UNIVERSITÀ
DEGLI STUDI
FIRENZE

Università degli Studi di Firenze

DIPARTIMENTO DI MATEMATICA E INFORMATICA ULISSE DINI
Corso di Laurea Triennale in Matematica

Tesi di laurea triennale

Integrazione in termini finiti: Il Teorema Di Liouville.

Perché "non esiste" la primitiva di e^{x^2}

Candidato:
Tommaso Mannelli Mazzoli
Matricola 5650541

Relatore:
prof. Andrea Colesanti

Anno Accademico 2016-2017

Indice

1 Introduzione

Ogni studente di Analisi 1 che prova ad integrare funzioni come e^{x^2}, $\sin(x^2)$, $e^{1/x}$ si sente dire che esse non sono elementarmente integrabili, ovvero non è possibile scrivere la primitiva combinando in modo finito le quattro operazioni elementari, elevamenti a potenza ed estrazioni di radici, logaritmi, esponenziali, funzioni trigonometriche e trigonometriche inverse. Ma come mai? Diamo un altro esempio di una funzione integrabile che non ammette una primitiva elementare. In teoria dei numeri c'è molto interesse per lo studio della funzione $\pi(x) = |\{1 \leq p \leq x : p \text{ primo}\}|$ di variabile reale x, che conta il numero di primi fino a x. Definita $\mathrm{Li}(x) = \int_2^x \frac{dt}{\ln(t)}$ la funzione *logaritmo integrale*, è stato dimostrato nel 1838 da Dirichlet che per $x \to \infty$, $\pi(x) \sim \mathrm{Li}(x)$. Questo esempio mostra quanto possa essere importante il calcolo di $\mathrm{Li}(x)$, che però non è esprimibile con funzioni elementari. Come è possibile provare un risultato simile? Sicuramente prima di tutto è necessario dare una definizione precisa di *funzione elementare* e lo strumento che ci permetterà di muoverci in questo campo con tranquillità è l'algebra differenziale. Grazie ad essa dimostreremo risultati (primo fra tutti il teorema di Liouville) col quale daremo una caratterizzazione delle funzioni elementarmente integrabili.

2 Prerequisiti

Le nozioni che riportiamo sono riprese da [Cas]
Un campo F è un anello commutativo con unità in cui ogni elemento non nullo è invertibile; denotiamo con $F^* = F \setminus \{0\}$. Siano F, E campi. E si dice *estensione* di F (e si scrive $E|F$) se esiste un omomorfismo iniettivo di campi (detto immersione):

$$\phi : F \longrightarrow E.$$

Sia F un campo, definiamo con $F[x]$ l'anello dei polinomi a coefficienti in F e con $F(x)$ il campo delle frazioni di $F[x]$. Quindi

$$F(x) = \left\{ \frac{f}{g} : \quad f, g \in F[x],\ g \neq 0 \right\}.$$

Notiamo che $F(x)$ è un campo e $F(x)|F$ è un'estensione di campi.
Sia $b \in E$. b si dice **algebrico** se esiste un polinomio $f \neq 0$ in $F[x]$ tale che $f(b) = 0$. Un'estensione $E|F$ si dice **estensione algebrica** se ogni elemento di E è algebrico su F.
Definizione Se $E|F$ è un'estensione di campi, allora è possibile vedere in modo naturale E come spazio vettoriale su F. La *dimensione* di E come spazio vettoriale su F si chiama **grado** di E su F e si denota con $[E : F]$, se $[E : F] < \infty$, allora $E|F$ si dice un'estensione **finita**. Inoltre osserviamo che ogni estensione algebrica è finita.
Definizione Un'estensione di campi $E|F$ si dice **normale** se ogni elemento $b \in E$ è algebrico su F e il suo polinomio minimo si fattorizza completamente in $E[x]$.
Definizione Un polinomio f si dice separabile se ogni suo fattore irriducibile ha tutte le radici semplici (in un campo di spezzamento), cioè se a è una radice, $f'(a) \neq 0$. Un'estensione di campi $E|F$ si dice **separabile** (su F) se è algebrica e per ogni $b \in E$, il polinomio minimo $\min_F(b)$ è separabile su F.
Definizione Sia R un anello e sia $1 \in R$ la sua unità moltiplicativa. La caratteristica R è 0 se $n \cdot 1 \neq m \cdot 1$ per ogni $n, m \in \mathbb{Z}$; altrimenti è il più piccolo naturale $n > 0$ tale che $n \cdot 1 = 0$
Proposizione Sia F un campo di caratteristica 0, oppure finito. Allora ogni estensione $E|F$ è separabile.
Definizione Un'estensione di campi $E|F$ che sia *finita, normale* e *separabile* si dice **di Galois**
Diamo alcuni richiami riguardo la teoria di Galois, che verrà utilizzata in seguito.
Definizione Sia $E|F$ un'estensione di campi. L'insieme degli F-automorfismi di E (cioè degli automorfismi di E che fissano ogni elemento di F) è un sottogruppo del gruppo di $\mathrm{Aut}(E)$ e si denota con $\mathrm{Gal}(E|F)$. Inoltre dato $f \in F[x]$ si definisce gruppo di Galois di f su F come $\mathrm{Gal}(E|F)$ con E dove E è il campo di spezzamento di f su F. Sia ora H sottogruppo di $\mathrm{Gal}(E|F)$, definiamo il campo degli invarianti $\mathrm{Inv}_E(H) = \{b \in E |\ \sigma(b) = b\ \forall \sigma \in \mathrm{Gal}(E|F)\}$.
Per la dimostrazione delle due proposizioni seguenti si veda [Cas]

Proposizione 1. *Sia E il campo di spezzamento di un polinomio separabile $f \in F[x]$ di grado n. Allora il sottogruppo di S_n isomorfo al gruppo di Galois di f su F è transitivo se e solo se f è irriducibile su F.*

Proposizione 2. *Sia $E|F$ un'estensione di Galois, allora* $\mathrm{Inv}_E(E) = F$.

Polinomi simmetrici in $F[x_1, \ldots, x_n]$

Definizione 1. Sia F un campo, $f \in F[x_1, \ldots, x_n]$. Si dice che f è simmetrico se per ogni permutazione $\sigma \in S_n$ si ha che $f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = f(x_1, \ldots, x_n)$.

Teorema 1. *Sia F un campo con* $\mathrm{char}(F) = 0$, *$f \in F[x]$ un polinomio monico di grado $n > 0$ con radici $a_1, \ldots, a_n$ in un suo campo di spezzamento su F. Allora per ogni polinomio simmetrico $p \in F[x_1, \ldots, x_n]$ si ha che $p(a_1, \ldots, a_n) \in F$.*

Dimostrazione. Sia f un polinomio come nelle ipotesi e sia E il suo campo di spezzamento, allora si ha che $E|F$ è un'estensione di Galois . Definiamo $G := \mathrm{Gal}(E|F)$ e consideriamo $p \in F[x_1, \ldots, x_n]$ un polinomio simmetrico. Ogni elemento permuta le radici di f, dunque per ogni $\sigma \in \mathrm{Gal}(E|F)$ si ha che $\sigma(p(a_1, \ldots, a_n)) = p(a_{\sigma(1)}, \ldots, a_{\sigma(n)}) = p(a_1, \ldots, a_n)$ e quindi, dalla Proposizione 2 segue che $p \in \mathrm{Inv}_G(G) = F$. □

Decomposizione in fratti semplici Un procedimento standard per il calcolo degli integrali di funzioni razionali del tipo

$$\int \frac{dx}{x^2 - 1}.$$

è lo spezzare la funzione integranda (che non sappiamo integrare) in somma di altre funzioni razionali più semplici (che sappiamo integrare). Ad esempio nel nostro caso

$$\int \frac{dx}{x^2 - 1} = \int \frac{1}{2}\left(\frac{1}{x-1} - \frac{1}{x+1}\right) dx = \int \frac{1}{2(x-1)} dx - \int \frac{1}{2(x+1)} dx.$$

Ma è sempre possibile agire in questo modo comunque si scelgano funzione razionale, ovvero per qualunque P, Q polinomi in $F[x]$?
Cominciamo con il fissare un campo F e scegliere una funzione razionale $v = \frac{P}{Q}$ con $P, Q \in F[x]$ primi tra loro. Scomponiamo Q in fattori irriducibili:

$$Q = Q_1^{k_1} \cdot Q_2^{k_2} \cdot \cdots \cdot Q_N^{k_N}.$$

Notiamo in particolare che $Q_1^{k_1}$ e $Q_2^{k_2} \cdots Q_N^{k_n}$ sono primi tra loro, e dunque per l'identità di Bézout sappiamo che esistono due polinomi T e S tali che $TQ_1^{k_1} + SQ_2^{k_2} \cdots Q_N^{k_N} = 1$ e dunque possiamo scrivere

$$v = \frac{P}{Q} = \frac{P(TQ_1^{k_1} + SQ_2^{k_2} \cdots Q_N^{k_N})}{Q_1^{k_1} \cdot Q_2^{k_2} \cdot \cdots \cdot Q_N^{k_N})} = \frac{PT}{Q_2^{k_2} \cdot \cdots \cdot Q_N^{k_N}} + \frac{PS}{Q_1^{k_1}}$$

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 $N - 1$ volte questo procedimento otteniamo una scrittura del tipo

$$v = \frac{T_1}{Q_1^{k_1}} + \frac{T_2}{Q_2^{k_2}} + \cdots + \frac{T_N}{Q_N^{k_N}} = \sum_{i=1}^{N} \frac{T_j}{Q_j^{k_j}}$$

dove ciascun Q_j è irriducibile. Se ora il grado di T_j fosse maggiore o uguale al grado di Q_j potremmo usare l'algoritmo di Euclide per scrivere $T_j = U_j Q_j + R_j$ dove R_j è un polinomio di grado minore di quello di Q_j. Come risultato otteniamo

$$\frac{T_j}{Q_j^{k_j}} = \frac{U_j}{Q_j^{k_j - 1}} + \frac{R_j}{Q_j^{k_j}}.$$

In un numero finito di passi arriviamo ad una identità della forma

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

dove, per $l \geq 1$, ciascun polinomio $S_{l,j}$ ha grado minore di Q_j.
Abbiamo dunque dimostrato il seguente teorema:

Teorema 2. *Sia F un campo, $v \in F(x)$ e $P, Q \in F[x]$ tali che $v = \frac{P}{Q}$. Sia $Q = Q_1^{k_1} \cdots Q_N^{k_N}$ la sua fattorizzazione in irriducibili. Allora esistono polinomi $T, S_{ij} \in F[x]$ tali che*

$$v = T + \sum_{i=1}^{n} \sum_{j=1}^{k_i} \frac{S_{ij}}{Q_i^j}$$

tale scrittura di v è detta ***decomposizione in fratti semplici****.*

3 Campi Differenziali

Definizioni e proprietà dei campi differenziali D'ora in poi ogni campo che considereremo, avrà caratteristica 0.

Definizione 2. Un anello differenziale è una coppia $(A, \ ')$ dove A è un anello e $' : A \to A$ una applicazione (detta derivata) tale che:

(D1) $(x+y)' = x' + y'$. per ogni $a, b \in A$;

(D2) $(xy)' = x'y + xy'$ per ogni $a, b \in A$.

Se A è un campo, diremo che $(A,')$ è un campo differenziale.

In generale un anello può avere più di una derivata definita su di esso. Per esempio l'anello dei polinomi a coefficienti razionali in due indeterminate $\mathbb{Q}[x, y]$ ha almeno tre derivate: $0, d/dx, d/dy$ ma in realtà ne ha molte di più: ogni combinazione lineare di derivate con coefficienti nell'anello è una derivata sull'anello. Un esempio di campo differenziale, che poi è quello che ci accompagnerà lungo questo percorso, è $(\mathbb{C}(x), \ ')$ dove $'$ è la derivata usuale. Infatti $\mathbb{C}(x)$ è un campo e $'$ una mappa che soddisfa le proprietà (D1)e (D2).

Proposizione 3. *Sia $(F, \ ')$ un campo differenziale, allora*

1. $1'_F = 0'_F = 0_F$;
2. $(x^k)' = kx^{k-1}x'$ *per ogni* $x \in F$ *e ogni* $k \in \mathbb{Z}$;
3. $(-x)' = -x'$ *per ogni* $x \in F$;
4. $\left(\frac{x}{y}\right)' = \frac{x'y - xy'}{y^2}$ *per ogni* $x, y \in F, y \neq 0$;

5. $\frac{\left(x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}\right)'}{x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}} = k_1\frac{x_1'}{x_1} + k_2\frac{x_2'}{x_2} + \ldots k_n\frac{x_n'}{x_n}$ *per ogni* $x_1, \ldots x_n \in F*$ *e* $k_1, \ldots, k_n \in \mathbb{Z}$.

Una dimostrazione (piuttosto routinaria) di queste proprietà si può trovare in [Del]

Definizione 3. Chiamiamo **sottocampo delle costanti di** $(F,')$ l'insieme

$$C_F = \{x \in F : x' = 0\}.$$

Osservazione Non è difficile dimostrare che C_F è un campo.

Estensioni di campi differenziali

Definizione 4. Siano $(F,\ ')$ e $(E,\ ^*)$ due campi differenziali. Si dice che $(E,\ ^*)$ è un'estensione differenziale di $(F,\ ')$ se valgono le seguenti proprietà:

(i) E è estensione di F. In simboli $E|F$;

(ii) * estende $'$. In simboli $x^* = x'$ per ogni $x \in F$.

Sia $(F,\ ')$ un campo differenziale. Consideriamo l'anello di polinomi $F[x]$ e le mappe $D_0, D_1 : F[x] \to F[x]$ definite nel modo seguente:

$$D_0\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} a_i' x^i;$$
$$D_1\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=1}^{n} i a_i x^{i-1}.$$

Con considerazioni di routine si può dimostrare la seguente proposizione:

Proposizione 4. *D_0 e D_1 sono derivate nell'anello $F[x]$.*

Il seguente teorema mostra come, data una estensione algebrica, è possibile estendere la derivata sul campo base in maniera unica.

Teorema 3. *Sia $(F,\ ')$ un campo differenziale , sia $E|F$ un'estensione algebrica. Allora esiste un'unica mappa *, :*

$$^* : E \longrightarrow E$$

tale che $(E,\ ^*)$ è un'estensione differenziale di $(F,\ ')$

Dimostrazione. Dimostriamo solo l'unicità (la dimostrazione dell'esistenza si può trovare in [Bro]) Supponiamo che esista una derivata * in E che estende quella su F. Sia $b \in E$ e sia $f \in F[x]$ il suo polinomio minimo su F (esiste poiché b è algebrico su F). Allora, usando le proprietà della derivata, si ha che

$$0 = (f(b))^* = \left(\sum_{i=0}^{n} a_i b^i\right)^* = \sum_{i=0}^{n} a_i' b^i + b^* \sum_{i=1}^{n} a_i b^{i-1} i = (D_0 f)(b) + b^*(D_1 f)(b),$$

da cui si ottiene che

$$b^* = -\frac{(D_0 f)(b)}{(D_1 f)(b)}.$$

(Notiamo che, dato che f è il polinomio minimo di b su F, allora $D_1 f$ è un polinomio di grado minore di f, dunque non può essere zero). Dunque se esiste una derivata che estende $'$ su $F[b]$, essa è unica. Adesso dato che $E|F$ è algebrica, per ogni $b \in E$ si ha che la derivata $'$ si estende a $F[b]$ in maniera unica. Per l'arbitrarietà di b si ottiene la tesi. □

Osservazione Il teorema precedente ci fornisce anche un modo di calcolare la derivata di elementi algebrici in maniera puramente astratta. Pensiamo ad esempio al campo differenziale delle frazioni di polinomi a coefficienti in $\mathbb{C}$ con la derivata usuale $(\mathbb{C}(x),')$. L'elemento $b = \sqrt{x}$ non appartiene al campo ma essa è radice del polinomio $\mathbb{C}(x)[t] \ni P(t) = t^2 - x$. Notiamo inoltre che dato che P è monico e irriducibile, esso è anche il polinomio minimo di b su $\mathbb{C}(x)$. Si trova subito che $(D_0)(b) = -1$ e $(D_1)(b) = 2b$. Dunque per quanto dimostrato sopra

$$(\sqrt{x})' = b' = -\frac{-1}{2b} = \frac{1}{2\sqrt{x}}.$$

4 Il Teorema di Liouville

Definizione 5. Sia $(F,\ ')$ un campo differenziale e E una sua estensione differenziale. Un elemento $t \in E$ è:

- un **logaritmo** su F se esiste $b \in F^*$ tale che $t' = b'/b$, e scriviamo $t = \log(b)$;
- un **esponenziale** su F se esiste $b \in F$ tale che $t' = tb'$ e scriviamo $t = e^b$;
- **elementare** su F se è algebrico o un esponenziale o un logaritmo.

Definizione 6. E è un'**estensione elementare** di F se esistono $t_1, \dots t_n$ in E tale che $E = F(t_1, \dots, t_n)$ e si ha che t_i è elementare su $F(t_1, t_2, \dots, t_{i-1})$. Diremo inoltre che $f \in F$ è **elementarmente integrabile** su F se esiste una estensione elementare $E|F$ e $g \in E$ tale che $g' = f$. Infine una **funzione elementare** è un qualunque elemento di una estensione elementare di $(\mathbb{C}(x), d/dx)$

Ad esempio $e^{(e^x)}$ è elementare (due estensioni esponenziali di $\mathbb{C}(x)$), così come $\sqrt{\log(x)}$ (una estensione logaritmica seguita da una algebrica).
Possiamo adesso definire precisamente il *problema dell'integrazione in termini finiti*: dato un campo differenziale F e $f \in F$, il problema consiste nel decidere in un numero finito di passi se f è elementarmente integrabile su F di calcolarne la primitiva, se esiste.

Osservazione Si noti come c'è una differenza tra l'avere una primitiva elementare e un integrale elementare su F: si consideri $F = \mathbb{C}(x, t_1, t_2)$ dove x, t_1, t_2 sono indeterminate su $\mathbb{C}$, con la derivata D tale che $Dx = 1, Dt_1 = t_1, Dt_2 = t_1/x$

(in pratica $t_1 = e^x$ e $t_2 = \mathrm{Ei}(x)$ con $\mathrm{Ei}(x) := \int e^x/x dx$ che dimostreremo in seguito non essere elementarmente integrabile). Allora

$$\int \frac{t_1 t_2}{x} dx = \frac{t_2^2}{2} \in F,$$

e dunque l'elemento $\frac{t_1 t_2}{x}$ (che moralmente è $\frac{e^x \mathrm{Ei}(x)}{x}$) è elementarmente integrabile su F (d'altronde il suo integrale sta in F, che è di certo un'estensione elementare di F) ma non è una funzione elementare, poiché non è elemento di un'estensione elementare di $(\mathbb{C}(x), d/dx)$.
Osservazione Le funzioni elementari della definizione 6 includono tutte le usuali funzioni elementari dell'analisi, dato che le funzioni trigonometriche e le loro inverse possono essere riscritte in termini di esponenziali e logaritmi complessi (grazie alla celebre formula di Eulero $e^{fi} = \cos(f) + i\sin(f)$)

Lemma 1. *Sia $(F, \ ')$ un campo differenziale. Sia $F(t)$ un'estensione differenziale di F con t trascendente su F tale che $C_F = C_{F(t)}$.*

1. *Se $t' \in F$, allora per ogni polinomio $f(t) \in F[t]$ di grado $n > 0$, $(f(t))'$ è un polinomio in $F[t]$ di grado n o $n-1$.*
2. *Se $t'/t \in F$, allora per ogni $a \in F$ si ha che $(at^n) = ht^n$ per qualche $h \in F$ e per ogni polinomio $f(t) \in F[t]$ si ha che $(f(t))'$ è un polinomio in $F[t]$ dello stesso grado di $f(t)$.*

Dimostrazione. 1. Siano $t' = b \in F$ e $n = \deg f(t)$. Allora possiamo scrivere $f(t) = a_n t^n + a_{n-1}t^{n-1} + \cdots + a_0$ con $a_i \in F$ e $a_n \neq 0$. Allora

$$f'(t) = a_n' t^n + (a_n bn + a_{n-1}')t^{n-1} + \cdots + (a_{n-i} b(n-i) + a_{n-i-1})t^{n-i} + \cdots +$$

Dunque la derivata di $f(t)$ continua a essere un polinomio in $F[t]$ di grado n se $a_n' \neq 0$. Supponiamo ora che $a_n' = 0$ e supponiamo per assurdo che $(a_n bn + a_{n-1}') = 0$, si avrebbe allora che $a_n bn + a_{n-1}' = (na_n t + a_{n-1})' = 0$ e dunque $na_n t + a_{n-1}$ sarebbe una costante, cioè un elemento di $C_{F(t)}$. Ma dato che abbiamo supposto $C_F = C_{F(t)}$, si avrebbe che $na_n t + a_{n-1} \in F$, ovvero $t \in F$, assurdo poiché t è trascendente su F, dunque se a_n è una costante, allora il grado di $(f(t))'$ è $n-1$.
2. Supponiamo ora che $t'/t = b \in F$. Sia $0 \neq a \in F$. Allora

$$(at^n)' = a' t^n + ant^{n-1} t' = (a' + abn)t^n$$

Ora se $a' + abn = 0$, allora $(at^n)' = 0$ e dunque at^n sarebbe una costante, dunque un elemento di F contraddicendo l'ipotesi di trascendenza di t su F. Dunque $a' + abn \neq 0$. Pertanto si ha che se $f(t) \in F[t]$, allora $(f(t))'$ è un polinomio di grado dello stesso grado di $f(t)$.

□

Dimostriamo adesso il risultato centrale della tesi.

Teorema 4 (Liouville)**.** *Sia $(F,')$ un campo differenziale e $f \in F$. Le due affermazioni seguenti sono equivalenti*

(i) Esiste una estensione elementare $E|F$ tali che $C_E = C_F$ e $g \in E$ con $g' = f$.

(ii) Esistono $v \in F, u_1, \ldots, u_n \in F^*$ e $c_1, \ldots, c_n \in C_F$ tale che

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

Dimostrazione. (ii) $\Rightarrow$ (i). Basta porre

$$g = \left(v + \sum_{i=1}^{N} c_i \log(u_i) \right).$$

In tal modo $g' = f$.
(i) $\Rightarrow$ (ii). Poiché l'estensione $E|F$ è elementare, esistono $t_1, t_2, \ldots, t_m \in F$ tali che $E = F(t_1, \ldots, t_m)$ e, per ogni $i = 1, \ldots, m$, t_i è un elemento algebrico, o esponenziale, o un logaritmo su $F(t_1, \ldots, t_{i-1})$. Inoltre poiché E ha lo stesso sottocampo delle costanti di F, allora ogni campo differenziale L tale che $E|L|F$ avrà lo stesso sottocampo delle costanti. Proviamo il teorema per induzione su m. Per $m = 0$ si ha che $E = F$ e dunque il teorema è banalmente dimostrato: con $v = y$. Assumiamo il teorema verso per ogni estensione elementare di campi $F(t_1, \ldots, t_m)$ e consideriamo la catena di estensioni $F(t_1, \ldots, t_m)|F(t_1)|F$. Per ipotesi induttiva esistono $c_1, \ldots, c_n \in C_F$, $u_1, \ldots, u_n \in F(t_1)^*, v \in F(t_1)$ tali che $f = v' + \sum_{i=1}^{n} c_i \frac{u_i'}{u_i}$. Dobbiamo dimostrare che esiste una tale espressione con per f con $u_1, \ldots, u_n \in F^*, v \in F$ (eventualmente per un n diverso). Sia $t = t_1$; dividiamo la dimostrazione in tre casi: quello in cui t è algebrico, quello in cui t è un logaritmo e infine quello in cui t è esponenziale.

Il caso algebrico Poiché t è algebrico su F, esistono $U_1, \ldots, U_n, V \in F[x]$ tale che $U_1(t) = u_1, \ldots, U_n(t) = u_n, V(t) = v$. Consideriamo ora il polinomio minimo di t su F $p_t = \min_F(b)$ e i coniugati distinti di t su $\tau_1(= t), \tau_2, \ldots, \tau_s$ in K, campo di spezzamento di p_t su F . Dato che $K|F$ è algebrica, grazie al Teorema 3 la derivata su F può essere estesa in modo unico su F. Per ipotesi si ha allora che

$$f = (V(\tau_1))' + \sum_{i=1}^{n} c_i \frac{(U_i(\tau_1))'}{U_i(\tau_1)} \tag{1}$$

Poiché il polinomio p_t è separabile e irriducibile su F, allora per la proposizione 1 il sottogruppo di S_n isomorfo al gruppo di Galois $\mathrm{Gal}(K|F)$ è transitivo e dunque per ogni τ_j coniugato di τ_1 esiste $\sigma \in \mathrm{Gal}(K|F)$ tale che $\sigma(\tau_1) = \tau_j$.

Applicando σ ad entrambi i membri dell'equazione (1) si ha:

$$\begin{aligned}\sigma(f) = f =&\sigma\left((V(\tau_1))' + \sum_{i=1}^{n} c_i \frac{(U_i(\tau_1))'}{U_i(\tau_1)}\right)\\ =&\sigma((V(\tau_1))') + \sum_{i=1}^{n} \sigma(c_i)\frac{\sigma(U_i(\tau_1))'}{\sigma(U_i(\tau_1))}\\ =&\sigma(V(\tau_1))' + \sum_{i=1}^{n} c_i \frac{\sigma((U_i(\tau_1))'}{U_i(\tau_j)}.\end{aligned}$$

Con le notazioni del Teorema 3 scriviamo meglio chi è $\sigma(V(\tau_1)')$:

$$\begin{aligned}\sigma(V(\tau_1)') =&\sigma((D_0V)(\tau_1) + (D_1V)(\tau_1)\tau_1'\\ =&D_0V(\sigma(\tau_1)) + D_1V(\sigma(\tau_1))\left(-\frac{(D_0V)(p_t)}{(D_1V)(\sigma(p_t))}\right)\\ =&D_0V(\tau_j) + D_1V(\tau_j)\left(-\frac{D_0V(p_t)}{D_1V(p_t)}\right) = (V(\tau_j))'.\end{aligned}$$

In modo analogo si ha che $\sigma(U_i(\tau_1))' = (U_i(\tau_j))'$. Si ha dunque che

$$f = (V(\tau_j))' + \sum_{i=1}^{n} c_i \frac{(U_i(\tau_j))'}{U_i(\tau_j)}, \quad \forall\, j \in \{1, \dots, s\}.$$

Sommando ora su j ad entrambi i membri e dividendo per s, si ottiene

$$\begin{aligned}f =&\frac{(V(\tau_1))'}{s} + \cdots + \frac{(V(\tau_s))'}{s} + \sum_{i=1}^{n} \frac{c_i}{s}\left(\frac{(U_i(\tau_1))'}{U_i(\tau_1)} + \cdots + \frac{(U_i(\tau_s))'}{U_i(\tau_s)}\right) =\\ &\left(\frac{V(\tau_1) + \cdots + V(\tau_s)}{s}\right)' + \sum_{i=1}^{n} \frac{c_i}{s}\frac{(U_i(\tau_1)\cdots U_i(\tau_s))'}{U_i(\tau_1)\cdots U_i(\tau_s)}\end{aligned}$$

in cui nel secondo passaggio si è usato il punto 5 della Proposizione 3. Adesso notiamo che $U_i(x_1)\cdots U_i(x_s)$ e $V(x_1) + \cdots + V(x_s)$ sono polinomi simmetrici in $F[x_1, \dots, x_s]$ e dato che $\tau_1 \dots, \tau_s$ sono le radici del polinomio minimo di t su F, allora per il Teorema 1 si ha che $U_i(\tau_1)\dots U_i(\tau_s), V(\tau_1) + \cdots + V(\tau_s) \in F$ e dunque si ha la tesi.
Prima di passare ai casi logaritmo ed esponenziale, è conveniente fare una premessa. Supponiamo che t sia trascendente su F. Allora per ipotesi sappiamo che esistono $u_1(t), \dots, u_n(t), v(t) \in F(t)$ e $c_1, \dots, c_n \in C_F$ tali che

$$f = (v(t))' + \sum_{i=1}^{n} c_i \frac{(u_i(t))'}{u_i(t)} \tag{2}$$

Ora dato che $u_i(t) \in F(t)$ per ogni $i = 1, \dots, n$, esistono $p_i, q_i \in F[t]$ tali che $u_i(t) = \frac{p_i}{q_i}$. Considerando la scomposizione in irriducibili di p_i e q_i si ottiene

$$u_i(t) = \frac{p_i}{q_i} = \frac{p_{1i}^{\alpha_{1i}} \dots p_{si}^{\alpha_{si}}}{q_{1i}^{\beta_{1i}} \dots q_{ri}^{\beta_{ri}}} = p_{1i}^{\alpha_{1i}} \dots p_{si}^{\alpha_{si}} q_{1i}^{-\beta_{1i}} \dots q_{ri}^{-\beta_{ri}}$$

Da cui segue, usando le proprietà della Proposizione 3 che

$$\frac{(u_i(t))'}{u_i(t)} = \sum_{j=1}^{s} \alpha_{ji} \frac{p'_{ji}}{pji} - \sum_{k=1}^{r} \beta_{ki} \frac{q'_{ki}}{q_{ri}}.$$

Da questa osservazione segue che la sommatoria nell'equazione (2) si può riscrivere nella forma

$$\sum_{i=1}^{N} \tilde{c}_i \frac{\tilde{u}'_i}{\tilde{u}_i}$$

in cui per ogni $i = 1, \dots N$ $\tilde{c}_i \in C_F$ e $u_i \in F[t]$ è monico e irriducibile (oppure direttamente un elemento di F). Consideriamo ora il Teorema 2, che ci dice che è possibile decomporre v in fratti semplici:

$$v = T + \sum_{i=1}^{n} \sum_{j=1}^{k_i} \frac{S_{ij}}{P_i^j}.$$

Possiamo perciò riscrivere l'equazione (2) nel seguente modo:

$$f = T' + \sum_{i=1}^{N} \tilde{c}_i \frac{\tilde{u_i}'}{\tilde{u}_i} + \sum_{i=1}^{n} \sum_{j=1}^{k_i} \left(\frac{S'_{ij}}{P_i^j} - \frac{j S_{ij} P_i^j}{P_i^{j+1}} \right). \tag{3}$$

Il caso logaritmo Supponiamo che $t' = a'/a$ (cioè $t = \log(a)$) per un certo $a \in F$, allora $t' \in F$. Per il lemma 1 si ha che per ogni polinomio monico $p(t) \in F[t]$ di grado $n > 0$, $(f(t))'$ è un polinomio in $F[t]$ di grado $n - 1$. Da ciò segue che $p(t)$ non divide $(p(t))'$. Applicando questo ragionamento ad uno dei P_i nella decomposizione in fratti semplici di v si ha che nell'equazione (3) compare un termine con $P_i^{k_i+1}$ al denominatore. Poiché non vi è alcun termine che cancella $P_i^{k_i+1}$, allora deve apparire nella scrittura di f, ma questo è assurdo perché f non dipende da t. Da ciò segue che $v = T \in F[t]$ e perciò

$$f = T' + \sum_{i=1}^{N} \tilde{c}_i \frac{\tilde{u_i}'}{\tilde{u}_i}.$$

Adesso riapplicando il ragionamento precedente a $\tilde{u_i}$ si ha che non vi è alcun termine a destra che cancella $\tilde{u_i}$ e dunque $\tilde{u_i}$ apparirà nella scrittura di f. Pertanto $\tilde{u_i} \in F$ per ogni $i = 1, \dots, N$. Abbiamo dimostrato dunque che

$$T' = f - \sum_{i=1}^{N} \tilde{c}_i \frac{\tilde{u_i}'}{\tilde{u}_i} \in F.$$

Dal Lemma 1, segue che $T = ct + d$ con $c \in C_F$ e $d \in F$. Infine quindi

$$f = \sum_{i=1}^{N} \tilde{c}_i \frac{\tilde{u_i}'}{\tilde{u}_i} + c\frac{a'}{a} + d',$$

che è un'espressione della forma desiderata.

Il caso esponenziale Supponiamo ora che $t = e^b \in F$. Allora, sempre per il Lemma 1 si ha che per ogni polinomio $f(t) \in F[t]$ monico, irriducibile e diverso da t, $f(t)$ non divide $(f(t))'$. Ragionando in modo analogo al caso sopra si può concludere che $v \in F[t]$ e $\tilde{u_i} \in F$ per ogni i, oppure uno di essi è uguale a t. Si conclude che

$$v' = f - \sum_{i=1}^{N} \tilde{c_i} \frac{\tilde{u_i}'}{\tilde{u_i}} \in F$$

e, ancora per il Lemma 1 si ha che $v \in F$ ottenendo un'espressione della forma desiderata. □

Utilizzando questo teorema si può dimostrare un risultato analogo nel caso in cui il campo delle costanti C_F sia algebricamente chiuso.

Teorema 5. *Sia $(F,')$ un campo differenziale con campo delle costanti C_F algebricamente chiuso e sia $f \in F$. Se esiste un'estensione elementare E di F e $g \in E$ tale che $g' = f$, allora esistono $v \in F, u_1, \dots u_n \in F^*$ e $c_1, \dots, c_n \in C_F$ tali che*

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

Il seguente teorema, che generalizza il risultato di Liouville rimuovendo la restrizione sul sottocampo delle costanti è stato provato da Risch nel nel 1970.

Teorema 6 (Risch, 1970)**.** *Sia $(F,')$ un campo differenziale, C il suo campo delle costanti e $f \in F$. Se esiste un'estensione elementare E di F e $g \in E$ tale che $g' = f$, allora esistono $v \in F, c_1, \dots, c_n \in \overline{C}$ e $u_1, \dots, u_n \in F(c_1, \dots, c_n)^*$ tale che*

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

Una dimostrazione di questi risultati si può trovare in [Bro]

5 Esempi di funzioni non integrabili elementarmente

In questo capitolo considereremo il campo differenziale $\mathbb{C}(x)$ con la derivata standard, che indicheremo col classico simbolo $'$. 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

$$f = \mathrm{Re} f + i\ \mathrm{Im} f.$$

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 dà le seguenti relazioni:

$$\sin(x) = \frac{e^{ix} - e^{-ix}}{2i}; \quad \cos(x) = \frac{e^{ix} + e^{-ix}}{2}; \quad \tan(x) = \frac{e^{ix} - e^{-ix}}{e^{ix} + e^{-ix}}$$

$$\arcsin(x) = \frac{\pi}{2} + i\ln(ix + \sqrt{1 - x^2}); \quad \arctan(x) = \frac{i}{2}[\ln(1 - ix) - \ln(1 + ix)]$$

Teorema 7. *Sia $g \in \mathbb{C}(x)$ una funzione razionale non costante. Allora la funzione e^g è trascendente su $\mathbb{C}(x)$.*

Una dimostrazione si può trovare per esempio in [Del]
Vogliamo adesso derivare un criterio per stabilire in quali casi $f(x)e^{g(x)}dx$ ammetta una primitiva elementare, con $f(x)$ e $g(x)$ funzioni razionali, $f(x) \neq 0$ e $g(x)$ non costante. Scriviamo $e^g = t$, in tal modo abbiamo $t'/t = g'$, e immaginiamo di lavorare nel campo differenziale $\mathbb{C}(x, t)$, una estensione trascendente di $\mathbb{C}(x)$

Teorema 8. *Siano $f, g \in \mathbb{C}(x)$, $f \neq 0, g$ non costante. Allora la funzione $h(x) = f(x)e^{g(x)}$ ammette una primitiva elementare se e solo se esiste $a \in \mathbb{C}(x)$ tale che $f = a' + ag'$*

Dimostrazione. ($\Leftarrow$) Scrivendo $e^g = t$, abbiamo che $t' = tg'$. Supponiamo ora che esista $a \in \mathbb{C}(x)$ tale che $f = a' + ag'$. Allora

$$(at)' = a't + at' = a't + ag't = (a' + ag')t = ft$$

e dunque at è una primitiva di h ed è una funzione elementare (che sta in $\mathbb{C}(x, t)$ che è elementare per la Definizione 6)
($\Rightarrow$) Supponiamo che h ammette una primitiva elementare $y \in E$ con E estensione elementare di $C(x, e^g)$. Allora per il teorema di Liouville esistono $c_1, \ldots, c_n \in \mathbb{C}$, $u_1, \ldots, u_n, v \in C(x, e^g)$ tali che

$$fe^g = v' + \sum_{i=1}^{n} c_i \frac{u_i'}{u_i}. \tag{4}$$

Essendo e^g un elemento non algebrico ed esponenziale su $\mathbb{C}(x)$, ricordando la dimostrazione del teorema di Liouville si può riscrivere l'equazione (4) come

$$fe^g = v' + \sum_{i=1}^{N} d_i \frac{v_i'}{v_i},$$

con $d_i \in \mathbb{C}, v_i \in \mathbb{C}(x)$ (oppure uno di essi uguale a e^g) e $v \in \mathbb{C}(x)[e^g]$. Posto $d = \sum_{i=1}^{N} d_i \frac{v_i'}{v_i} \in \mathbb{C}(x)$ si ha

$$fe^g = d + v'.$$

Poiché il membro a sinistra è un polinomio in $\mathbb{C}(x)[e^g]$ di grado 1, allora anche il membro a destra deve esserlo. Dunque si ha che $v = s_0 + s_1 e^g$ con $s_0, s_1 \in \mathbb{C}(x)$. Pertanto si ottiene

$$fe^g = d + (s_0 + s_1 e^g)' = d + s_0' + s_1' e^g + s_1 g' e^g,$$

da cui

$$e^g(f - s_1' - s_1 g') = d + s_0'. \tag{5}$$

Poiché $f - s_1' - s_1 g'$ e $d + s_0'$ sono funzioni razionali mentre e^g non lo è, si ha che l'equazione (5) è soddisfatta se e solo se

$$f - s_1' + s_1 g' = 0.$$

Ponendo $a := s_1$ si ha la tesi.

□

Esempi notevoli Utilizzando il Teorema 8 è possibile dimostrare che non esiste una primitiva elementare per alcune note funzioni.

$$\boldsymbol{e^{x^2}}$$

Il nostro obiettivo è negare l'esistenza di una funzione razionale $a = \frac{P}{Q}$ tale che $a' + ag' = e^{x^2}$, con P e Q polinomi a coefficienti complessi, che supponiamo primi tra loro. Visto che $g(x) = x^2$ e $f(x) = 1$, l'identità che essi risolverebbero sarebbe

$$\frac{P'Q - PQ'}{Q^2} + \frac{2xP}{Q} = 1$$

che è equivalente a

$$P'Q - Q'P + 2xPQ = Q^2. \tag{6}$$

Da questa relazione si nota che, dato che Q divide Q^2, allora Q dovrebbe dividere il polinomio $Q'P$. Visto però che Q e P sono primi tra loro, Q dovrebbe dividere Q'. D'altra parte questo implicherebbe che $\deg(Q) \leq \deg(Q')$ e ciò è possibile solo se Q è un polinomio costante. Dunque l'identità (6) diverrebbe

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

Chiaramente però nessun polinomio può soddisfare quest'ultima uguaglianza. Non è difficile vedere che non cambia nulla se al posto di e^{x^2} prendiamo e^{-x^2} ovvero la Gaussiana.

$$\boldsymbol{\frac{e^x}{x}}$$

Supponiamo esista una funzione razionale $a \in \mathbb{C}(x)$ tale che

$$\frac{1}{x} = a' + a. \tag{7}$$

Allora, scrivendo a come $\frac{P}{Q}$ con $P, Q \in \mathbb{C}[x]$ primi tra loro, si può riscrivere (7) come

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

che diventa

$$1 = \frac{x(PQ + P'Q - PQ')}{Q^2} \quad \text{cioé } Q^2 = x(PQ + P'Q - PQ').$$

In particolare si ha che Q^2 deve dividere il numeratore, ma Q^2 non divide x in quanto il primo è un prodotto di polinomi di secondo grado e il secondo è un polinomio lineare. Inoltre $Q(x)$ non divide né Q' (sempre perché $\deg(Q) \leq \deg(Q')$) né P (perché abbiamo supposto che P, Q siano primi tra di loro). Dunque, come in precedenza, si ha che $a \in \mathbb{C}[x]$. L'equazione (7) diventa della forma

$$\frac{1}{x} = P + P'.$$

Poiché il membro a destra dell'equazione è un polinomio e il membro a sinistra è una funzione razionale, si può concludere che non esiste alcun $a \in \mathbb{C}[x]$ che soddisfi l'uguaglianza, e dunque per il Teorema 8 la funzione $\frac{e^x}{x}$ non ammette una primitiva elementare.

$$\frac{\boldsymbol{\sin x}}{\boldsymbol{x}}$$

Risulta

$$\int \frac{\sin x}{x} dx = \int \frac{e^{ix} - e^{-ix}}{2ix} dx = \frac{1}{2i} \left(\int \frac{e^{ix}}{x} dx - \int \frac{e^{-ix}}{x} dx \right)$$

che, per quanto visto in precedenza non è elementarmente integrabile.

$$\frac{\boldsymbol{e^x}}{\boldsymbol{x^n}} \quad n \in \mathbb{N}$$

Per $n > 0$ definiamo I_n nel seguente modo:

$$I_n = \int \frac{e^x}{x^n} dx.$$

Tramite integrazioni per parte possiamo scrivere

$$I_n = \frac{1}{n-1} \left(\int \frac{e^x}{x^{n-1}} dx - \frac{e^x}{x^{n-1}} \right) = \frac{1}{n-1} \left(I_{n-1} - \frac{e^x}{x^{n-1}} \right).$$

Si nota che I_n è elementarmente integrabile se e solo se lo è I_{n-1}. Possiamo dunque esprimere I_n in termini di I_{n-1}. Iterando questo procedimento $n-1$ volte arriviamo infine a scrivere I_n in funzione di I_1, ovvero di $\int \frac{e^x}{x} dx$, che abbiamo dimostrato non essere elementarmente integrabile.

$$\frac{\mathbf{1}}{\mathbf{ln^n(x)}} \quad n \in \mathbb{N}$$

Per quanto riguarda questa funzione, con facili passaggi di integrazione per sostituzione si ha che

$$\int \frac{dt}{\ln^n(t)} \underbrace{=}_{\ln(t)=x} \int \frac{e^x}{x^n} dx$$

E dunque, per quanto dimostrato in precedenza, anche $\frac{1}{\ln^n(x)}$ non è elementarmente integrabile.

Integrali Ellittici

La teoria delle funzioni ellittiche nasce dal calcolo della lunghezza dell'ellisse, esse si ottengono invertendo funzioni della forma $\int dx/\sqrt{P(x)}$ per particolari polinomi P con $P \in \mathbb{R}[x]$ senza radici multiple. In generale se $P \in \mathbb{R}[x]$ ha grado ≥ 3 e ha tutte radici semplici, allora $\int dx/\sqrt{P(x)}$ non è elementarmente integrabile. Dato che $F := \mathbb{C}(x, \sqrt{P})$ è un campo differenziale, dal teorema di Liouville è sufficiente provare che non esiste un'identità della forma

$$\frac{1}{\sqrt{P(x)}} = v' + \sum_{i=1}^{n} c_i \frac{u_i'}{u_i},$$

con $c_1, \ldots, c_n \in \mathbb{C}$ e $u_1, \ldots, u_n, v \in F$. Dalla teoria delle superfici di Riemann compatte si deduce l'impossibilità di una tale identità. Per i dettagli si può vedere [Con]

Riferimenti bibliografici

[Cas] C.Casolo, Dispense del corso di Algebra II, Università degli studi di Firenze

[Del] C.De Lellis, Il Teorema di Liouville ovvero perché non esiste la primitiva di e^{x^2} , `http://www.math.uzh.ch/fileadmin/user/delellis/publikation/Liouville_finale.pdf`

[Bro] M.Bronstein, Symbolic Integration I Trascendental Functions, Springer, 2005

[Gre] A. Greco, Integrazione in termini finiti, Archimede Vol 2 ,(1999), 82-88

[Ris] R.Risch, The problem of integration in finite terms, 1968

[Con] B. Conrad, Impossibility theorems for elementary integration, `http://math.stanford.edu/~conrad/papers/elemint.pdf`