico polinomio di quinto grado non sono esprimibili per radicali. Se è pur vero che per *alcuni* polinomi di quinto grado le soluzioni per radicali esistono, si può dimostrare che le funzioni f_i possono essere scelte in modo che i polinomi P_t non siano in questa classe. Le funzioni $g_1, \ldots, g_5$ non si potranno allora esprimere, in genere, come radicali di funzioni razionali.

4. Il teorema di Liouville e la primitiva di e^{x^2}

Siamo ora pronti per enunciare il teorema fondamentale di Liouville.

Teorema 4.1 (Teorema di Liouville). *Siano K un campo differenziale di funzioni e α un elemento di K. Se esiste un'estensione elementare L di K con un elemento y tale che $y' = \alpha$ allora esistono elementi $u_1, \ldots, u_n, v \in K$ e costanti $c_1, \ldots, c_n \in \mathbb{C}$ tali che*

$$\alpha = \sum_{j=1}^{n} c_j \frac{u_j'}{u_j} + v' \,, \tag{4.1}$$

e viceversa.

Il teorema di Liouville è profondo e sorprendente. L'esistenza di una primitiva in una qualsiasi estensione elementare L (ovvero un oggetto "esterno" al campo K che può essere costruito in una miriade di modi) è ridotto a un'identità, la (4.1), in cui tutti i termini in gioco sono elementi del campo originale K!

Osservazione 4.2. Notiamo che il "viceversa" è relativamente semplice. Supponiamo infatti che $\alpha, u_1, \ldots, u_n, v \in K$ e $c_1, \ldots, c_n \in \mathbb{C}$ soddisfino (4.1) e assumiamo, senza perdita di generalità, che non esista alcun elemento a di K tale che $\frac{u_j'}{u_j} = a'$ per qualche j. A patto di restringere l'intervallo I di definizione delle nostre funzioni, possiamo supporre che nessuno degli elementi u_j si annulli su I. Ma allora possiamo scegliere una determinazione log del logaritmo complesso e porre $a_j := \log u_j$. Ne segue che $L = K(a_1, \ldots, a_N)$ è un'estensione elementare di K (stiamo assumendo che $a_j \notin K(a_1, \ldots, a_{j-1})$... ma d'altra parte se così non fosse, tanto meglio: dovremo solo "estendere meno" il campo K). Inoltre è ovvio che $y := \sum_j c_j a_j + v$ è un elemento di L: differenziando otteniamo allora $y' = \sum_j c_j a_j + v = \sum_j c_j \frac{u_j'}{u_j} + v'$ e concludiamo da (4.1) che $y' = \alpha$.

La precedente osservazione ci dà un'informazione estremamente interessante: aggiungere elementi algebrici o esponenziali su K **non ci è di alcun aiuto** nel trovare una primitiva che non era già in K. L'unica speranza è che basti aggiungere un numero finito di logaritmi.

La dimostrazione del Teorema di Liouville ci costerà la maggior parte dello sforzo nelle prossime pagine. Con (relativamente) meno fatica dedurremo da esso la seguente

Proposizione 4.3. *Siano $f, g \in \mathbb{C}(x)$ tali che g non sia costante e f sia non nulla. Allora la funzione $x \mapsto f(x)e^{g(x)}$ ha una primitiva elementare (su un qualche intervallo J in cui entrambe f e g sono ovunque definite) se e solo se esiste $a \in \mathbb{C}(x)$ tale che $f = a' + ag'$.*

Da questa proposizione deriveremo tra breve il nostro agognato corollario. Prima però è utile commentarla, per farcela un po' amica. Una direzione è assolutamente ovvia. Supponiamo che ci sia $a \in \mathbb{C}(x)$, ovvero una funzione razionale a, tale che $f = a' + ag'$. Allora la funzione $x \mapsto h(x) = a(x)e^{g(x)}$ è ovviamente una funzione elementare, perché $\xi := e^g$ è un esponenziale su $K = \mathbb{C}(x)$ e $h \in K(\xi)$. D'altra parte è un gioco da ragazzi derivare h e vedere che $h' = (a' + ag')e^g = fe^g$. La parte interessante della Proposizione è quindi l'implicazione inversa, ovvero il fatto che se una primitiva elementare esiste, allora (a meno di costanti) è necessariamente della forma ae^g, dove a è una *funzione razionale*. Il succo è tutto in questa informazione aggiuntiva, ovvero la razionalità di a! Altrimenti l'esistenza di una funzione regolare a che soddisfi l'equazione differenziale $a' + ag' = f$ (dove f e g' sono funzioni "note") è garantita da un qualsiasi testo di Analisi, si veda ad esempio il Capitolo 7.1 di [1]. Abbiamo anche una bella formula per a ... che però presuppone il calcolo di integrali che ovviamente coinvolgono la funzione fe^g (si veda (7.20) in [1]): in quanto a decidere se la soluzione è razionale siamo da capo a dodici, come si dice dalle mie parti.

Notiamo anche che la proposizione è piuttosto intuitiva: ci dice in pratica che c'è poco da guadagnare nell'inserire altre funzioni elementari in gioco, siano esse trascendenti o algebriche, quando tentiamo di "primitivare" fe^g: o funziona qualcosa della forma ae^g con a razionale o non c'è trippa per gatti. Tutti quelli che hanno perso un po' del loro tempo a "cercare" la primitiva di e^{x^2} hanno fatto proprio questa esperienza.

Ci accontentiamo di finire questa sezione con la parte facile: grazie alla Proposizione 4.3 mostreremo il

Corollario 4.4. *Non c'è una funzione elementare f definita su un intervallo J tale che $f'(x) = e^{x^2}$.*

DIMOSTRAZIONE. Vista la Proposizione 4.3, il nostro obiettivo è negare l'esistenza di una funzione razionale $a = \frac{P}{Q}$ tale che $a' + ag' = f$. Ovviamente P e Q sono due polinomi a coefficienti complessi, che assumiamo primi tra loro. Visto che $g(x) = x^2$ e $f(x) = 1$ l'identità che essi risolverebbero sarebbe

$$\frac{P'(x)Q(x) - Q'(x)P(x)}{Q(x)^2} + \frac{2xP(x)}{Q(x)} = 1\,,$$

che è equivalente a

$$P'(x)Q(x) - Q'(x)P(x) + 2xP(x)Q(x) = Q(x)^2\,. \tag{4.2}$$

Ovviamente la Proposizione 4.3 ci direbbe che quest'ultima identità deve essere soddisfatta solo su J. D'altra parte, trattandosi di polinomi, l'identità è soddisfatta su un intervallo non banale se e solo se è soddisfatta **ovunque**. Supponendo allora l'esistenza di due polinomi che soddisfino (4.2) ne concluderemmo che Q divide il polinomio $Q'P$. Visto però che Q e P sono primi tra loro, Q dovrebbe dividere Q'. D'altra parte questo implicherebbe che il grado di Q' sia almeno quello di Q e ciò sarebbe possibile solo se Q fosse un polinomio costante. Per il momento non c'è niente di male: vuol solo dire che una funzione razionale a non ha chances di risolvere $a' + ag' = f$ a meno che non sia un polinomio P. L'identità (4.2) diverrebbe allora

$$P'(x) + 2xP(x) = 1$$

ovvero $2xP(x) = 1 - P'(x)$. È ovvio però che nessun polinomio soddisfa quest'ultima uguaglianza: se P ha grado m, allora il grado del membro sinistro è necessariamente $m + 1$, salvo quando P è identicamente nullo. D'altra parte il grado del membro destro non è mai maggiore di m. Rimarrebbe da esaminare il caso banale $P = 0$, che ovviamente non dà una soluzione. Ne concludiamo che una soluzione *razionale* a di $a' + ag' = f$ non esiste. Pertanto, grazie alla Proposizione 4.3, non c'è una funzione elementare definita su un intervallo J tale che $f'(x) = e^{x^2}$.

Osservazione 4.5. È facile vedere che non cambia nulla se al posto di e^{x^2} prendiamo la sua "sorella" più famosa e^{-x^2}, ovvero la Gaussiana: il Corollario 4.4 è un fatto puramente algebrico, come era lecito aspettarsi. Pertanto le proprietà che rendono $x \mapsto e^{-x^2}$ "migliore" di $x \mapsto e^{x^2}$ come funzione *di variabile reale* (ad esempio le proprietà di decadimento a $\pm\infty$) non giocano alcun ruolo nel nostro caso.

5. Alcuni strumenti algebrici

Nel resto di questa nota ci occuperemo delle dimostrazioni del Teorema 4.1 e della Proposizione 4.3. Avremo però bisogno di alcuni importanti strumenti algebrici, che raccoglieremo (e giustificheremo) in questa sezione.

5.1. Esistenza delle radici di un polinomio

Consideriamo un campo di funzioni K – ovviamente i campi che ci interessano veramente sono quelli differenziali, ma in questo capitoletto possiamo lavorare con molta più generalità – e un polinomio irriducibile $P \in K[X]$ di grado m. Ci aspettiamo allora l'esistenza di m radici distinte in una opportuna estensione del campo K. Questo è vero per un teorema generale che garantisce l'esistenza di una chiusura algebrica per qualsiasi campo (si veda ad esempio le p. 11-12 di [2]). Tuttavia vogliamo mostrare qui che è possibile trovare m radici distinte in una estensione che è a sua volta un campo di funzioni in accordo con le definizioni di

questa nota, senza scomodare grossi risultati dell'algebra astratta. Dovremo però scomodare qualche risultato di analisi complessa classica – ma, si sa, è difficile ottenere qualcosa di interessante senza un po' di fatica! Il lettore interessato alle idee p rincipali che si nascondono dietro al Teorema di Liouville può saltare la dimostrazione, che è un po' tecnica e ha poco a che fare con il resto.

Lemma 5.1. *Consideriamo un campo di funzioni K definite su un intervallo I e un polinomio $P \in K[X]$ irriducibile di grado m. Allora esistono un sottointervallo $J \subset I$ e m funzioni distinte $f_i : I \to \mathbb{C}$ che soddisfano (M) e tali che $P(f_i) = 0$ per ogni i.*

DIMOSTRAZIONE. Ricordiamo il seguente risultato. Sia $P(x) = \sum_{j=0}^{m} c_j x^j$ un polinomio monico a coefficienti complessi che ha m radici distinte

$$z_1, \dots, z_m \in \mathbb{C}\,.$$

Allora esistono m funzioni olomorfe $\zeta_1, \dots, \zeta_m : \mathbb{C}^m \supset U \to \mathbb{C}$ definite in un intorno U di $(c_0, \dots, c_{m-1})$ tali che, per ogni i,

- $\zeta_i(a_0, \dots, a_{m-1})$ è uno zero del polinomio $x^m + a_{m-1}x^{m-1} + \dots + a_0$ per ogni $(a_0, \dots, a_{m-1}) \in U$;
- $\zeta_i(c_0, \dots, c_{m-1}) = z_i$.

L'asserzione è un risultato diretto del teorema della funzione implicita per funzioni olomorfe. Infatti l'esistenza di m radici distinte è equivalente al fatto che la derivata $P'(x) := \sum_{j=1}^{m} j c_j x^{j-1}$ non si annulla in nessuno dei punti $z_1, \dots, z_m$. Se introduciamo la funzione olomorfa di $m+1$ variabili complesse $\mathcal{P}(x, a_0, \dots, a_{m-1}) = x^m + a_{m-1}x^{m-1} + \dots + a_0$, ne concludiamo allora che

$$\frac{\partial \mathcal{P}}{\partial x}(z_i, a_0, \dots, a_{m-1}) \neq 0 \qquad \forall i$$

e possiamo quindi applicare il teorema della funzione implicita (si veda ad esempio la p. 19 in [4]).

Veniamo ora alle funzioni f_i. Innanzitutto scriviamo $P(X) = \sum_{j=0}^{m} g_j X^j$. Restringendo l'intervallo I di definizione possiamo supporre, senza perdita di generalità, che le funzioni g_j siano tutte definite su I e che la g_m non si annulli mai su I (ricordiamo che le g_j soddisfano (M)). Dividendo per g_m possiamo allora suppore che g_m sia identicamente 1. Per ogni t consideriamo il polinomio $P_t(x) := \sum_{j=0}^{m} g_j(t) x^j$, che è un onesto polinomio monico a coefficienti complessi. Cerchiamo ora un punto $t_0 \in I$ tale che $P_{t_0}(x)$ abbia m radici distinte $z_1, \dots, z_m$. Se lo troviamo, possiamo usare le funzioni ζ_i di cui sopra e, in un intorno di t_0, definire le nostre funzioni f_i come

$$f_i(t) = \zeta_i(g_0(t), \dots, g_{m-1}(t))\,.$$

La condizione (M) è semplice da verificare (in effetti le f_i posseggono un prolungamento *olomorfo* a un intorno complesso di I).

Per trovare il punto t_0 consideriamo il polinomio $P'(X) := \sum_{j=1}^{m} j g_j X^{j-1}$. Essendo P un polinomio irriducibile, P' e P sono primi tra loro e l'identità di Bézout ci garantisce l'esistenza di due polinomi $Q, R \in K[X]$ tali che

$$QP + RP' = 1\,. \tag{5.1}$$

I coefficienti dei polinomi Q e R sono un numero finito di elementi di K, che quindi soddisfano (M). A patto di restringerci a un sottointervallo di I possiamo allora supporre che queste funzioni siano definite per ogni valore t di I. Per ogni t costruiamo i polinomi $P_t', Q_t, R_t \in \mathbb{C}[x]$ alla stregua di P_t. L'identità di Bézout diventa allora l'identità $Q_t P_t + R_t P_t' = 1$ per tali polinomi a coefficienti complessi. Questo ci mostra che P_t e P_t' sono primi tra loro. D'altra parte P_t' è proprio la derivata del polinomio P_t: ne concludiamo allora che questi due polinomi non hanno radici in comune, che è equivalente al fatto che P_t abbia m radici distinte.

5.2. Un'osservazione innocente

Consideriamo ora due estensioni algebriche $K(f_1)$ e $K(f_2)$ dello stesso campo differenziale di funzioni K e supponiamo che f_1 e f_2 siano due soluzioni dello stesso polinomio irriducibile $P \in K[X]$ di grado m. Si può facilmente verificare che i campi $K(f_1)$ e $K(f_2)$ sono isomorfi come campi differenziali, nel seguente senso. Ricordiamo che ciascun elemento a in $K(f_1)$ ha una rappresentazione unica come $a = Q(f_1)$, dove $Q \in K[X]$ è un polinomio di grado minore di m. Definiamo allora la mappa $\pi : K(f_1) \to K(f_2)$ ponendo $\pi(a) = Q(f_2)$. Non è difficile vedere che

(O1) π è iniettiva e surgettiva;

(O2) π è un omomorfismo di campo, ovvero $\pi(ab) = \pi(a)\pi(b)$ e $\pi(a+b) = \pi(a) + \pi(b)$ per ogni coppia di elementi $a, b \in K(f_1)$;

(O3) π commuta con la derivata, ovvero $\pi(a)' = \pi(a')$ per ogni $a \in K(f_1)$;

(O4) π è l'identità sugli elementi di K.

Questa osservazione apparentemente innocente è foriera di tante conseguenze. In particolare ne deriviamo il seguente potente principio.

Lemma 5.2 (Principio di sostituzione). *Sia K un campo differenziale di funzioni e siano f_1 e f_2 due elementi algebrici su K che sono radici dello stesso polinomio irriducibile. Se abbiamo un'identità del tipo*

$$\alpha = \mathcal{E}(f_1, f_1')\,, \tag{5.2}$$

dove $\mathcal{E}(X, Y)$ è un polinomio in due variabili a coefficienti in K e α è un elemento di K, allora vale anche

$$\alpha = \mathcal{E}(f_2, f_2')\,. \tag{5.3}$$

DIMOSTRAZIONE. L'argomento è estremamente semplice. Applichiamo la mappa π sia a destra che a sinistra di (5.2). Usando le proprietà (On) otteniamo:

$$\alpha \overset{(O4)}{=} \pi(\alpha) = \pi\left(\mathcal{E}(f_1, f_1)\right) \overset{(O2)}{=} \mathcal{E}\left(\pi(f_1), \pi(f_1')\right) \overset{(O3)}{=} \mathcal{E}(f_2, f_2')\,.$$

5.3. Funzioni simmetriche delle radici

Un fatto che gioca un ruolo assolutamente primario nella Teoria di Galois è la semplice osservazione che se valutiamo delle funzioni simmetriche sulle radici di un polinomio allora otteniamo delle funzioni dei coefficienti del polinomio. Prendiamo ad esempio il polinomio $P(X) = X^m + c_{m-1}X^{m-1} + \ldots + c_1X + c_0$ e assumiamo per semplicità che abbia m radici distinte $z_1, \ldots, z_m$. Come è noto il coefficiente c_j è la somma di tutti i possibili prodotti di $m - j$ radici distinte (tali espressioni vengono chiamate *funzioni simmetriche elementari di m variabili*). Pertanto $z_1 + \ldots + z_m = c_{m-1}$ e, ad esempio,

$$z_1^2 + z_2^2 + \ldots + z_m^2 = (z_1 + \ldots + z_m)^2 - 2\sum_{i<j} z_i z_j = c_{m-1}^2 - c_{m-2}\,.$$

Con simili argomenti non è difficile dimostrare il seguente lemma (si veda ad esempio la Sezione 5.6 in [6]).

Lemma 5.3. *Siano K un campo e $P \in K[X]$ un polinomio della forma $P(x) = x^m + c_{m-1}X^{m-1} + \ldots + c_1X + c_0$ con m radici distinte $\omega_1, \ldots, \omega_m$ in un campo $L \supset K$. Se $\mathcal{P}$ è un polinomio simmetrico in m variabili a coefficienti in K, allora $\mathcal{P}(\omega_1, \ldots, \omega_m)$ è un elemento di K.*

5.4. Espansione in frazioni parziali

Un ultimo strumento puramente algebrico che useremo frequentemente è l'espansione di una funzione razionale a coefficienti in un campo K in frazioni parziali. Non si tratta di altro che di una generalizzazione del solito procedimento di espansione in fratti semplici utilizzato per trovare la primitiva di una funzione razionale.

Cominciamo con il fissare un campo K e scegliere una funzione razionale $\xi \in K(X)$. Possiamo allora rappresentare ξ come il rapporto di due polinomi $P, Q \in K[X]$ primi tra loro. Supponiamo che sia Q il denominatore e scomponiamolo in fattori irriducibili:

$$Q = P_1^{k_1} \cdot P_2^{k_2} \cdot \ldots \cdot P_N^{k_N}\,.$$

In particolare, $P_1^{k_1}$ e $\tilde{Q} = P_2^{k2} \cdot \ldots \cdot P_N^{k_N}$ sono primi tra loro. Allora dall'identità di Bézout sappiamo che esistono due polinomi R e S tali che $RP_1^{k_1} + S\tilde{Q} = 1$. Scriviamo pertanto

$$\xi = \frac{P}{Q} = \frac{P(RP_1^{k_1} + S\tilde{Q})}{P_1^{k_1}\tilde{Q}} = \frac{PR}{\tilde{Q}} + \frac{PS}{P_1^{k_1}}\,.$$

Cosa ci abbiamo guadagnato? Abbiamo ottenuto due funzioni razionali in cui un denominatore è una potenza di un polinomio irriducibile, mentre l'altro denominatore ha un fattore in meno, rispetto a Q, nella sua scomposizione. Applicando altre $N-1$ volte questo procedimento otteniamo allora una scrittura del tipo

$$\xi = \sum_{j=1}^{N} \frac{R_j}{P_j^{k_j}} \tag{5.4}$$

dove ciascun polinomio P_j è irriducibile. Esaminiamo più in dettaglio ciascun addendo della somma in (5.4). Se il grado di R_j è maggiore o uguale al grado m_j di P_j possiamo usare l'algoritmo euclideo di divisione per scrivere $R_j = Q_j P_j + S_j$, dove S_j è un polinomio di grado minore di m_j. Come risultato otteniamo

$$\frac{R_j}{P_j^{k_j}} = \frac{Q_j}{P_j^{k_j-1}} + \frac{S_j}{P_j^{k_j}}\,.$$

Procedendo, in un numero finito di passi arriviamo a un'identità della forma

$$\frac{R_j}{P_j^{k_j}} = S_{0,j} + \sum_{l=1}^{k_j} \frac{S_{l,j}}{P_j^l}$$

dove, per $l \geq 1$, ciascun polinomio $S_{l,j}$ con $l \geq 1$ ha grado minore di m_j. Possiamo inoltre supporre che ciascun polinomio P_j sia monico.

Riassumendo il nostro discorso abbiamo ottenuto la seguente

Proposizione 5.4 (Espansione in frazioni parziali). *Sia K un campo. Per ogni funzione razionale $\xi \in K(X)$ esistono:*

- *N polinomi* distinti *monici irriducibili $P_1, \dots P_N \in K[X]$ di grado, rispettivamente, $m_1, \dots, m_N$;*
- *polinomi $S_{l,j}$ di grado minore di m_j, per $j \in \{1, \dots, N\}$ e $l \in \{1, \dots, m_j\}$;*
- *un polinomio S_0*

tali che valga l'identità

$$\xi = S_0 + \sum_{j=1}^{N} \sum_{l=1}^{m_j} \frac{S_{l,j}}{P_j^l}\,. \tag{5.5}$$

6. Dimostrazione del Teorema 4.1

Abbiamo ora tutti gli strumenti per affrontare il compito più arduo, ovvero la dimostrazione del risultato fondamentale di Liouville. Nell'Osservazione 4.2 abbiamo già esaminato la parte facile. Ci interessa ora mostrare che (4.1) è una condizione *necessaria* per l'esistenza di una primitiva di α in un'estensione elementare.

6.1. Induzione

Vogliamo dimostrare l'asserzione per una qualsiasi estensione elementare L di un qualsiasi campo differenziale K di funzioni. L sarà allora della forma $K(f_1, \dots, f_N)$. Il risultato verrà dimostrato per induzione su N. Il passo iniziale è ovvio: se $N = 0$, allora $L = K$ e α ha una primitiva in $L = K$ se e solo se esiste $v \in K$ tale che $\alpha = v'$. Ci occuperemo ora del passo induttivo. Supponiamo quindi che il teorema sia vero per ogni campo differenziale di funzioni $\mathcal{K}$ e ogni estensione elementare della forma $\mathcal{L} = \mathcal{K}(g_1, \dots, g_{N-1})$. Dato un qualsivoglia campo differenziale di funzioni K mostreremo che il teorema è vero per ogni estensione elementare della forma $L = K(f_1, \dots, f_N)$. Prendiamo allora un arbitrario $\alpha \in K$ per il quale esiste un $y \in L$ tale che $\alpha = y'$. Consideriamo ora $\mathcal{K} = K(f_1)$ e notiamo che $L = \mathcal{K}(f_2, \dots, f_N)$. D'altra parte $\alpha \in \mathcal{K}$ e $y \in L$ è un elemento tale che $y' = \alpha$. Possiamo allora utilizzare l'ipotesi induttiva e concludere l'esi stenza di elementi $\zeta_1, \dots, \zeta_n, \xi \in \mathcal{K} = K(f_1)$ e $c_1, \dots, c_n \in \mathbb{C}$ tali che

$$\alpha = \sum_{j=1}^{n} c_j \frac{\zeta_j'}{\zeta_j} + \xi' \,. \tag{6.1}$$

Il nostro obiettivo, ovvero la (4.1), differisce però dalla (6.1) perché gli ζ_j e lo ξ sono elementi di $K(f_1)$ e non di K (come nella (4.1)). Nel resto della dimostrazione lo scopo sarà derivare dalla (6.1) una scrittura analoga dove al posto degli elementi ζ_j e ξ ci siano degli elementi di K. Va però notato che **non** dimostreremo che gli ζ_j e lo ξ sono elementi di K, **né** che le costanti della (4.1) sono le stesse della (6.1): vedremo in generale che per passare da (6.1) a (4.1) avremo bisogno di manipolare l'identità (6.1) in modo piuttosto complesso. Tra l'altro utilizzeremo tre diversi argomenti a seconda delle tre possibilità seguenti:

- f_1 è algebrico su K;
- f_1 è un logaritmo su K e **non è** algebrico;
- f_1 è un esponenziale su K e **non è** algebrico.

Tuttavia la dimostrazione del passo induttivo negli ultimi due casi differisce solo per alcuni dettagli tecnici, ma non nella strategia generale.

6.2. Il caso algebrico

In questo caso sappiamo che ciascun elemento ζ_j è del tipo $P_j(f_1)$, mentre $\xi = Q(f_1)$, dove $P_1, \dots, P_n, Q$ sono polinomi in $K[X]$. Infatti, visto che il reciproco di ciascun ζ_j è anche un elemento di $K(f_1)$, anch'esso è della forma $R_j(f_1)$ per qualche polinomio $R_j \in K[X]$. Possiamo allora riscrivere (6.1) come

$$\alpha = \sum_{j=1}^{n} c_j (P_j(f_1))' R_j(f_1) + (Q(f_1))' \,. \tag{6.2}$$

Sia ora $P \in K[X]$ un polinomio irriducibile monico di cui f_1 è uno zero e sia m il suo grado. Usando il Lemma 5.1 possiamo supporre (a patto di restringere il dominio di f_1 e delle funzioni di K) che P abbia m radici distinte $\omega_1, \ldots, \omega_m$ che soddisfano (M). Una di queste radici è ovviamente f_1 (un polinomio di grado m non può avere più di m radici!). Calcolando le derivate usando la regola di Leibniz e la linearità, è facile vedere che il membro destro di (6.2) è della forma $\mathcal{E}(f_1, f_1')$, dove $\mathcal{E}$ è un polinomio di due variabili a coefficienti in K. Possiamo quindi applicare il principio di sostituzione del Lemma 5.2 e concludere che vale l'identità

$$\alpha = \sum_{j=1}^{n} c_j (P_j(\omega_k))' R_j(\omega_k) + (Q(\omega_k))' \tag{6.3}$$

per ogni k. Sommiamo quindi la (6.2) su k per ottenere

$$\begin{aligned} \alpha &= \frac{1}{m} \sum_{k=1}^{m} \left(\sum_{j=1}^{n} c_j (P_j(\omega_k))' R_j(\omega_k) + (Q(\omega_k))' \right) \\ &= \frac{1}{m} \sum_{j=1}^{n} \sum_{k=1}^{m} \frac{(P_j(\omega_k))'}{P_j(\omega_k)} + \frac{1}{m} \left(\sum_{k=1}^{m} Q(\omega_k) \right)' . \end{aligned} \tag{6.4}$$

Facciamo ora una piccola digressione per notare che, presi due qualsiasi elementi non nulli a e b di un campo differenziale K, abbiamo l'identità

$$\frac{(ab)'}{ab} = \frac{a'}{a} + \frac{b'}{b} . \tag{6.5}$$

È ovviamente quello che ci aspettiamo dalla derivata logaritmica! Ovvero

$$\frac{(ab)'}{ab} = (\log(ab))' = (\log a)' + (\log b)' = \frac{a'}{a} + \frac{b'}{b} . \tag{6.6}$$

D'altra parte la giustificazione rigorosa del calcolo (6.6) non richiede l'introduzione dei logaritmi. È valida in un qualsiasi campo differenziale ed è molto semplice mostrarlo con la regola di Leibniz:

$$\frac{(ab)'}{ab} = \frac{a'b + ab'}{ab} = \frac{a'}{a} + \frac{b'}{b} .$$

Ovviamente, la (6.5) è facilmente generalizzabile a

$$\frac{(a_1 a_2 \ldots a_N)'}{a_1 a_2 \ldots a_N} = \frac{a_1'}{a_1} + \ldots + \frac{a_N'}{a_N} .$$

Usando quest'ultima identità nella (6.4) otteniamo allora

$$\alpha = \frac{1}{m} \sum_{j=1}^{n} \frac{\left(P_j(\omega_1) P_j(\omega_2) \ldots P_j(\omega_m)\right)'}{P_j(\omega_1) P_j(\omega_2) \ldots P_j(\omega_m)} + \frac{1}{m} \left(\sum_{k=1}^{m} Q(\omega_k) \right)' . \tag{6.7}$$

Se introduciamo $\mathcal{P}_j(X_1, X_2, \ldots, X_m) = P_j(X_1) P_j(x_2) \ldots P_j(x_m)$, abbiamo ovviamente che $\mathcal{P}_j$ è un polinomio simmetrico a coefficienti in K. Possiamo allora applicare il Lemma 5.3 per concludere che ogni

$$u_j := P_j(\omega_1) P_j(\omega_2) \ldots P_j(\omega_m)$$

è in realtà un elemento di K. Per lo stesso motivo anche $v = \frac{1}{m}\sum_{k=1}^{m} Q(\omega_k)$ è un elemento di K. Concludiamo allora che

$$\alpha = \sum_{j=1}^{m} \frac{c_j}{m}\frac{u_j'}{u_j} + v' \,, \tag{6.8}$$

che era ovviamente il nostro obiettivo (ovvero la (4.1), a patto di cambiare i coefficienti costanti).

Osservazione 6.1. A rigor di logica, se il campo iniziale K era definito su un intervallo I, la f_1 potrebbe essere definita su un intervallo più piccolo e quindi (6.8) è stato dimostrato in un sottointervallo J di I. D'altra parte, $\beta := \alpha - \sum_j \frac{c_j}{m}\frac{u_j'}{u_j} - v'$ è un elemento di K e quindi soddisfa (M). Da (M2) o β ha un insieme discreto di zeri su I o è identicamente nulla. Visto che si annulla su J, allora deve essere identicamente nulla.

6.3. Il caso logaritmo

In questo caso sappiamo che ciascun elemento ζ_j in (6.1) è della forma $P_j(f_1)/Q_j(f_1)$ per dei polinomi $P_j, Q_j \in K(X)$ primi tra loro. Usando però (6.5) è semplice vedere che vale l'identità

$$\frac{\left(\frac{a}{b}\right)'}{\frac{a}{b}} = \frac{a'}{a} - \frac{b'}{b}\,.$$

Possiamo allora riscrivere la (6.1) come

$$\alpha = \sum_{j=1}^{n} c_j \frac{P_j(f_1))'}{P_j(f_1)} - \sum_{j=1}^{n} c_j \frac{Q_j(f_1))'}{Q_j(f_1)} + \xi' \,. \tag{6.9}$$

Andiamo oltre: ciascun polinomio P_j e ciascun Q_j può essere scomposto in fattori primi. Possiamo allora applicare (6.5) per riscrivere (6.9) come

$$\alpha = \sum_{j=1}^{N} \gamma_j \frac{(M_j(f_1))'}{M_j(f_1)} + \xi' \tag{6.10}$$

dove ciascun M_j è un polinomio irriducibile in $K[X]$ e $\gamma_j \in \mathbb{C}$. Facciamo un'ulteriore semplificazione: scriviamo $M_j = u_j R_j$, dove R_j è un polinomio monico e $u_j \in K$. Allora avremo

$$\alpha = \sum_{j=1}^{N} \gamma_j \frac{u_j'}{u_j} + \sum_{j=1}^{N} \gamma_j \frac{(R_j(f_1))'}{R_j(f_1)} + \xi' \,. \tag{6.11}$$

Accorpiamo ora tutti i termini uguali per ottenere

$$\alpha = \sum_{j=1}^{N} \gamma_j \frac{u_j'}{u_j} + \sum_{j=1}^{\tilde{N}} \lambda_j \frac{(R_j(f_1))'}{R_j(f_1)} + \xi' \,, \tag{6.12}$$

dove gli R_j sono tutti distinti.

Per ξ utilizziamo invece l'espansione in frazioni parziali data dalla Proposizione 5.4:

$$\xi = S_0(f_1) + \sum_{j=1}^{\bar{N}} \sum_{l=1}^{m_j} \frac{S_{l,j}(f_1)}{V_j^l(f_1)}\,. \tag{6.13}$$

Inserendo nella (6.12) e differenziando:

$$\begin{aligned}\alpha = &\sum_{j=1}^{N} \gamma_j \frac{u_j'}{u_j} + \sum_{j=1}^{\bar{N}} \lambda_j \frac{(R_j(f_1))'}{R_j(f_1)} + (S_0(f_1))' \\ &+ \sum_{j=1}^{\bar{N}} \sum_{l=1}^{m_j} \frac{(S_{l,j}(f_1))'}{V_j^l(f_1)} - \sum_{j=1}^{\bar{N}} \sum_{l=1}^{m_j} l \frac{S_{l,j}(f_1)(V_j(f_1))'}{V_j^{l+1}(f_1)}\end{aligned} \tag{6.14}$$

È ora venuto il momento di capire cosa succede quando differenziamo un elemento della forma $P(f_1)$ con $P \in K[X]$. Scriviamo

$$P(X) = a_m X^m + \ldots + a_0\,.$$

Allora otteniamo

$$(P(f_1))' = \sum_{j=1}^{m} j a_j f_1' f_1^{j-1} + \sum_{j=0}^{m} a_j' f_1^j\,.$$

Ricordiamo però che f_1 è un logaritmo su K, quindi esiste $b \in K$ tale che che $f_1 = b'/b$. Pertanto

$$(P(f_1))' = a_m' f_1^m + \sum_{j=0}^{m-1} \left((j+1) \frac{b'}{b} a_{j+1} + a_j' \right) f_1^j$$

Quindi $(P(f_1))'$ è della forma $Q(f_1)$ dove $Q \in K[X]$. Q ha grado m se a_m non è una costante. Se invece a_m è una costante α_m, allora il grado del polinomio è necessariamente $m-1$, altrimenti avremmo

$$\alpha_m m \frac{b'}{b} + a_{m-1}' = 0$$

ovvero $(\alpha_m m f_1 + a_{m-1})' = 0$, cioè $\alpha_m m f_1 + a_{m-1} \in \mathbb{C}$, che non è possibile perché f_1 non appartiene a K.

Allora concludiamo che in (6.14) tutte le derivate che appaiono possono essere rappresentate come $Q(f_1)$ per qualche polinomio in $K[X]$. Inoltre, le derivate $(R_j(f_1))'$ sono della forma $\tilde{R}_j(f_1)$ per dei polinomi $\tilde{R}_j \in K[X]$ di grado $\deg(\tilde{R}_j) = \deg(R_j) - 1$, perché R_j è monico. Analogamente, $(V_j(f_1))' = \tilde{V}_j(f_1)$ per un polinomio $\tilde{V}_j$ di grado $\deg(\tilde{V}_j) = \deg(V_j) - 1$.

Riscriviamo allora l'identità (6.14) come

$$\begin{aligned}\alpha = &\sum_{j=1}^{N} \gamma_j \frac{u_j'}{u_j} + \sum_{j=1}^{\bar{N}} \lambda_j \frac{\tilde{R}_j(f_1)}{R_j(f_1)} + \tilde{S}_0(f_1) \\ &+ \sum_{j=1}^{\bar{N}} \sum_{l=1}^{m_j} \frac{\tilde{S}_{l,j}(f_1)}{V_j^l(f_1)} - \sum_{j=1}^{\bar{N}} \sum_{l=1}^{m_j} l \frac{S_{l,j}(f_1)\tilde{V}_j(f_1)}{V_j^{l+1}(f_1)}\,.\end{aligned} \tag{6.15}$$

Vorremmo moltiplicare l'identità (6.14) per il minimo comune multiplo dei denominatori, in modo da ricondurci a un'identità polinomiale. Notiamo che, benché siamo sicuri che i V_j siano tutti distinti e gli R_j anche, può benissimo darsi che $R_j = V_k$ per qualche j e k. Denotiamo con $R_{j_1}, \dots, R_{j_s}$ quei polinomi R_j che non coincidono con alcun V_k. Allora il minimo comune multiplo dei denominatori è

$$M := V_1^{m_1+1} \dots V_{\tilde{N}}^{m_{\tilde{N}}+1} R_{j_1} \dots R_{j_s}\,.$$

Moltiplichiamo ambo i membri di (6.15) per $M(f_1)$ e spostiamo il membro destro dell'equazione risultante a sinistra in modo da ottenere un'identità del tipo

$$\mathcal{P}(f_1) = 0$$

dove $\mathcal{P}$ è un polinomio a coefficienti in K. Questo è possibile solo se $\mathcal{P}$ è il polinomio identicamente nullo, perché f_1 è trascendente. D'altra parte è facile vedere che possiamo scrivere:

$$\begin{aligned}\mathcal{P}(X) &= V_1^{m_1}(X)\mathcal{Q}(X)\\ &+ S_{m_1,1}(X)\tilde{V}_1(X)V_2^{m_2+1}(X)\dots V_{\tilde{N}}^{m_N+1}(X)R_{j_1}(X)\dots R_{j_l}(X)\end{aligned} \tag{6.16}$$

(il motivo per cui il primo addendo nella somma (6.16) ha solo un fattore $V_1^{m_1}$ e non il fattore $V_1^{m_1+1}$ è che un qualche R_j potrebbe coincidere con V_1!)

Ora, dalle nostre considerazioni segue che l'ultimo addendo di (6.16) è primo con il polinomio V_1. Ma allora $\mathcal{P}$ non sarebbe banale. Ne concludiamo perciò che le frazioni non sono presenti nella (6.13) e quindi abbiamo

$$\begin{aligned}\alpha &= \sum_{j=1}^{N}\gamma_j\frac{u_j'}{u_j} + \sum_{j=1}^{\tilde{N}}\lambda_j\frac{(R_j(f_1))'}{R_j(f_1)} + (S_0(f_1))'\\ &= \sum_{j=1}^{N}\gamma_j\frac{u_j'}{u_j} + \sum_{j=1}^{\tilde{N}}\lambda_j\frac{\tilde{R}_j(f_1)}{R_j(f_1)} + \tilde{S}_0(f_1)\,.\end{aligned} \tag{6.17}$$

D'altra parte possiamo usare di nuovo lo stesso argomento per concludere che non ci può essere nessuna frazione della forma $\frac{\tilde{R}_j(f_1)}{R_j(f_1)}$ in (6.17) e quindi che

$$\alpha = \sum_{j=1}^{N}\gamma_j\frac{u_j'}{u_j} + \tilde{S}_0(f_1)\,. \tag{6.18}$$

Applicando un'ultima volta la stessa idea concludiamo infine che $\tilde{S}_0$ deve essere un polinomio di grado 0. Ma visto che $\tilde{S}_0(f_1) = (S_0(f_1))'$ sappiamo che o S_0 è esso stesso un polinomio di grado 0, o è un polinomio di grado 1 della forma $c_0X + v$ con $c_0 \in \mathbb{C}\setminus\{0\}$. Allora possiamo in entrambi i casi scrivere

$$\alpha = \sum_{j=1}^{N}\gamma_j\frac{u_j'}{u_j} + c_0f_1' + v' \tag{6.19}$$

con $c_0 \in \mathbb{C}$. Ricordiamo però che f_1 è un logaritmo e quindi $f_1' = b'/b$ con $b \in K$. Concludiamo pertanto

$$\alpha = \sum_{j=1}^{N} \gamma_j \frac{u_j'}{u_j} + c_0 \frac{b'}{b} + v' \,, \tag{6.20}$$

che ovviamente è la tanto sospirata (4.1).

6.4. Il caso esponenziale

Possiamo usare lo stesso argomento della sezione precedente per arrivare all'identità (6.14), che ripetiamo qui di seguito

$$\begin{aligned} \alpha = &\sum_{j=1}^{N} \gamma_j \frac{u_j'}{u_j} + \sum_{j=1}^{\tilde{N}} \lambda_j \frac{(R_j(f_1))'}{R_j(f_1)} + (S_0(f_1))' \\ &+ \sum_{j=1}^{\tilde{N}} \sum_{l=1}^{m_j} \frac{(S_{l,j}(f_1))'}{V_j^l(f_1)} - \sum_{j=1}^{\tilde{N}} \sum_{l=1}^{m_j} l \frac{S_{l,j}(f_1)(V_j(f_1))'}{V_j^{l+1}(f_1)} \,, \end{aligned} \tag{6.21}$$

ricordando che i polinomi V_j e R_j sono monici e irriducibili, gli R_j sono tutti distinti tra loro e i V_j sono tutti distinti tra loro (mentre potrebbe ben darsi che $V_j = R_k$ per qualche j e k!).

Vogliamo ora capire che cosa succede quando differenziamo un elemento della forma $P(f_1)$ con $P \in K[X]$. Come nel caso del logaritmo scriviamo

$$P(X) = a_m X^m + \ldots + a_0$$

per ottenere

$$(P(f_1))' = \sum_{j=1}^{m} j a_j f_1' f_1^{j-1} + \sum_{j=0}^{m} a_j' f_1^j \,.$$

In questo caso, però, f_1 è un esponenziale e quindi esiste $b \in K$ tale che $f_1' = b' f_1$. Ne concludiamo

$$(P(f_1))' = \sum_{j=1}^{m} (j a_j b' + a_j') f_1^j \,.$$

Notiamo che a_m è sicuramente non nullo. Infatti, se fosse $m a_m b' + a_m' = 0$ avremmo allora $(a_m f_1^m)' = 0$. D'altra parte questo vorrebbe dire che $a_m f_1^m = c_0$ per qualche costante $c_0 \in \mathbb{C}$, che non è possibile perché $a_m \in K$ è non nullo e f_1 è trascendente su K. Pertanto $(P(f_1))' = \tilde{P}(f_1)$ per un polinomio $\tilde{P} \in K[X]$ con grado $\deg(\tilde{P}) = \deg(P)$. Notiamo inoltre che, se a_m è costante, allora P divide $\tilde{P}$ se e solo se P è un monomio. Infatti la condizione che P divida $\tilde{P}$ è equivalente a

$$a_j m a_m b' = a_m (j a_j b' + a_j') \qquad \forall j \in \{0, \ldots, m-1\} \,.$$

Dividendo quest'ultima identità per a_m otteniamo $a_j' - (m-j) b' a_j = 0$, che implica

$$\left(\frac{a_j}{f_1^{m-j}} \right)' = 0 \,,$$

ovvero $a_j = cf_1^{m-j}$ per qualche costante c. D'altra parte per la trascendentalità di f_1 abbiamo necessariamente $a_j = c$.

Torniamo ora alla (6.21). Procediamo come nella seconda parte della Sezione 6.3 ricavando

$$\begin{aligned}\alpha = &\sum_{j=1}^{N} \gamma_j \frac{u_j'}{u_j} + \sum_{j=1}^{\tilde{N}} \lambda_j \frac{\tilde{R}_j(f_1)}{R_j(f_1)} + \tilde{S}_0(f_1) \\ &+ \sum_{j=1}^{\tilde{N}} \sum_{l=1}^{m_j} \frac{\tilde{S}_{l,j}(f_1)}{V_j^l(f_1)} - \sum_{j=1}^{\tilde{N}} \sum_{l=1}^{m_j} m_j \frac{S_{l,j}(f_1)\tilde{V}_j(f_1)}{V_j^{l+1}(f_1)}\,. \end{aligned} \tag{6.22}$$

Moltiplicando entrambi i membri di (6.22) per

$$V_1^{m_1+1}(f_1)\dots V_{\tilde{N}}^{m_{\tilde{N}}+1}(f_1)R_{j_1}(f_1)\dots R_{j_s}(f_1)$$

e spostando il membro sinistro dell'equazione risultante a destra otteniamo un'identità del tipo

$$\mathcal{P}(f_1) = 0\,.$$

Di nuovo, visto che f_1 è trascendente, il polinomio $\mathcal{P}$ deve essere banale. Ragionando ancora come nella Sezione 6.3 possiamo scrivere

$$\begin{aligned}&\mathcal{P}(X) = V_1^{m_1}(X)\mathcal{Q}(X) \\ &+ S_{m_1,j}(X)\tilde{V}_1(X)V_2^{m_2+1}(X)\dots V_{\tilde{N}}^{m_N+1}(X)R_{j_1}(X)\dots R_{j_l}(X)\,. \end{aligned} \tag{6.23}$$

per qualche polinomio $\mathcal{Q} \in K[X]$. Visto che V_1 è primo con tutti i fattori del secondo addendo di (6.23) eccetto al più $\tilde{V}_1$, V_1 dovrebbe necessariamente dividere $\tilde{V}_1$. Dalle considerazioni precedenti questo è possibile se e solo se V_1 è un monomio. D'altra parte, visto che V_1 è un polinomio irriducibile monico, deve essere necessariamente $V_1(X) = X$. Osserviamo anche che non può essere $m_1 \geq 2$ perché il secondo addendo in (6.23) non sarebbe divisibile per X^2. Pertanto abbiamo necessariamente

$$\xi = S_0(f_1) + \frac{a}{f_1}\,, \tag{6.24}$$

per un qualche polinomio $S_0 \in K[X]$ e per un $a \in K$. Lo stesso ragionamento ci dice anche che $R_j(X) = X$ per ogni j. Quindi ci siamo ridotti all'identità

$$\alpha = \sum_{j=1}^{N} \gamma_j \frac{u_j'}{u_j} + \lambda_1 \frac{f_1'}{f_1} + (S_0(f_1))' + \left(\frac{a}{f_1}\right)'\,. \tag{6.25}$$

Ricordiamo però che $f_1' = b'f_1$ e quindi otteniamo

$$\alpha = \sum_{j=1}^{N} \gamma_j \frac{u_j'}{u_j} + \lambda_1 b' + (S_0(f_1))' + \frac{a' + ab'}{f_1}\,. \tag{6.26}$$

Abbiamo anche $(S_0(f_1))' = \tilde{S}_0(f_1)$ per un polinomio $\tilde{S}_0$ che ha lo stesso grado di S_0. Moltiplicando la (6.26) per f_1 concludiamo allora

$$f_1\tilde{Q}(f_1) = a' + ab' \tag{6.27}$$

per un polinomio $\tilde{Q} \in K[X]$ che ha lo stesso grado di $\tilde{S}_0$. Di nuovo la trascendentalità di f_1 forza $a' + ab' = 0$. Sempre per lo stesso motivo, il grado di $\tilde{S}_0$ deve essere 0 e questo è possibile se e solo se il grado di S_0 è esso stesso 0. Allora otteniamo l'esistenza di un $s_0 \in K$ tale che

$$\alpha = \sum_{j=1}^{N} \gamma_j \frac{u_j'}{u_j} + \lambda_1 b' + s_0' \,. \tag{6.28}$$

Visto che λ_1 è costante, se poniamo $v := \lambda_1 b + s_0$, dalla (6.28) concludiamo la (4.1).

7. Dimostrazione della Proposizione 4.3

Ahinoi, per attaccare la Proposizione 4.3 non basta il Teorema 4.1 ma ci serve un'ultima tessera del puzzle, ovvero la trascendentalità della funzione e^g su $K = \mathbb{C}(x)$ quando $g \in \mathbb{C}(x)$ è una funzione non costante. Sembra assolutamente ovvio... ma bisogna mostrarlo – questo ci impone il Bushido dei matematici! Tuttavia, come il Lemma 5.1, la trascendentalità di e^g su $\mathbb{C}(x)$ non è, a mio avviso, uno degli aspetti centrali della teoria qui esposta, ma piuttosto un dettaglio occasionale, che il lettore meno pignolo può tranquillamente omettere.

Lemma 7.1. *Sia $g \in \mathbb{C}(x) = K$ una funzione razionale non costante. Allora e^g è trascendente su K, ovvero: non esistono un polinomio $P \in K[X]$ e un intervallo $I \subset \mathbb{R}$ su cui la funzione $t \mapsto P(f(t))$ sia identicamente nulla.*

DIMOSTRAZIONE. Supponiamo per assurdo che un tale intervallo e un tale polinomio esistano. In particolare, possiamo supporre che tale polinomio sia monico. Avremo allora

$$P(X) = X^n + \sum_{j=0}^{n-1} f_j X^j$$

dove ciascun f_j è una funzione razionale. Sia ora F l'insieme finito di punti sul piano complesso su cui almeno una delle funzioni $f_{m-1}, \ldots, f_0, g$ non è definita. Un semplice argomento di continuazione analitica (si veda ad esempio [16]) mostra che, se

$$P(f(t)) = e^{ng(t)} + \sum_{j=0}^{n-1} f_j(t) e^{jg(t)} = 0 \qquad \forall t \in I$$

allora

$$P(f(z)) = e^{ng(z)} + \sum_{j=0}^{n-1} f_j(z) e^{jg(z)} = 0 \qquad \forall z \in \mathbb{C} \setminus F \,.$$

Se la funzione razionale g non è un polinomio e ζ è uno zero del denominatore, allora per un'opportuna costante $c > 0$ e in un opportuno intorno di ζ avremo

$$|g(z)| \geq \frac{c}{|z - \zeta|} \qquad \forall z \in U \,. \tag{7.1}$$

D'altra parte, per una costante $C > 0$ e un intero $N \in \mathbb{N}$ opportuni, in un intorno V di ζ possiamo anche stimare

$$\left| \sum_{j=0}^{n-1} f_j(z) e^{jg(z)} \right| \leq C e^{(n-1)|g(z)|} |z - \zeta|^{-N} \qquad \forall z \in V .$$

Ne concludiamo:

$$|P(f(z))| \geq e^{(n-1)|g(z)|} \left(e^{|g(z)|} - C|z - \zeta|^{-N} \right) \tag{7.2}$$

D'altra parte, da (7.1) e dalle proprietà di crescita dell'esponenziale, segue che in un intorno di ζ il membro destro di (7.2) è positivo e che

$$\lim_{z \to \zeta} |P(f(z))| = \infty ,$$

in contraddizione col fatto che $P(f)$ dovrebbe essere identicamente nulla in ogni intorno di ζ.

Pertanto abbiamo escluso che e^g possa essere algebrica su $\mathbb{C}(x)$ quando g non è un polinomio. D'altra parte, con un ragionamento del tutto analogo si vede che, se g è un polinomio non costante, allora

$$\lim_{|z| \to \infty} |P(f(z))| = \infty .$$

Ora siamo finalmente pronti per l'ultimo sforzo!

DIMOSTRAZIONE DELLA PROPOSIZIONE 4.3. Abbiamo già visto che, se c'è una funzione razionale a tale che $a' + ag' = f$, allora la primitiva (o meglio le primitive) di fe^g è una funzione elementare. Pertanto il nostro obiettivo è mostrare l'implicazione opposta.

Supponiamo quindi che g non sia costante e che ci sia un'estensione elementare L di $\mathbb{C}(x)$ in cui troviamo una primitiva y di $\alpha = fe^g$. Poiché $y' = \alpha \in L$, L contiene anche $h = e^g$. Pertanto L è una estensione elementare di $K := \mathbb{C}(x)(h)$. Applichiamo il Teorema 4.1 e troviamo elementi $u_1, \ldots, u_n, v \in K$ e costanti $c_1, \ldots, c_n \in \mathbb{C}$ tali che

$$\alpha = \sum_{i=1}^{n} c_i \frac{u_i'}{u_i} + v' .$$

Notiamo che $\alpha = A(h)$, dove $A \in \mathbb{C}(x)[X]$ è il polinomio $A(X) = fX$. Possiamo ora procedere esattamente come nella Sezione 6.4 per trovare:

- costanti $\gamma_1, \ldots, \gamma_N$, $\lambda_1, \ldots, \lambda_{\tilde{N}}$,
- elementi $\zeta_1, \ldots, \zeta_n \in \mathbb{C}(x)$,
- polinomi monici irriducibili distinti $R_1, \ldots, R_{\tilde{N}} \in \mathbb{C}(x)[X]$,
- polinomi monici irriducibili distinti $V_1, \ldots, V_{\tilde{N}} \in \mathbb{C}(x)[X]$,

- interi $m_1, \dots, m_{\bar N} \geq 1$,
- polinomi $S^l_j \in \mathbb{C}(x)[X]$ di grado $\deg(S^l_j) < \deg(V_j)$,
- un polinomio $S_0 \in \mathbb{C}(x)[X]$,

tali che valga l'identità

$$A(h) = \alpha = \sum_{j=1}^{N} \gamma_j \frac{\zeta_j'}{\zeta_j} + \sum_{j=1}^{\tilde N} \lambda_j \frac{(R_j(h))'}{R_j(h)} + (S_0(h))' + \sum_{j=1}^{\bar N} \sum_{l=1}^{m_j} \frac{(S_{l,j}(h))'}{V_j^l} - \sum_{j=1}^{\bar N} \sum_{l=1}^{m_j} l \frac{S_{l,j}(h)(V_j(h))'}{V_j^{l+1}(h)}\,. \tag{7.3}$$

Visto che g non è costante, grazie al Lemma 7.1 h è un esponenziale trascendente su $\mathbb{C}(x)$ e possiamo procedere esattamente come nella Sezione 6.4 per concludere che:

- non appaiono le frazioni con V_j al denominatore;
- c'è al più un R_j, che è il polinomio identico X.

Arriviamo pertanto all'identità

$$A(h) = \sum_{j=1}^{N} \gamma_j \frac{\zeta_j'}{\zeta_j} + (S_0(h))' + \lambda_1 g'\,. \tag{7.4}$$

Da qui in poi però non possiamo più seguire gli argomenti della Sezione 6.4 perché ora al membro sinistro di (7.4) abbiamo un polinomio di grado 1 in h (mentre nella Sezione 6.4 avevamo un polinomio di grado 0 in f_1). Questo vuole semplicemente dire che $(S_0(h))' = \tilde S_0(h)$ per un polinomio $\tilde S_0$ di grado 1. D'altra parte, per le considerazioni fatte nella Sezione 6.4 sulle derivate di $(P(h))'$ quando h è un esponenziale trascendente, questo è possibile se e solo se S_0 è esso stesso un polinomio di grado 1. Poniamo allora

$$S_0(X) = s_1 X + s_0$$

(dove $s_0, s_1 \in \mathbb{C}(x)$) e $d = \sum_j \gamma_j \frac{\zeta_j'}{\zeta_j} \in \mathbb{C}(x)$. Ricordandoci che $A(h) = fh$ e che $h' = g'h$, dalla (7.4) otteniamo

$$fh = d + s_1' h + s_1 g' h + s_0' + \lambda_1 g'\,, \tag{7.5}$$

ovvero

$$(f - s_1' - s_1 g')h = s_0' + d + \lambda_1 g'\,.$$

Visto però che h non è una funzione razionale mentre entrambe $f - s_1' - s_1 g'$ e $s_0' + d + \lambda_1 g'$ lo sono, ne concludiamo che $f = s_1' + s_1 g'$. Se poniamo $a = s_1$, visto che $s_1 \in \mathbb{C}(x)$, abbiamo trovato una soluzione razionale dell'equazione $a' + ag' = f$, che è esattamente la tesi della Proposizione.

Bibliografia

[1] ACQUISTAPACE, P., CONTI, F. & SAVOJNI, A. *Analisi matematica. Teoria e applicazioni*. McGraw Hill, Milano, 2001.

[2] ATIJAH, M. F. & MACDONALD, I. G. *Introduction to commutative algebra*. Addison-Wesley series in mathematics. Westview Press, 1969.

[3] CZAPORT, S. R., GEDDES, G. O. & LABAHN, G. *Algorithms for computer algebra*. Kluwer Academic Publishers, 1992.

[4] GRIFFITHS, P. & HARRIS, J. *Principles of algebraic geometry*. Wiley classic library. Wiley, New York, 1994.

[5] HARDY, G. H. *The integration of functions of a single variable*. Cambridge Univ. Tracts in Mathematics and Mathematical physics. Cambridge University Press, Cambridge, 1916.

[6] HERSTEIN, I. N. *Algebra*. Editori Riuniti, 1999.

[7] LIOUVILLE, J. *Mémoire sur les Trascendantes Elliptiques et sur l'impossibilité d'exprimer les racines de certaines équations en fonction finie explicite des coefficients*. J. Math. Pures Appl. **2** pp. 124–193 (1837).

[8] MAGID, A. R. *Lectures on differential Galois theory*. University Lecture Series, 7. American Mathematical Society, Providence, RI, 1994.

[9] MAGID, A. R. *Differential Galois theory*. Notices Amer. Math. Soc. **46** (9) pp. 1041–1049 (1999).

[10] MORDUKHAI-BOLTOVSKOJ, D. D. *Sur la résolution des équations différentielles du premier ordre en forme finie*. Rend. Circ. Mat. Palermo **61** pp. 49–72 (1937).

[11] OSTROWSKI, A. *Sur l'intégrabilité élémentaire de quelques classes d'expressions*. Comm. Math. Helv. **18** pp. 283–308 (1946).

[12] VAN DER PUT, M. & SINGER, M. F. *Galois theory of linear differential equations*. Grundlehren der Mathematischen Wissenschaften, 328. Springer-Verlag, Berlin, 2003.

[13] RISCH, R. H. *The solution of the problem of integration in finite terms*. Bull. Amer. Math. Soc. **76** pp. 605–608 (1970).

[14] RITT, J.F. *Integration in finite terms: Liouville's theory of elementary models*. Columbia Univ. Press, New York, 1948.

[15] ROSENLICHT, M. *Integration in finite terms*. Amer. Math. Monthly **79** (9) pp. 963–972 (1972).

[16] SHABAT, B. V. *Introduction to complex analysis*. American Mathematical Society, Providence, RI, 1992.

CAMILLO DE LELLIS
Institut für Mathematik, Universität Zürich
CH-8057 Zürich
e–mail: camillo.delellis@math.uzh.ch